NSC NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA	Narodowy Standard Cyberbezpieczeństwa		
Nazwa standardu	Symbol	Wersja	Data wydania
ZABEZPIECZENIA I OCHRONA PRYWATNOŚCI SYSTEMÓW INFORMATYCZNYCH ORAZ ORGANIZACJI	**NSC 800-53**	2.0	01/09/2021

Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji

PEŁNOMOCNIK RZĄDU DS. CYBERBEZPIECZEŃSTWA

Warszawa 2021

Szanowni Państwo,

Departament Cyberbezpieczeństwa Kancelarii Prezesa Rady Ministrów udostępnia do wykorzystania w Państwa działalności zestaw publikacji specjalnych. Stanowią one rekomendację w postaci Narodowych Standardów Cyberbezpieczeństwa, o których mowa w kierunku interwencji 6.1 Celu szczegółowego 2 Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024, *Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń*. Mimo, że prezentowane standardy zostały opracowane na podstawie publikacji amerykańskiego National Institute of Science and Technology (NIST), to posiadają one mapowanie na obowiązujące w polskim systemie prawnym Polskie Normy, stosowane w zarządzaniu bezpieczeństwem informacji przez podmioty krajowego systemu cyberbezpieczeństwa, w tym podmioty realizujące zadania publiczne, operatorów usług kluczowych i dostawców usług cyfrowych.

Zaprezentowane publikacje stanowią przewodniki metodyczne, które ułatwiają zbudowanie efektywnego systemu zarządzania bezpieczeństwem informacji w oparciu o praktykę, jaka w tym zakresie stosowana jest w administracji federalnej USA.

Na prezentowany zestaw publikacji składają się następujące pozycje:[1]

- NSC[2] 199, *Standardy kategoryzacji bezpieczeństwa* – na podstawie FIPS 199;
- NSC 200, *Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych* – na podstawie FIPS 200;
- NSC 500-92, *Architektura referencyjna chmury obliczeniowej – rekomendacje* – na podstawie NIST SP 500-292;
- NSC 800-18, *Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych* – na podstawie NIST SP 800- 18;
- NSC 800-30, *Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne* – na podstawie NIST SP 800-30;
- NSC 800-34, *Poradnik planowania awaryjnego* – na podstawie NIST SP 800-34;

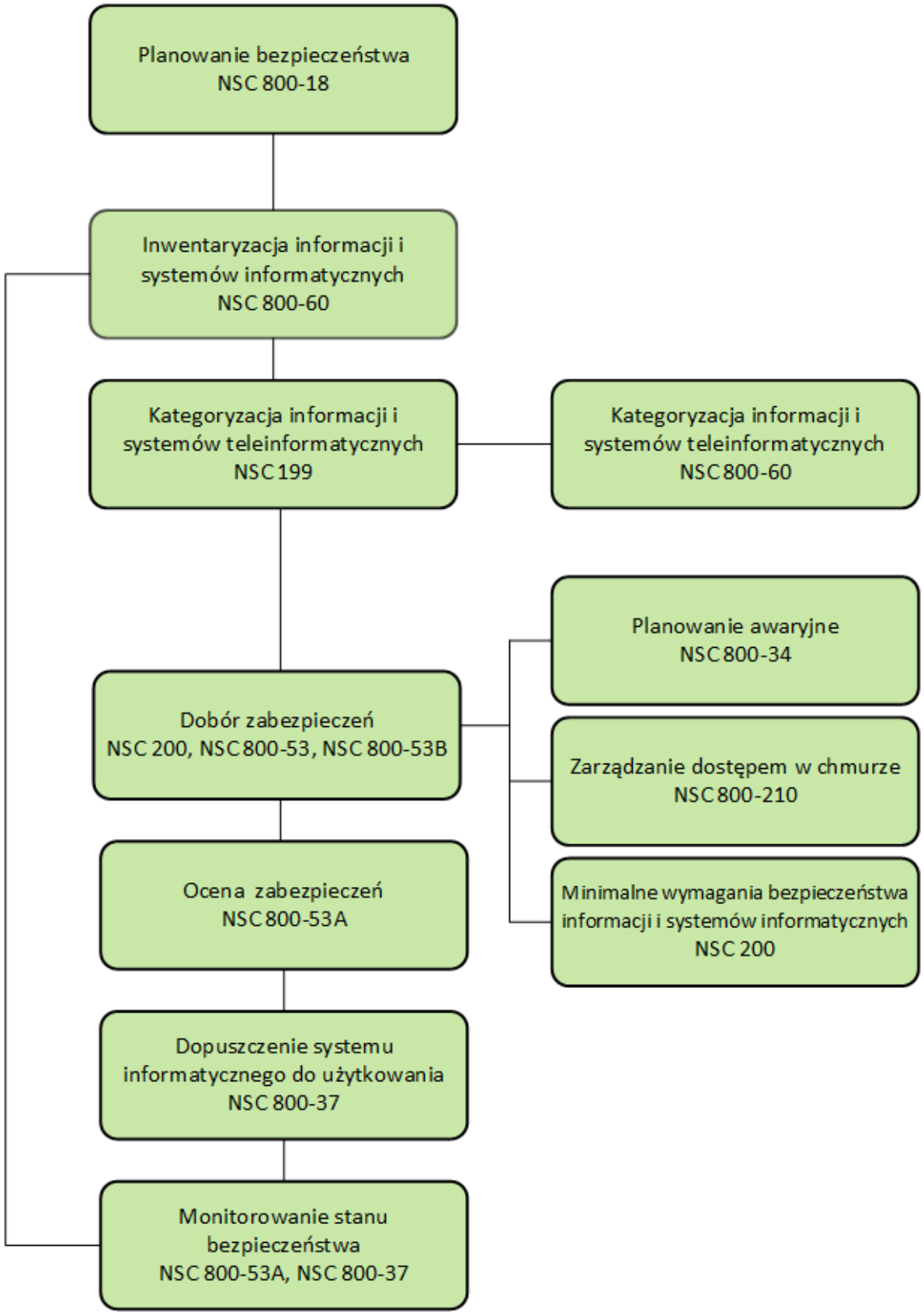
[1] Wymienione są podstawowe dokumenty. Każdy z nich może się odwoływać w rozdziale *Referencje* do szeregu powiązanych publikacji, które składają się na całościowy proces osiągania cyberbezpieczeństwa.

[2] NSC – Narodowy Standard Cyberbezpieczeństwa.

- NSC 800-37, *Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu* – na podstawie NIST SP 800-37;
- NSC 800-53, *Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji* – na podstawie NIST SP 800-53;
- NSC 800-53A, *Ocena środków bezpieczeństwa i ochrony prywatności systemów informatycznych oraz organizacji. Tworzenie skutecznych planów oceny* – na podstawie NIST SP 800-53A;
- NSC 800-53B, *Zabezpieczenia bazowe systemów informatycznych oraz organizacji* – na podstawie NIST SP 800-53B;
- NSC 800-60, *Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego* – na podstawie NIST SP 800-60;
- NSC 800-61, *Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego* – na podstawie NIST SP 800-61;
- NSC 800-210, *Ogólne wytyczne dotyczące kontroli dostępu do systemów chmury obliczeniowej* – na podstawie NIST SP 800-210.

Korzystając z tych publikacji można stosunkowo łatwo zbudować system zarządzania bezpieczeństwem informacji i sprawować nad nim niezbędną kontrolę.

Cykl zarządzania bezpieczeństwem bazujący na publikacjach NIST wykorzystuje następujące dokumenty:


Planowanie bezpieczeństwa
NSC 800-18
Inwentaryzacja informacji i systemów informatycznych
NSC 800-60
Kategoryzacja informacji i systemów teleinformatycznych
NSC 199
Kategoryzacja informacji i systemów teleinformatycznych
NSC 800-60
Planowanie awaryjne
NSC 800-34
Dobór zabezpieczeń
NSC 200, NSC 800-53, NSC 800-53B
Zarządzanie dostępem w chmurze
NSC 800-210
Ocena zabezpieczeń
NSC 800-53A
Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych
NSC 200
Dopuszczenie systemu informatycznego do użytkowania
NSC 800-37
Monitorowanie stanu bezpieczeństwa
NSC 800-53A, NSC 800-37

WSPÓLNE FUNDAMENTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

National Institute of Standards and Technology (NIST) opracował wiele standardów i wytycznych w celu zapewnienia wspólnego podejścia do problematyki bezpieczeństwa informacji i systemów teleinformatycznych administracji federalnej USA. Podstawową rolę w podejściu do zagadnień związanych z zapewnieniem bezpieczeństwa informacji, bezpieczeństwa systemów teleinformatycznych oraz ochrony prywatności odgrywa elastyczny i spójny sposób zarządzania ryzykiem związanym z bezpieczeństwem i prywatnością operacji organizacyjnych i majątku, osób fizycznych, innych organizacji i Państwa. Zarządzanie ryzykiem stanowi podstawę do wdrożenia stosownych zabezpieczeń w systemach informacyjnych, ocenę tych zabezpieczeń, wzajemną akceptację dowodów oceny bezpieczeństwa i ochrony prywatności oraz decyzji autoryzacyjnych, a także dzięki jednolitemu podejściu, ułatwia wymianę informacji i współpracę pomiędzy różnymi podmiotami.

NIST kontynuuje współpracę z sektorem publicznymi i prywatnym w celu stworzenia map i relacji pomiędzy opracowanymi przez siebie standardami i wytycznymi, a tymi, które zostały opracowane przez inne organizacje (np. ISO), co zapewnia zgodność w przypadku, gdy regulacje wymagają stosowania tych innych standardów.

Publikacje NIST, co do zasady, nie są objęte restrykcjami wynikającymi z autorskich praw majątkowych. Są powszechnie dostępne oraz dozwolone do użytku poza administracją federalną USA. Charakteryzują się pragmatycznym podejście do zagadnień związanych z bezpieczeństwem informacji, systemów teleinformatycznych oraz ochrony prywatności, przez co ułatwiają podmiotom opracowanie i eksploatację systemu zarządzania tym bezpieczeństwem.

Biorąc pod uwagę wszystkie powyższe aspekty, autorzy niniejszej publikacji polecają opracowania NIST, jako godne zaufania i rekomendują stosowanie ich przez polskie podmioty w opracowywaniu systemów zarządzania bezpieczeństwem informacji, wdrażaniu zabezpieczeń i ocenie ich działania.

Podmioty, urządzenia lub materiały prezentowane są w niniejszym dokumencie w celu odpowiedniego opisania procedury lub koncepcji eksperymentalnej. Identyfikacja taka nie ma na celu nakłaniania do nich lub ich poparcia, nie ma też na celu sugerowania, że te podmioty, materiały lub sprzęt są najlepsze z dostępnych w tym obszarze.

W niniejszym Narodowym Standardzie Cyberbezpieczeństwa (NSC) mogą znajdować się odniesienia do innych publikacji opracowywanych obecnie przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa zgodnie z przypisanymi mu obowiązkami ustawowymi. Informacje zawarte w tej publikacji, w tym koncepcje, praktyki i metodologie, mogą być wykorzystywane przez organizacje jeszcze przed ukończeniem innych towarzyszących temu standardowi publikacji. W związku z tym, do czasu ukończenia każdej publikacji, obowiązują aktualne wymagania, wytyczne i procedury, jeśli takie istnieją. W celach planistycznych i wprowadzania zmian, organizacje będą mogły uważnie śledzić rozwój tych nowych publikacji opracowywanych przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa.

Niniejsza publikacja, ***Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji***, opracowana została za zgodą National Institute of Science and Technology (NIST) na podstawie specjalnej publikacji NIST SP 800-53, Rev. 5 (zawierającej poprawki z dnia 10.12.2020 r.).

Tam, gdzie to było możliwe i nie budziło kontrowersji, nazwy ról i kluczowych uczestników procesu zarządzania ryzykiem zostały podane w języku polskim. Pozostałe role i funkcje zostały przedstawione w języku angielskim. Do wszystkich tych ról / funkcji zastosowano akronimy terminologii angielskiej.

Terminologia angielska i akronimy oraz kluczowe pojęcia z zakresu cyberbezpieczeństwa występujące w publikacji zdefiniowane są w dokumencie NSC 7298, ***Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa***.

Sprawozdania dotyczące technologii systemów informatycznych

Promowana jest gospodarka polska i opieka społeczna poprzez zapewnienie technicznego zaangażowania w infrastrukturę pomiarową i normalizacyjną kraju. Służy temu m. in. opracowywanie testów, metod badań, danych referencyjnych; dowody realizacji koncepcji oraz analizy techniczne w celu przyspieszenia rozwoju i produktywnego wykorzystania technologii informatycznych (*ang. Information Technology - IT*)[3]. Obejmuje to rozwój standardów zarządzania, administracyjnych, technicznych i fizycznych oraz wytycznych dotyczących efektywnego kosztowo bezpieczeństwa w systemach informatycznych. Publikacje serii 800, zawierają raporty dotyczące badań, wytycznych i działań informatycznych w zakresie bezpieczeństwa i ochrony prywatności systemów informatycznych.

Abstrakt

Niniejsza publikacja zawiera katalog środków bezpieczeństwa i ochrony prywatności systemów informatycznych oraz organizacji, mających na celu ochronę operacji organizacyjnych i aktywów, osób, innych organizacji i Państwa, przed zróżnicowanym zestawem zagrożeń i ryzyka, w tym wrogimi atakami, błędami ludzkimi, klęskami żywiołowymi, awariami strukturalnymi, podmiotami obcego wywiadu oraz zagrożeniami dla prywatności. Zabezpieczenia są elastyczne i możliwe do dostosowania, a ich wdrożenie stanowi część procesu zarządzania ryzykiem w całej organizacji. Zabezpieczenia spełniają zróżnicowane wymagania wynikające z misji i potrzeb biznesowych, prawa, rozporządzeń wykonawczych, dyrektyw, regulacji, polityk, standardów i wytycznych. Skonsolidowany katalog zabezpieczeń odnosi się do bezpieczeństwa i ochrony prywatności z perspektywy funkcjonalności (tj. siły funkcji i mechanizmów zapewnianych przez zabezpieczenia) oraz z perspektywy wiarygodności (tj. miary zaufania do bezpieczeństwa lub możliwości ochrony prywatności zapewnianych przez środki bezpieczeństwa). Uwzględnianie funkcjonalności

[3] Terminologia angielska i akronimy występujące w publikacji zdefiniowane są w dokumencie NSC 7298, Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa.

i wiarygodności zabezpieczeń przyczynia się do zapewnienia, że technologie i systemy informatyczne, które opierają się na tych produktach, są wystarczająco godne zaufania.

Słowa kluczowe

Wiarygodność; dostępność; bezpieczeństwo komputerowe (cyberbezpieczeństwo); poufność; zabezpieczenia (środki bezpieczeństwa); bezpieczeństwo informacji; system informatyczny; integralność; dane osobowe; ustawa o ochronie danych osobowych; ustawa o ochronie informacji niejawnych; zabezpieczenia prywatności; funkcje ochrony prywatności; wymagania dotyczące prywatności; ramy zarządzania ryzykiem; funkcje bezpieczeństwa; wymagania dotyczące bezpieczeństwa; system informatyczny; bezpieczeństwo systemu.

ZARZĄDZANIE RYZYKIEM

Organizacje muszą zachować należytą *staranność* w zarządzaniu ryzykiem związanym z bezpieczeństwem informacji i ochroną prywatności. Osiąga się to częściowo poprzez ustanowienie kompleksowego programu zarządzania ryzykiem, który wykorzystuje elastyczność właściwą publikacjom NSC do kategoryzacji systemów, doboru i wdrażania środków bezpieczeństwa i ochrony prywatności, które odpowiadają misji i potrzebom biznesowym, oceny skuteczności zabezpieczeń, autoryzacji systemów do działania oraz ciągłego monitorowania systemów. Badanie *due diligence* i wdrażanie solidnych i kompleksowych programów zarządzania ryzykiem związanym z bezpieczeństwem informacji i ochroną prywatności, może ułatwić zachowanie zgodności z obowiązującymi przepisami prawa, regulacjami, rozporządzeniami wykonawczymi i polityką rządu. Ramy zarządzania ryzykiem oraz procesy zarządzania ryzykiem są niezbędne do opracowania, wdrożenia i utrzymania środków bezpieczeństwa niezbędnych do zaspokojenia potrzeb interesariuszy oraz bieżących zagrożeń dla działalności i majątku organizacji, osób fizycznych, innych organizacji i Państwa. Zastosowanie efektywnych procesów, procedur, metod i technologii opartych na analizie ryzyka gwarantuje, że systemy informatyczne i organizacje posiadają niezbędną wiarygodność i odporność, aby wspierać najważniejsze misje i funkcje biznesowe, infrastrukturę krytyczną oraz ciągłość działania.

ROZWÓJ SYSTEMÓW INFORMATYCZNYCH, KOMPONENTÓW I USŁUG

Przy zwiększonym nacisku na stosowanie wiarygodnych, bezpiecznych systemów informatycznych i bezpieczeństwo łańcucha dostaw, niezbędne jest, aby organizacje wyraziły swoje wymagania w zakresie bezpieczeństwa i ochrony prywatności w sposób jasny i konkretny, w celu nabycia systemów, komponentów i usług niezbędnych dla misji i sukcesu biznesowego. W związku z tym, niniejsza publikacja przedstawia zabezpieczenia w kategoriach **Nabywanie systemu i usług** (*ang. System and Services Acquisition - SA*) oraz **Zarządzanie ryzykiem w łańcuchu dostaw** (*ang. Supply Chain Risk Management - SR*), które są skierowane do deweloperów. Zakres zabezpieczeń w tych kategoriach obejmuje rozwój systemów informatycznych, komponentów systemów i usług systemowych oraz związanych z nimi programistów, niezależnie od tego, czy rozwój jest prowadzony wewnętrznie przez organizacje, czy też zewnętrznie w ramach procesów kontraktowania i nabywania usług. Zawarte w katalogu zabezpieczeń środki bezpieczeństwa, których to dotyczą obejmują pozycje: SA-8, SA-10, SA-11, SA-15, SA-16, SA-17, SA-20, SA-21, SR-3, SR-4, SR-5, SR-6, SR-7, SR-8, SR-9 oraz SR-11.

SYSTEMY INFORMATYCZNE - SZEROKIE PERSPEKTYWY ROZWOJU

W miarę jak doprowadzamy komputery do "stanu granicznego", budując coraz bardziej złożony zbiór połączonych systemów i urządzeń, bezpieczeństwo i prywatność nadal dominują w krajowym dialogu. Istnieje pilna potrzeba dalszego wzmacniania podstawowych systemów, produktów i usług, od których jesteśmy zależni w każdym sektorze infrastruktury krytycznej, aby zapewnić, że te systemy, produkty i usługi są wystarczająco godne zaufania I zapewniają niezbędną odporność w celu wspierania gospodarczych i krajowych interesów bezpieczeństwa Państwa. NSC 800-53, wer. 2, odpowiada na tę potrzebę, podejmując proaktywne i systemowe podejście w celu opracowania i udostępnienia szerokiej bazie organizacji sektora publicznego i prywatnego kompleksowego zestawu środków bezpieczeństwa i ochrony prywatności dla wszystkich rodzajów platform obliczeniowych, w tym systemów obliczeniowych ogólnego przeznaczenia, systemów cyberfizycznych (ang. *Cyber-physical Systems – CPS*), systemów chmury obliczeniowej, systemów mobilnych, przemysłowych systemów zabezpieczeń oraz Internetu rzeczy (*ang. Internet of things - IoT*). Zabezpieczenia obejmują zarówno środki bezpieczeństwa i ochrony prywatności w celu ochrony krytycznych i zasadniczych operacji i aktywów organizacji oraz prywatności osób fizycznych. Celem jest uczynienie systemów, od których jesteśmy zależni, bardziej odpornymi na penetrację, ograniczenie szkód wyrządzanych przez te ataki w momencie ich wystąpienia oraz uczynienie systemów odpornymi, zdolnymi do przetrwania i chroniącymi prywatność osób fizycznych.

ZABEZPIECZENIA BAZOWE

Zestawy minimalnych zabezpieczeń (tzw. zabezpieczenia bazowe)[4], które w standardzie NSC 800-53 wer. 1[5] były przypisane do niskiego, umiarkowanego i wysokiego poziomu wpływu na bezpieczeństwo, zostały przeniesione do publikacji NSC 800-53B, ***Zabezpieczenia bazowe systemów informatycznych oraz organizacji***.[6] NSC 800-53B zawiera bazowe środki bezpieczeństwa i zabezpieczenia prywatności systemów informatycznych i organizacji.

Standard NSC 800-53B zawiera wytyczne dotyczące dostosowywania zabezpieczeń bazowych oraz opracowywania nakładek w celu spełnienia wymagań dotyczących bezpieczeństwa i ochrony prywatności stawianych przez interesariuszy i ich organizacje.

[4] W potocznym języku technicznym – „bejslajny".

[5] NSC 800-53 wer. 1, Zasady stosowania zabezpieczeń w systemach informatycznych podmiotów publicznych.

[6] NSC 800-53B opracowany został na podstawie publikacji NIST SP 800-53B, opublikowanej 12.10.2020 r.

KORZYSTANIE Z PRZYKŁADÓW W NINIEJSZEJ PUBLIKACJI

W niniejszej publikacji wykorzystano przykłady, wyjaśnienia lub opisy do zilustrowania niektórych pozycji zawartych w zabezpieczeniach i rozszerzeniach zabezpieczeń. Przykłady te mają charakter ilustracyjny i *nie mają na celu ograniczenia* lub zawężania stosowania przez organizacje zabezpieczeń lub zabezpieczeń rozszerzonych.

SPIS TREŚCI

STRESZCZENIE

W miarę jak doprowadzamy komputery do "stanu granicznego", budując coraz bardziej złożony zbiór połączonych systemów i urządzeń, bezpieczeństwo i prywatność nadal dominują w krajowym dialogu. W swoim sprawozdaniu z 2017 r. [DSB 2017][7] *grupa zadaniowa ds. walki z cyberprzestępczością* Rady Naukowej ds. Obrony (*ang. Defense Science Board*) przedstawiała alarmującą ocenę obecnych słabych punktów amerykańskiej infrastruktury krytycznej oraz systemów informatycznych, które wspierają działania i aktywa niezbędne do realizacji misji w sektorze publicznym i prywatnym.

> *"... Grupa zadaniowa zauważa, że cyberzagrożenia dla amerykańskiej infrastruktury krytycznej przewyższają wysiłki na rzecz ograniczenia wszechobecnych słabych punktów, tak, że przynajmniej przez następne dziesięć lat Stany Zjednoczone muszą się opierać w znacznym stopniu na środkach zapobiegawczych, aby stawić czoła cyberzagrożeniu stwarzanemu przez najbardziej zdolnych amerykańskich przeciwników. Oczywiste jest, że pilnie potrzebne jest bardziej proaktywne i systematyczne podejście do amerykańskiego odstraszania w cyberprzestrzeni...".*

Stawiając to jako przykład, należy stwierdzić, że istnieje pilna potrzeba dalszego wzmacniania podstawowych systemów informatycznych, komponentów i usług systemowych, od których obywatel jest zależny w każdym sektorze infrastruktury krytycznej - zapewnienia, że te systemy, komponenty i usługi są wystarczająco wiarygodne i zapewniają niezbędną odporność, aby wspierać interesy gospodarcze i interesy bezpieczeństwa narodowego. Niniejsza aktualizacja publikacji NSC 800-53 stanowi odpowiedź na wyzwanie, jakie stawia przed cyberbezpieczeństwem aktualny rynek, podejmując proaktywne i systemowe podejście do opracowania i udostępnienia szerokiej bazie organizacji sektora publicznego i prywatnego kompleksowego zestawu środków zabezpieczających dla wszystkich rodzajów platform obliczeniowych, w tym systemów obliczeniowych ogólnego przeznaczenia, systemów cyberfizycznych, systemów opartych na chmurach obliczeniowych, urządzeń

[7] Wykaz publikacji prezentowanych w nawiasach kwadratowych [] przestawiony jest w rozdziale *Referencje.*

przenośnych, urządzeń Internetu rzeczy (IoT), systemów uzbrojenia, systemów powietrznych, systemów łączności, systemów zabezpieczeń środowiska, superkomputerów i zabezpieczeń systemów przemysłowych. Te zabezpieczenia obejmują wdrożenie środków bezpieczeństwa i ochrony prywatności w celu ochrony krytycznych i istotnych operacji i aktywów organizacji oraz prywatności osób fizycznych. Celem jest uczynienie systemów informatycznych, od których jesteśmy zależni, bardziej odpornymi na penetrację, ograniczenie szkód spowodowanych atakami w momencie ich wystąpienia, uczynienie systemów odpornymi na działanie cyberprzestrzeni i zdolnymi do przetrwania oraz ochrona prywatności osób fizycznych.

Publikacja ta stanowi wieloletni wysiłek mający na celu opracowanie nowej generacji środków bezpieczeństwa i ochrony prywatności, które będą konieczne do osiągnięcia powyższych celów. Obejmuje ona zmiany mające na celu zwiększenie użyteczności zabezpieczeń przez różne grupy konsumentów (np. przedsiębiorstwa realizujące misje i funkcje biznesowe; organizacje inżynieryjne opracowujące systemy informatyczne, urządzenia IoT i system systemów (*ang. system-of-systems);* oraz partnerów przemysłowych budujących komponenty, produkty i usługi systemowe). Do najistotniejszych zmian w tej publikacji należą:

- Uzależnienie zabezpieczeń od wyników poprzez usunięcie z oświadczenia o zabezpieczeniu podmiotu odpowiedzialnego za spełnienie zabezpieczeń (np. systemu informatycznego, organizacji);
- Integracja środków bezpieczeństwa i ochrony prywatności informacji w jednolity, skonsolidowany katalog zabezpieczeń systemów i organizacji informatycznych;
- Stworzenie nowego katalogu zabezpieczeń zarządzania ryzykiem w łańcuchu dostaw;
- Wydzielenie ze środków bezpieczeństwa *procesów* selekcji zabezpieczeń, co pozwala na korzystanie z nich przez różne grupy zainteresowanych, w tym inżynierów systemów, architektów bezpieczeństwa, programistów, architektów korporacyjnych, inżynierów bezpieczeństwa systemów i ochrony prywatności oraz właścicieli misji lub firm;

- Wydzielenie z publikacji NSC 800-53 wer. 2 zabezpieczeń bazowych oraz wskazówek dotyczących dostosowywania i przeniesienie ich do standardu NSC 800-53B, *Zabezpieczenia bazowe systemów informatycznych oraz organizacji;*
- Wyjaśnienie związku między wymogami bezpieczeństwa i środkami bezpieczeństwa oraz związku między środkami bezpieczeństwa i ochrony prywatności; oraz
- Włączenie nowych, aktualnych środków bezpieczeństwa (np. zabezpieczeń wspierających cyberodporność, wspierających projektowanie bezpiecznych systemów oraz wzmacniających zarządzanie i rozliczalność w zakresie bezpieczeństwa i ochrony prywatności) w oparciu o najnowsze dane dotyczące zagrożeń i cyberataków.

Wyodrębniając z katalogu zabezpieczeń NSC 800-53 wer. 2 zawartość dotyczącą procesu wyboru zabezpieczeń i przenosząc zabezpieczenia bazowe (zestawy minimalnych zabezpieczeń), wyeliminowano znaczną ilość wskazówek i innych materiałów informacyjnych zawartych w NSC 800-53 wersja 1. Zawartość ta została przeniesiona do innych publikacji NSC, takich jak NSC 800-37, *Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych*; oraz NSC 800-53B. Planowane jest również udostępnienie treści zawartych w NSC 800-53A i NSC 800-53B na portalu internetowym, aby zapewnić swoim odbiorcom interaktywny, internetowy dostęp do wszystkich informacji dotyczących zabezpieczeń, stanu wyjściowego zabezpieczeń, nakładek i oceny.

Prolog

"...W procesie zarządzania ryzykiem liderzy muszą brać pod uwagę ryzyko dla interesów kraju ze strony przeciwników wykorzystujących cyberprzestrzeń na swoją korzyść oraz nasze własne wysiłki zmierzające do wykorzystania globalnego charakteru cyberprzestrzeni do osiągnięcia celów w działaniach wojskowych, wywiadowczych i biznesowych...". "

"W przypadku opracowywania planów operacyjnych należy ocenić połączenie zagrożeń, słabych punktów i skutków, aby zidentyfikować ważne tendencje i zdecydować, jakie działania należy podjąć w celu wyeliminowania lub ograniczenia zdolności do przeciwdziałania zagrożeniom, wyeliminowania lub ograniczenia słabych punktów, a także ocenić, skoordynować i zlikwidować konflikty we wszystkich operacjach w cyberprzestrzeni".

"Liderzy na wszystkich poziomach są odpowiedzialni za zapewnienie gotowości i bezpieczeństwa w takim samym stopniu, jak w każdej innej dziedzinie."

THE NATIONAL STRATEGY FOR CYBERSPACE OPERATIONS

OFFICE OF THE CHAIRMAN, JOINT CHIEFS OF STAFF, U.S. DEPARTMENT OF DEFENSE

"Sieci i technologie informacyjne przekształciły życie w XXI wieku, zmieniając sposób interakcji między ludźmi, przedsiębiorstwami i rządem. Ogromne ulepszenia w dziedzinie informatyki, przechowywania danych i komunikacji stwarzają nowe możliwości poprawy naszego dobrobytu społecznego; poprawa zdrowia i opieki zdrowotnej; wyeliminowanie barier w edukacji i zatrudnieniu; oraz zwiększenie wydajności w wielu sektorach, takich jak produkcja, transport i rolnictwo.

Obietnica tych nowych aplikacji często wynika z ich zdolności do tworzenia, gromadzenia, przekazywania, przetwarzania i archiwizowania informacji na masową skalę. Jednak ogromny wzrost ilości danych osobowych, które są gromadzone i przechowywane, w połączeniu ze zwiększoną zdolnością do ich analizy i łączenia z innymi informacjami, stwarza uzasadnione obawy dotyczące prywatności i zdolności podmiotów do zarządzania tymi bezprecedensowymi ilościami danych w sposób odpowiedzialny.

Kluczowym wyzwaniem tej ery jest zapewnienie, że rosnąca zdolność do tworzenia, przechwytywania, przechowywania i przetwarzania ogromnych ilości informacji nie zaszkodzi podstawowym wartościom kraju...".

"... Kiedy systemy przetwarzają dane osobowe, czy to poprzez zbieranie, analizowanie, generowanie, ujawnianie, zachowywanie lub wykorzystywanie w inny sposób tych informacji, mogą one wpływać na prywatność osób fizycznych. Projektanci systemów muszą brać pod uwagę osoby fizyczne, jako interesariuszy w ogólnym rozwoju projektu. Projektowanie z myślą o ochronie prywatności musi łączyć pragnienia ochrony prywatności osób fizycznych z wymaganiami i zabezpieczeniami systemu w sposób, który skutecznie łączy aspiracje z rozwojem...".

THE NATIONAL PRIVACY RESEARCH STRATEGY

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT PROGRAM

Errata

W tabeli zawarte będą zmiany wprowadzane w publikacji NSC 800-53. Aktualizacje danych mogą zawierać poprawki, wyjaśnienia lub inne drobne zmiany w publikacji, które mają charakter *redakcyjny* lub *merytoryczny*.

Data	Typ	Treść poprawki	Strona

ROZDZIAŁ PIERWSZY WPROWADZENIE

KONIECZNOŚĆ OCHRONY INFORMACJI, SYSTEMÓW, ORGANIZACJI I OSÓB FIZYCZNYCH

Nowoczesne systemy informatyczne mogą obejmować różne platformy obliczeniowe (np. przemysłowe systemy zabezpieczeń, systemy obliczeniowe ogólnego przeznaczenia, systemy cyberfizyczne, superkomputery, systemy uzbrojenia, systemy łączności, systemy zabezpieczeń środowiska, urządzenia medyczne, urządzenia wbudowane, czujniki i urządzenia przenośne, takie jak smartfony i tablety). Wszystkie te platformy mają wspólny fundament - komputery ze złożonym sprzętem, aplikacjami i oprogramowaniem układowym zapewniającym możliwości, które wspierają podstawową misję i funkcje biznesowe organizacji.

Środki bezpieczeństwa to zabezpieczenia lub środki zaradcze stosowane w ramach systemu lub organizacji w celu ochrony poufności, integralności i dostępności systemu i jego informacji oraz w celu zarządzania ryzykiem bezpieczeństwa informacji.[8] Środki ochrony prywatności to administracyjne, techniczne i fizyczne zabezpieczenia stosowane w systemie lub organizacji w celu zarządzania ryzykiem związanym z ochroną prywatności i zapewnienia zgodności z obowiązującymi wymogami w zakresie ochrony prywatności.[9] Środki bezpieczeństwa i ochrony prywatności wybierane są i wdrażane w celu spełnienia wymogów bezpieczeństwa i ochrony prywatności nakładanych na system lub organizację. Wymagania dotyczące bezpieczeństwa i ochrony prywatności wynikają z obowiązujących przepisów prawa, rozporządzeń, dyrektyw, regulacji, zasad, standardów i misji, które mają na celu zapewnienie poufności, integralności i dostępności informacji przetwarzanych, przechowywanych lub przesyłanych oraz zarządzanie ryzykiem dla indywidualnej prywatności.

[8] Oba terminy "*bezpieczeństwo informacji*" i "*bezpieczeństwo*" są w niniejszej publikacji używane synonimicznie.

[9] Zgodnie z ustawą o ochronie danych osobowych.

Wybór, opracowanie i wdrożenie środków bezpieczeństwa i ochrony prywatności[10] są ważnymi zadaniami, które mają istotny wpływ na działania[11] i majątek organizacji, a także dobrobyt jednostek i narodu. Organizacje powinny odpowiedzieć na kilka kluczowych pytań dotyczących bezpieczeństwa informacji i ochrony prywatności:

- Jakie środki bezpieczeństwa i ochrony prywatności są potrzebne, aby spełnić wymogi bezpieczeństwa i ochrony prywatności oraz odpowiednio zarządzać ryzykiem związanym z misją/przedsiębiorstwem lub ryzykiem odnoszącym się do osób fizycznych?
- Czy wybrane zabezpieczenia zostały wdrożone lub czy istnieje plan ich implementacji?
- Jaki jest wymagany poziom wiarygodności (tzn. podstawy zaufania), że wybrane zabezpieczenia, tak jak zostały zaprojektowane i wdrożone, są skuteczne?[12]

Odpowiedzi na te pytania nie są udzielane w odosobnieniu, ale raczej w kontekście procesu zarządzania ryzykiem organizacji, która na bieżąco identyfikuje, ocenia, reaguje i monitoruje zagrożenia bezpieczeństwa i ochrony prywatności wynikające z przetwarzanych informacji oraz posiadanych systemów.[13] Środki bezpieczeństwa i ochrony prywatności w niniejszej publikacji, zalecane są do stosowania przez organizacje w celu spełnienia ich wymagań dotyczących bezpieczeństwa i ochrony prywatności informacji. Katalog środków bezpieczeństwa może być postrzegany, jako zestaw narzędzi zawierający zbiór zabezpieczeń, mechanizmów zaradczych, technik i procesów służących do reagowania na zagrożenia bezpieczeństwa i ochrony prywatności. Zabezpieczenia są stosowane, jako część ściśle zdefiniowanego procesu zarządzania ryzykiem, który wspiera organizacyjne programy bezpieczeństwa i ochrony prywatności informacji. Z kolei te programy bezpieczeństwa

[10] Środki bezpieczeństwa i ochrony prywatności zapewniają zabezpieczenia i środki zaradcze w procesach inżynierii bezpieczeństwa systemów i prywatności w celu zmniejszenia ryzyka w trakcie cyklu życia systemu.

[11] Działania organizacyjne obejmują misję, funkcje, wizerunek i reputację.

[12] Skuteczność środków bezpieczeństwa i ochrony prywatności odnosi się do zakresu, w jakim zabezpieczenia są prawidłowo wdrażane, działają zgodnie z założeniami i przynoszą pożądane rezultaty w odniesieniu do spełnienia wyznaczonych wymogów bezpieczeństwa i ochrony prywatności [NSC 800-53A].

[13] Ramowy system zarządzania ryzykiem opisany w NSC 800-37, jest przykładem kompleksowego procesu zarządzania ryzykiem.

informacji i ochrony prywatności stanowią podstawę sukcesu misji i funkcji biznesowych organizacji.

Ważne jest, aby odpowiedzialne osoby w organizacji rozumieli zagrożenia bezpieczeństwa i ochrony prywatności, które mogą mieć negatywny wpływ na działalność organizacji i jej aktywa, osoby prywatne, inne organizacje i Państwo.[14] Personel ten powinien również rozumieć aktualny stan programów bezpieczeństwa i ochrony prywatności oraz zabezpieczenia planowane lub stosowane w celu ochrony informacji, systemów informatycznych oraz organizacji, w celu dokonywania świadomych decyzji i inwestycji, które odpowiadają na zidentyfikowane zagrożenia w akceptowalny sposób. Celem jest zarządzanie tymi zagrożeniami poprzez wybór i wdrożenie środków bezpieczeństwa I ochrony prywatności.

1.1. CEL I ZASTOSOWANIE

Niniejsza publikacja ustanawia zabezpieczenia systemów i organizacji. Zabezpieczenia te mogą być wdrożone w każdej organizacji lub systemie przetwarzającym informacje. Stosowanie tych środków bezpieczeństwa jest obowiązkowe w przypadku krajowego systemu cyberbezpieczeństwa i wymaga wdrożenia, co najmniej minimalnych mechanizmów zabezpieczeń.[15] Niniejszy standard, wraz z innymi wspierającymi publikacjami, ma na celu pomóc organizacjom w określeniu środków bezpieczeństwa i ochrony prywatności niezbędnych do zarządzania ryzykiem oraz w spełnieniu wymogów bezpieczeństwa i ochrony prywatności zawartych m.in. w ustawie o ochronie danych osobowych oraz wydanych Narodowych Standardach Cyberbezpieczeństwa (NSC). Cel ten jest osiągany poprzez zapewnienie kompleksowego i elastycznego katalogu środków bezpieczeństwa i ochrony prywatności w celu zaspokojenia obecnych i przyszłych potrzeb ochrony w oparciu o zmieniające się zagrożenia, słabe punkty, wymagania i technologie. Publikacja poprawia

[14] Obejmuje to ryzyko dla infrastruktury krytycznej i kluczowych zasobów.

[15] Organizacje publiczne, jak również organizacje sektora prywatnego, są zachęcane do rozważenia zastosowania tych wytycznych w stosownych przypadkach. Patrz NSC 800-53B, aby zapoznać się z zabezpieczeniami bazowymi.

również komunikację między organizacjami poprzez zapewnienie wspólnego leksykonu, który wspiera dyskusję na temat bezpieczeństwa, prywatności i koncepcji zarządzania ryzykiem.

Wreszcie, zabezpieczenia te są niezależne od przebiegu samego procesu ich wyboru. Proces selekcji zabezpieczeń może być częścią procesu zarządzania ryzykiem w całej organizacji, procesu inżynierii systemów [NIST SP 800-160],[16] ram zarządzania ryzykiem [NIST SP 800-37], ram cyberbezpieczeństwa infrastruktury krytycznej [NIST CSF] lub ram ochrony prywatności [NIST PF].[17] Kryteria wyboru zabezpieczeń mogą opierać się na wielu czynnikach, w tym misjach i potrzebach biznesowych, potrzebach w zakresie ochrony interesariuszy, zagrożeniach, słabych punktach i wymaganiach dotyczących zgodności z przepisami, rozporządzeniami, dyrektywami, regulacjami, zasadami, standardami i wytycznymi. Połączenie katalogu środków bezpieczeństwa i ochrony prywatności z procesem wyboru zabezpieczeń opartym na analizie ryzyka może pomóc organizacjom spełnić określone wymagania w zakresie bezpieczeństwa i ochrony prywatności, uzyskać odpowiednie bezpieczeństwo systemów informatycznych oraz chronić prywatność jednostek.

1.2. DOCELOWI ODBIORCY

Niniejsza publikacja ma na celu służyć zróżnicowanej publiczności. Powinni z niej korzystać wszyscy zainteresowani sprawami bezpieczeństwa informacji, w szczególności:

- Osoby odpowiedzialne za system, bezpieczeństwo informacji, ochronę prywatności lub zarządzanie ryzykiem i nadzór, w tym *AO, CIO, SAISO, SAOP*;[18]

[16] Zarządzanie ryzykiem jest integralną częścią inżynierii systemów, inżynierii bezpieczeństwa systemów i inżynierii ochrony prywatności.

[17] [OMB A-130] wymaga od agencji federalnych wdrożenia NIST Risk Management Framework w celu wyboru zabezpieczeń dla federalnych systemów informacyjnych. [EO 13800] wymaga od agencji federalnych wdrożenia NIST Framework for Improving Critical Infrastructure Cybersecurity w celu zarządzania ryzykiem cyberbezpieczeństwa. Ramy NIST są również dostępne dla organizacji niefederalnych, jako zasoby opcjonalne.

[18] Patrz: NSC 800-37; NSC 7298.

- Osoby odpowiedzialne za rozwój systemów, w tym właściciele misji, kierownicy programów, inżynierowie systemów, inżynierowie bezpieczeństwa systemów, inżynierowie ochrony prywatności, twórcy sprzętu i oprogramowania, integratorzy systemów oraz personel zajmujący się zakupami lub zamówieniami;
- Osoby odpowiedzialne za logistykę lub dystrybucję, w tym kierownicy programów, personel ds. zaopatrzenia, integratorzy systemów i zarządcy nieruchomości;
- Osoby odpowiedzialne za bezpieczeństwo i ochronę prywatności oraz działania operacyjne, w tym właściciele misji lub firm, właściciele systemów, właściciele lub władający informacją, administratorzy systemów, planiści ciągłości działania oraz to osoby odpowiedzialne za bezpieczeństwo oraz prywatność i ochronę danych osobowych w systemach;
- Osoby odpowiedzialne za ocenę i monitorowanie bezpieczeństwa i ochrony prywatności, w tym audytorzy, osoby oceniające system, osoby oceniające zabezpieczenia, niezależni weryfikatorzy, walidatorzy i analitycy; oraz
- Podmioty komercyjne (w tym partnerzy przemysłowi) wytwarzające produkty i systemy składowe, tworzące technologie bezpieczeństwa i ochrony prywatności lub świadczące usługi lub oferujące możliwości wspierające bezpieczeństwo lub prywatność informacji.

1.3. OBOWIĄZKI ORGANIZACYJNE

Zarządzanie zagrożeniami bezpieczeństwa i ochrony prywatności jest złożonym, wieloaspektowym przedsięwzięciem, które wymaga:

- Zdefiniowania adekwatnych wymagań dotyczących bezpieczeństwa i ochrony prywatności systemów i organizacji;
- Zastosowania godnych zaufania komponentów systemu informatycznego opartych na najnowocześniejszym sprzęcie, oprogramowaniu sprzętowym oraz procesach tworzenia i pozyskiwania oprogramowania;
- Rygorystycznego planowania bezpieczeństwa i ochrony prywatności oraz zarządzania cyklem życia systemu;

- Zastosowania zasad i praktyk inżynierii bezpieczeństwa systemu i prywatności w celu bezpiecznego rozwoju i integracji komponentów systemu w systemach informatycznych;
- Stosowania praktyk w zakresie bezpieczeństwa i ochrony prywatności, które są odpowiednio udokumentowane i zintegrowane z procesami instytucjonalnymi i operacyjnymi organizacji oraz wspierają je; oraz
- Ciągłego monitorowania systemów informatycznych i organizacji w celu określania bieżącej skuteczności zabezpieczeń, zmian w systemach informatycznych i środowiskach działania oraz stanu bezpieczeństwa i ochrony prywatności w całej organizacji.

Organizacje powinny w sposób ciągły oceniać zagrożenia bezpieczeństwa i ochrony prywatności operacji organizacyjnych i aktywów, osób fizycznych, innych organizacji oraz Państwa. Zagrożenia dla bezpieczeństwa i ochrony prywatności wynikają z planowania i realizacji misji organizacji i funkcji biznesowych, uruchamiania systemów informatycznych lub kontynuacji działania systemu. Realistyczna ocena ryzyka wymaga dogłębnego zrozumienia podatności na zagrożenia w oparciu o konkretne słabe punkty systemów informatycznych i organizacji oraz prawdopodobieństwo i potencjalne negatywne skutki skutecznego wykorzystania tych słabych punktów przez te zagrożenia.[19] Ocena ryzyka wymaga również zrozumienia zagrożeń dla prywatności.[20]

Wychodząc naprzeciw oczekiwaniom organizacji związanym z oceną i określaniem ryzyka, wymagania dotyczące bezpieczeństwa i ochrony prywatności są spełniane poprzez zapoznawanie się i zrozumienie strategii zarządzania ryzykiem w organizacji.[21] Strategia zarządzania ryzykiem uwzględnia koszty, harmonogram, wyniki i kwestie dotyczące łańcucha dostaw powiązane z projektowaniem, rozwojem, pozyskiwaniem, wdrażaniem, eksploatacją,

[19] [NSC 800-30] zawiera wytyczne dotyczące procesu oceny ryzyka.

[20] [IR 8062] wprowadza pojęcia zagrożenia prywatności.

[21] [NIST SP 800-39] zawiera wytyczne dotyczące procesów i strategii zarządzania ryzykiem.

utrzymaniem i utylizacją systemów organizacyjnych. Proces zarządzania ryzykiem jest następnie stosowany w celu bieżącego zarządzania ryzykiem.[22]

Katalog środków bezpieczeństwa i ochrony prywatności może być skutecznie wykorzystywany do ochrony organizacji, osób fizycznych i systemów informatycznych przed tradycyjnymi i zaawansowanymi trwałymi zagrożeniami i zagrożeniami dla prywatności wynikającymi z przetwarzania informacji umożliwiających identyfikację osoby w różnych scenariuszach operacyjnych, środowiskowych i technicznych. Zabezpieczenia te mogą być stosowane w celu wykazania zgodności z różnymi rządowymi, organizacyjnymi lub instytucjonalnymi wymogami w zakresie bezpieczeństwa i ochrony prywatności. Organizacje są odpowiedzialne za wybór odpowiednich środków bezpieczeństwa i ochrony prywatności, prawidłowe wdrożenie zabezpieczeń oraz wykazanie ich skuteczności w spełnianiu wymogów bezpieczeństwa i ochrony prywatności.[23] Środki bezpieczeństwa i ochrony prywatności mogą być również stosowane przy opracowywaniu specjalistycznych *zestawów minimalnych zabezpieczeń (zabezpieczeń bazowych)* lub *nakładek* dla unikalnych lub specjalistycznych misji lub aplikacji biznesowych, systemów informatycznych, zagrożeń, środowisk operacyjnych, technologii lub grup interesów.[24]

Oceny ryzyka organizacyjnego są częściowo wykorzystywane w procesie selekcji w zakresie bezpieczeństwa i ochrony prywatności. Rezultatem procesu selekcji jest uzgodniony zestaw środków bezpieczeństwa i ochrony prywatności uwzględniający konkretną misję lub potrzeby biznesowe zgodne z tolerancją ryzyka organizacyjnego.[25] Proces ten zachowuje, w możliwie największym stopniu, zdolność i elastyczność, których organizacje potrzebują,

---

[22] [NSC 800-37] zapewnia kompleksowy proces zarządzania ryzykiem.

[23] [NSC 800-53A] zawiera wytyczne dotyczące oceny skuteczności zabezpieczeń.

[24] [NSC 800-53B] zawiera wytyczne dotyczące dostosowania podstawowych mechanizmów zabezpieczeń (zabezpieczeń bazowych) w zakresie bezpieczeństwa i ochrony prywatności oraz opracowania nakładek w celu wsparcia konkretnych potrzeb i wymogów ochrony interesariuszy i ich organizacji.

[25] Personel zatwierdzający lub ich wyznaczeni przedstawiciele, akceptując plany bezpieczeństwa i ochrony prywatności, wyrażają zgodę na stosowanie środków bezpieczeństwa i ochrony prywatności zaproponowanych w celu spełnienia wymogów bezpieczeństwa i ochrony prywatności dla organizacji i systemów informatycznych.

aby stawić czoła coraz bardziej zaawansowanej i wrogiej przestrzeni zagrożeń, misji i wymaganiom biznesowym, szybko zmieniającym się technologiom, złożonym łańcuchom dostaw i wielu rodzajom środowisk operacyjnych.

1.4. ZWIĄZEK Z INNYMI PUBLIKACJAMI

Niniejsza publikacja określa zabezpieczenia mające na celu spełnienie różnorodnych wymagań w zakresie bezpieczeństwa i ochrony prywatności, które zostały nałożone na systemy informatyczne i organizacje, oraz są zgodne z innymi ustanowionymi krajowymi i międzynarodowymi standardami bezpieczeństwa i ochrony prywatności oraz uzupełniają je. W celu opracowania szeroko stosowanego i technicznie uzasadnionego zestawu zabezpieczeń systemów i organizacji, podczas opracowywania niniejszej publikacji wzięto pod uwagę wiele źródeł. Źródła te obejmowały wymagania i zabezpieczenia ze środowisk produkcyjnych, obronnych, finansowych, opieki zdrowotnej, transportowych, energetycznych, wywiadowczych, przemysłowych i audytorskich, a także krajowych i międzynarodowych organizacji normalizacyjnych. Tam, gdzie było to możliwe, zabezpieczenia zostały przyporządkowane do międzynarodowych standardów, aby zapewnić maksymalną użyteczność i możliwość zastosowania.[26] Związek tej publikacji z innymi publikacjami dotyczącymi bezpieczeństwa, prywatności i zarządzania ryzykiem można znaleźć w [FISMA IMP].

1.5. NOWE WESJE I ZMIANY

Opisane w niniejszej publikacji środki bezpieczeństwa i ochrony prywatności stanowią najnowocześniejsze środki ochrony osób, systemów informatycznych i organizacji. Zabezpieczenia są okresowo przeglądane i poprawiane w celu odzwierciedlenia: doświadczeń zdobytych podczas ich stosowania; nowych lub poprawionych ustaw, zarządzeń, dyrektyw, rozporządzeń, polityk i standardów; zmieniających się wymagań

[26] Tabele mapowania zabezpieczeń NIST SP 800-53, Rewizja 5 do zabezpieczeń ISO/IEC 27001 dostępne są w publikacji [NSC 800-53 MAP].

dotyczących bezpieczeństwa i ochrony prywatności; pojawiających się zagrożeń, słabych punktów, metod ataków i przetwarzania informacji; oraz dostępności nowych technologii.

Oczekuje się również, że środki bezpieczeństwa i ochrony prywatności zawarte w katalogu zabezpieczeń z czasem ulegną zmianie w miarę wycofywania, zmiany i dodawania nowych zabezpieczeń. Oprócz potrzeby zmian, konieczność stabilności została uwzględniona poprzez wprowadzenie wymogu, aby proponowane zmiany w zakresie środków bezpieczeństwa i ochrony prywatności przechodziły przez rygorystyczny i przejrzysty publiczny proces przeglądu w celu uzyskania informacji zwrotnych od sektora publicznego i prywatnego oraz osiągnięcia konsensusu w sprawie takich zmian. Proces przeglądu zapewnia solidny technicznie, elastyczny i stabilny zestaw środków bezpieczeństwa i ochrony prywatności dla organizacji, które korzystają z katalogu zabezpieczeń.

1.6. ORGANIZACJA PUBLIKACJI

Pozostała część tej publikacji jest zorganizowana w następujący sposób:

- **W rozdziale drugim** opisano podstawowe pojęcia związane ze środkami bezpieczeństwa i ochrony prywatności, w tym strukturę zabezpieczeń, sposób organizacji zabezpieczeń w skonsolidowanym katalogu, podejścia do wdrażania zabezpieczeń, związek między środkami bezpieczeństwa i ochrony prywatności oraz wiarygodność i zaufanie.
- **W rozdziale trzecim** znajduje się skonsolidowany katalog środków bezpieczeństwa i ochrony prywatności, w tym sekcja Omówienie wyjaśniająca cel każdego zabezpieczenia i dostarczająca użytecznych informacji dotyczących wdrażania i oceny zabezpieczeń, lista powiązanych zabezpieczeń ukazująca związki i zależności pomiędzy tymi zabezpieczeniami oraz lista odniesień do publikacji pomocniczych, które mogą być pomocne dla organizacji.

- **Referencje**, **Słownik**, **Akronimy** i **Podsumowanie dotyczące zabezpieczeń** dostarczają dodatkowych informacji na temat korzystania ze środków bezpieczeństwa i ochrony prywatności.[27]

[27] O ile nie podano inaczej, wszystkie odniesienia do publikacji NSC odnoszą się do najnowszej wersji tej publikacji.

ROZDZIAŁ DRUGI PODSTAWY

STRUKTURA, RODZAJ I ORGANIZACJA ŚRODKÓW BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

W niniejszym rozdziale przedstawiono podstawowe pojęcia związane ze środkami bezpieczeństwa i ochrony prywatności, w tym związek między wymaganiami, a zabezpieczeniami, strukturę zabezpieczeń, sposób organizacji zabezpieczeń w skonsolidowanym katalogu środków bezpieczeństwa, różne podejścia do wdrażania zabezpieczeń w systemach informatycznych i organizacjach, związek między środkami bezpieczeństwa i ochrony prywatności, znaczenie koncepcji wiarygodności i gwarancji środków bezpieczeństwa i ochrony prywatności oraz wpływ zabezpieczeń na tworzenie wiarygodnych, bezpiecznych i odpornych systemów.

2.1. WYMAGANIA I ZABEZPIECZENIA

Ważne jest, aby zrozumieć związek pomiędzy wymaganiami, a zabezpieczeniami. W przypadku polityki bezpieczeństwa informacji i ochrony prywatności, termin "*wymóg*" jest zwykle używany w odniesieniu do zapewnienia bezpieczeństwa informacji i nałożonych na organizacje obowiązków w zakresie ochrony prywatności. Termin "*wymóg*" może być również używany w szerszym znaczeniu w odniesieniu do wyrażania potrzeb w zakresie ochrony interesariuszy danego systemu lub organizacji.

Potrzeby w zakresie ochrony interesariuszy i odpowiadające im wymagania dotyczące bezpieczeństwa i ochrony prywatności mogą pochodzić z wielu źródeł (np. z przepisów prawa, rozporządzeń, dyrektyw, regulacji, polityk, standardów, misji i potrzeb biznesowych lub oceny ryzyka). Termin "*wymóg*", używany w niniejszych wytycznych, obejmuje zarówno wymogi prawne, jak i zasady (reguły), a także stanowi wyraz szerszego zestawu potrzeb w zakresie ochrony interesariuszy, które mogą pochodzić z innych źródeł.

Wszystkie te wymagania, gdy są stosowane w systemie, pomagają określić niezbędne cechy systemu - obejmujące bezpieczeństwo, prywatność i wiarygodność.[28]

Organizacje mogą podzielić wymagania dotyczące bezpieczeństwa i ochrony prywatności na bardziej szczegółowe kategorie, w zależności od tego, w którym momencie cyklu życia systemu (*ang. System Development Life Cycle - SDLC*) wymagania te są stosowane i w jakim celu. Organizacje mogą używać terminu "*wymagania dotyczące zdolności*" do opisania zdolności, którą system lub organizacja musi zapewnić, aby zaspokoić potrzebę ochrony interesariuszy. Ponadto organizacje mogą odnosić się do wymagań systemowych, które odnoszą się do konkretnego sprzętu, oprogramowania i elementów firmware'u systemu, jako do *wymagań specyfikacji,* czyli do zdolności, które realizują całość lub część zabezpieczeń i które mogą być oceniane (tj. jako część procesów weryfikacji, testowania, zatwierdzania i oceny). Wreszcie, organizacje mogą używać terminu "*wymagania dotyczące specyfikacji pracy*" *w* odniesieniu do działań, które muszą być wykonywane operacyjnie lub podczas rozwoju systemu.

Zabezpieczenia mogą być postrzegane, jako opisy środków bezpieczeństwa i możliwości ochrony właściwe dla osiągnięcia poszczególnych celów organizacji w zakresie bezpieczeństwa i ochrony prywatności oraz odzwierciedlające potrzeby ochrony interesariuszy organizacji. Zabezpieczenia są wybierane i wdrażane przez organizację w celu spełnienia wymagań systemowych. Zabezpieczenia mogą obejmować aspekty administracyjne, techniczne i fizyczne. W niektórych przypadkach, wybór i wdrożenie zabezpieczeń może wymagać od organizacji dodatkowej specyfikacji w postaci *wymagań pochodnych* lub wartości parametrów zabezpieczeń. Pochodne wymagania i wartości

[28] Cechy charakterystyczne systemu mające wpływ na bezpieczeństwo i prywatność są różne i obejmują: typ systemu i funkcję w zakresie jego podstawowego przeznaczenia; strukturę systemu w zakresie technologii, elementów mechanicznych, fizycznych i ludzkich; tryby i stany realizacji funkcji i usług przez system; krytyczność lub znaczenie systemu oraz jego funkcji i usług składowych; wrażliwość danych lub informacji przetwarzanych, przechowywanych lub przesyłanych; konsekwencje utraty, awarii lub pogorszenia w stosunku do zdolności systemu do prawidłowego działania i zapewnienia własnej ochrony (tj., ochrony osobistej); oraz wartości pieniężnej lub innej wartości [NIST SP 800-160].

parametrów zabezpieczeń mogą być niezbędne do zapewnienia odpowiedniego poziomu szczegółowości implementacji dla poszczególnych zabezpieczeń w ramach SDLC.

2.2. STRUKTURA I ORGANIZACJA ZABEZPIECZEŃ

Opisane w niniejszej publikacji środki bezpieczeństwa i ochrony prywatności mają dokładnie określoną organizację i strukturę. Dla ułatwienia stosowania w procesie wyboru i specyfikacji środków bezpieczeństwa i ochrony prywatności, zabezpieczenia są zorganizowane w 20 *kategoriach*[29]. Każda kategoria zawiera zabezpieczenia, które są związane z konkretnym tematem danej kategorii. Dwuznakowy identyfikator jednoznacznie identyfikuje każdą kategorię zabezpieczeń (np. *PS* dla bezpieczeństwa osobowego). Środki bezpieczeństwa i ochrony prywatności mogą obejmować aspekty zasad, nadzoru, zabezpieczeń, procesów ręcznych oraz zautomatyzowanych mechanizmów, które są wdrażane przez systemy lub działania poszczególnych osób. Tabela 1 zawiera wykaz kategorii środków bezpieczeństwa i ochrony prywatności oraz powiązanych z nimi identyfikatorów (ID) kategorii.

[29] Spośród 20 kategorii zabezpieczeń zawartych w NSC 800-53, siedemnaście jest zgodnych z minimalnymi wymogami bezpieczeństwa zawartymi w [NSC 200]. Kategorie Programy zarządzania (PM), Przejrzystość przetwarzania danych osobowych (PT) oraz Zarządzanie ryzykiem w łańcuchu dostaw (SR) odnoszą się do zarządzania programami, prywatności i ryzyka w łańcuchu dostaw na poziomie przedsiębiorstwa, które pojawiły się od czasu wydania [NSC 200].

TABELA 1: KATEGORIE ŚRODKÓW BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

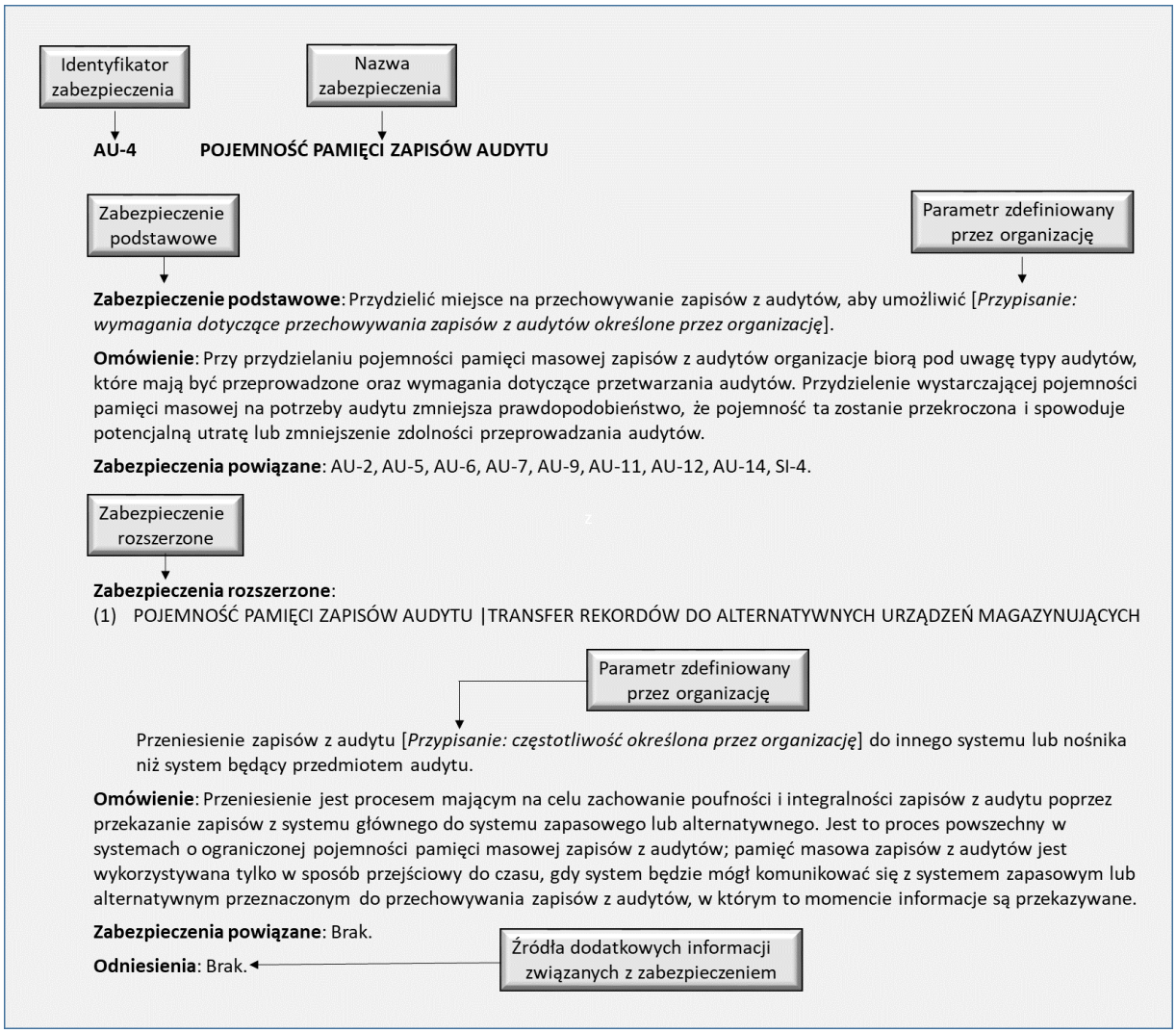
ID	KATEGORIA	ID	KATEGORIA
AC	Kontrola dostępu	**PE**	Ochrona fizyczna i środowiskowa
AT	Uświadamianie i szkolenia	**PL**	Planowanie
AU	Audyt i rozliczalność	**PM**	Programy zarządzania
CA	Ocena, autoryzacja i monitorowanie	**PS**	Bezpieczeństwo osobowe
CM	Zarządzanie konfiguracją	**PT**	Przejrzystość przetwarzanie danych osobowych
CP	Planowanie awaryjne / ciągłość działania	**RA**	Ocena ryzyka
IA	Identyfikacja i uwierzytelnianie	**SA**	Nabywanie systemu i usług
IR	Reagowanie na incydenty	**SC**	Ochrona systemów i sieci telekomunikacyjnych
MA	Utrzymanie i wsparcie	**SI**	Integralność systemu i informacji
MP	Ochrona nośników danych	**SR**	Zarządzanie ryzykiem w łańcuchu dostaw

Kategorie zabezpieczeń zawierają zabezpieczenia podstawowe i zabezpieczenia rozszerzone. Zabezpieczenia rozszerzone są bezpośrednio związane z danym zabezpieczeniem podstawowym. Zabezpieczenia rozszerzone albo zwiększają funkcjonalność lub szczegółowość zabezpieczeń podstawowych, albo zwiększają skuteczność zabezpieczenia podstawowego. Zabezpieczenia rozszerzone są stosowane w systemach i środowiskach

pracy, które wymagają większej ochrony niż zapewniana przez zabezpieczenia podstawowe. Potrzeba wybrania i wdrożenia zabezpieczeń rozszerzonych jest spowodowana potencjalnym niekorzystnym wpływem na organizacje lub osoby fizyczne lub gdy organizacja wymaga uzupełnienia podstawowych zabezpieczeń lub zapewnienia wiarygodności w oparciu o ocenę ryzyka. Wybór i wdrożenie zabezpieczeń rozszerzonych *zawsze* wymaga wyboru i wdrożenia zabezpieczenia podstawowego.

Kategorie są ułożone w porządku alfabetycznym, podczas gdy zabezpieczenia oraz zabezpieczenia rozszerzone w każdej kategorii są ułożone w porządku numerycznym. Kolejność kategorii, zabezpieczeń podstawowych i zabezpieczeń rozszerzonych *nie* oznacza żadnego logicznego postępu, poziomu priorytetu lub znaczenia, ani też kolejności, w jakiej zabezpieczenia lub zabezpieczenia rozszerzone mają zostać wdrożone. Odzwierciedla ona kolejność, w jakiej zostały one włączone do katalogu. Oznaczenia zabezpieczeń nie są ponownie wykorzystywane, gdy dane zabezpieczenie jest wycofywane z użycia.

Środki bezpieczeństwa i ochrony prywatności mają następującą strukturę: sekcja *Zabezpieczenie podstawowe*, sekcja *Omówienie*, sekcja *Zabezpieczenia powiązane*, sekcja *Zabezpieczenia rozszerzone* oraz sekcja *Odniesienia.* Rysunek 1 ilustruje strukturę typowego zabezpieczenia.



Rysunek 1. Struktura typowego zabezpieczenia.

W części dotyczącej zabezpieczeń przewidziano możliwość wdrożenia zabezpieczeń lub ochrony prywatności. Zdolności w zakresie bezpieczeństwa i ochrony prywatności są osiągane poprzez działania lub czynności, zautomatyzowane lub niezautomatyzowane, przeprowadzane przez systemy informatyczne i organizacje. Organizacje określają odpowiedzialność za opracowanie, wdrożenie, ocenę i monitorowanie zabezpieczeń. Organizacje mają możliwość elastycznego wdrażania wybranych zabezpieczeń w sposób, który spełnia misję organizacji lub potrzeby biznesowe zgodne z prawem, przepisami i zasadami.

W sekcji *Omówienie* znajdują się dodatkowe informacje na temat zabezpieczeń. Organizacje mogą wykorzystywać te informacje w razie potrzeby podczas opracowywania, dostosowywania, wdrażania, oceny lub monitorowania zabezpieczeń. Informacje te dostarczają ważnych informacji na temat wdrażania zabezpieczeń w oparciu o misję lub wymagania biznesowe, środowisko operacyjne lub ocenę ryzyka. Dodatkowe informacje mogą również wyjaśniać cel zabezpieczeń i często zawierają przykłady. Zabezpieczenia rozszerzone mogą dodatkowo obejmować oddzielną sekcję *Omówienie* w przypadku, gdy informacje w zawarte w tej sekcji mają zastosowanie jedynie do konkretnego zabezpieczenia rozszerzonego.

Sekcja *Zabezpieczenia powiązane* zawiera listę zabezpieczeń z katalogu zabezpieczeń, które mają wpływ lub wspierają wdrożenie określonego zabezpieczenia podstawowego lub zabezpieczenia rozszerzonego, odnoszą się do *zabezpieczenia powiązanego* lub możliwości ochrony prywatności, lub są wymienione w sekcji *Omówienie*. Zabezpieczenia rozszerzone są nieodłącznie związane z powiązanym z nimi zabezpieczeniem podstawowym. W związku z tym zabezpieczenia powiązane, do których odnosi się zabezpieczenie podstawowe, nie są powtarzane w ramach zabezpieczeń rozszerzonych. Mogą jednak istnieć powiązane mechanizmy bezpieczeństwa zidentyfikowane w odniesieniu do zabezpieczeń rozszerzonych, które nie są wymienione w zabezpieczeniu podstawowym (tj. zabezpieczenie powiązane jest związane jedynie z określonym zabezpieczeniem rozszerzonym). Zabezpieczenia mogą być również powiązane z zabezpieczeniami rozszerzonymi innych zabezpieczeń podstawowych. Jeżeli zabezpieczenie jest oznaczone jako powiązane, to odpowiednie oznaczenie jest dokonywane przy tym zabezpieczeniu w jego źródłowej lokalizacji w katalogu w celu zilustrowania dwukierunkowego związku. Dodatkowo, każde zabezpieczenie w danej kategorii jest nieodłącznie związane z zabezpieczeniem oznaczonym cyfrą -1 (Polityka i Procedury) w tej samej kategorii zabezpieczeń (np. AC-1, AU-1, IR-1, itd.). Dlatego związek pomiędzy zabezpieczeniem -1 i innymi zabezpieczeniami w tej samej kategorii nie jest określony w sekcji dotyczącej *zabezpieczeń powiązanych* dla każdego zabezpieczenia.

W sekcji *Zabezpieczenia rozszerzone* znajdują się informacje na temat bezpieczeństwa i możliwości ochrony prywatności, które zwiększają zabezpieczenie podstawowe.

Zabezpieczenia rozszerzone są kolejno ponumerowane w ramach każdego zabezpieczenia, tak, aby można je było łatwo zidentyfikować, gdy zostaną wybrane, jako uzupełnienie zabezpieczenia podstawowego. Każde zabezpieczenie rozszerzone ma krótki podtytuł wskazujący na zamierzoną funkcję lub możliwość zapewnianą przez to zabezpieczenie rozszerzenie. W przykładzie AU-4, jeżeli wybrano zabezpieczenie rozszerzone nr 1, oznaczenie tego zabezpieczenia to AU-4(1). Numeryczne oznaczenie zabezpieczenia rozszerzonego jest używane tylko do identyfikacji tego rozszerzenia w obrębie zabezpieczenia. Oznaczenie nie wskazuje na siłę wzmocnienia wnoszoną przez zabezpieczenie rozszerzone, poziom ochrony, priorytet, stopień ważności lub jakikolwiek hierarchiczny związek pomiędzy zabezpieczeniami rozszerzonymi. Zabezpieczenia rozszerzone nie są przeznaczone do samodzielnego wyboru. Oznacza to, że jeżeli wybrane jest zabezpieczenie rozszerzone to zostanie również wybrane i zaimplementowane odpowiednie zabezpieczenie podstawowe.

W częściach *Odniesienia* znajduje się lista obowiązujących przepisów, zasad, standardów, wytycznych, stron internetowych i innych przydatnych odniesień, które są istotne dla konkretnego zabezpieczenia podstawowego lub zabezpieczenia rozszerzonego.[30] Sekcja ta zawiera również hiperłącza do publikacji w celu uzyskania dodatkowych informacji dotyczących rozwoju, wdrażania, oceny i monitorowania zabezpieczeń.

W przypadku niektórych zabezpieczeń, dodatkowa elastyczność jest zapewniona poprzez umożliwienie organizacjom definiowania specyficznych wartości dla wyznaczonych parametrów związanych z zabezpieczeniami. Elastyczność jest osiągana w ramach procesu dopasowywania za pomocą operacji: *przypisywanie* i *wybór*, wbudowanych w opis zabezpieczenia i zamkniętych w nawiasach klamrowych. Operacje *przypisywania* i *wyboru* dają organizacjom możliwość dostosowywania zabezpieczeń w oparciu o wymagania bezpieczeństwa i ochrony prywatności organizacji. W przeciwieństwie do operacji *przypisywania*, które pozwalają na pełną elastyczność w wyznaczaniu wartości parametrów,

[30] Referencje mają na celu pomóc organizacjom w zrozumieniu i wdrożeniu środków bezpieczeństwa i ochrony prywatności i nie są wyczerpujące ani kompletne.

operacje *wyboru* zawężają zakres potencjalnych wartości, dostarczając specyficzną listę elementów, z których organizacje dokonują wyboru.

Określenie parametrów zdefiniowanych przez organizację może pochodzić z wielu źródeł, w tym z przepisów prawa, rozporządzeń, dyrektyw, regulacji, zasad, standardów, wytycznych oraz misji lub potrzeb biznesowych. Ocena ryzyka organizacyjnego i tolerancja ryzyka są również ważnymi czynnikami przy określaniu wartości parametrów zabezpieczeń. Po określeniu przez organizację wartości dla operacji *przypisywania* i *wyboru* stają się częścią zabezpieczeń. Zdefiniowane przez organizację parametry zabezpieczeń stosowane w zabezpieczeniach podstawowych, mają również zastosowanie do zabezpieczeń rozszerzonych związanych z tymi zabezpieczeniami. Wdrożenie zabezpieczeń jest oceniane pod względem skuteczności w stosunku do przeprowadzonego badania zatwierdzającego zabezpieczenia.

Poza operacjami *przypisywania* i *wyboru* wbudowanymi w zabezpieczenie, dodatkowa elastyczność jest osiągana poprzez *iterację* i działania *udoskonalające.* Iteracja pozwala organizacjom na wielokrotne użycie zabezpieczeń o różnych wartościach przypisywania i wyboru, być może stosowanych w różnych sytuacjach lub podczas wdrażania wielu reguł (polityk). Na przykład, organizacja może mieć wiele systemów wdrażających zabezpieczenie, ale o różnych parametrach ustalonych w celu uwzględnienia różnych zagrożeń dla danego systemu i środowiska pracy. *Udoskonalenie* to proces dostarczania dodatkowych szczegółów wdrożeniowych do zabezpieczeń. *Udoskonalenie* może być również wykorzystane do zawężenia zakresu zabezpieczeń w połączeniu z iteracją, w celu objęcia wszystkich odpowiednich obszarów (np. zastosowanie różnych mechanizmów uwierzytelniania do różnych interfejsów systemowych). Połączenie operacji *przypisania* i *wyboru* oraz działań *iteracyjnych* i *udoskonalających* w przypadku zastosowania zabezpieczeń, zapewnia niezbędną elastyczność, aby umożliwić organizacjom spełnienie szerokiej bazy wymagań w zakresie bezpieczeństwa i ochrony prywatności w organizacji, misji i procesie biznesowym oraz na poziomie wdrożenia systemu.

2.3. PODEJŚCIA DO WDRAŻANIA ZABEZPIECZEŃ

W rozdziale trzecim przedstawiono trzy podejścia do wdrażania zabezpieczeń: 1) zabezpieczenie *wspólne/dziedziczone*, 2) zabezpieczenie *specyficzne systemu* (w ramach danego systemu) oraz 3) zabezpieczenie *hybrydowe*. Podejścia w zakresie wykonywania zabezpieczeń określają zakres zastosowania zabezpieczeń, wspólny rodzaj lub dziedziczenie zabezpieczeń oraz zakres rozliczalności za rozwój, wykonywanie, ocenę i autoryzację zabezpieczeń. Każde podejście do realizacji zabezpieczeń ma określony cel i ukierunkowanie, które pomagają organizacjom wybierać odpowiednie zabezpieczenia, wdrażać zabezpieczenia w sposób efektywny oraz spełniać wymogi bezpieczeństwa i ochrony prywatności. Konkretne podejście do wdrażania zabezpieczeń może przynieść korzyści kosztowe poprzez wykorzystanie możliwości w zakresie bezpieczeństwa i ochrony prywatności w wielu systemach i środowiskach działania.[31]

Wspólne zabezpieczenia to zabezpieczenia, których wdrożenie skutkuje możliwością *dziedziczenia* przez wiele systemów lub programów. Zabezpieczenie jest uznawane za dziedziczne, gdy system lub program chroniony jest przez wdrożone zabezpieczenie, ale zabezpieczenie jest rozwijane, wdrażane, oceniane, zatwierdzane i monitorowane przez wewnętrzną lub zewnętrzną jednostkę, inną niż podmiot odpowiedzialny za system lub program. Możliwości w zakresie bezpieczeństwa i ochrony prywatności zapewniane przez zabezpieczenia wspólne mogą być dziedziczone z wielu źródeł, w tym z misji lub działalności biznesowych, organizacji, enklaw, środowisk działania, witryn lub innych systemów lub programów. Wdrożenie środków bezpieczeństwa, jako wspólnych środków bezpieczeństwa, może wprowadzić ryzyko pojedynczego punktu awarii.

Wiele środków bezpieczeństwa potrzebnych do ochrony systemów informatycznych organizacji - w tym wiele środków bezpieczeństwa w zakresie ochrony fizycznej i ochrony

[31] [NSC 800-37] zawiera dodatkowe wytyczne dotyczące metod wdrażania zabezpieczeń oraz sposobu stosowania różnych metod w ramach zarządzania ryzykiem.

środowiska, środków bezpieczeństwa osobowego oraz środków bezpieczeństwa reagowania na incydenty - jest dziedzicznych i dlatego są odpowiednie do wspólnego systemu zabezpieczeń. Wspólne zabezpieczenia mogą również obejmować zabezpieczenia oparte na technologii, takie jak zabezpieczenia identyfikacji i uwierzytelniania, zabezpieczenia ochrony granic systemu, zabezpieczenia audytu i rozliczalności oraz zabezpieczenia dostępu. Koszty opracowania, wdrożenia, oceny, zatwierdzenia i monitorowania mogą być amortyzowane w ramach wielu systemów, elementów organizacyjnych i programów przy zastosowaniu wspólnego podejścia do wdrażania zabezpieczeń.

Zabezpieczenia niewdrożone jako zabezpieczenia wspólne, są wdrażane jako zabezpieczenia *specyficzne dla systemu* lub zabezpieczenia *hybrydowe*. Implementacja zabezpieczeń specyficznych dla systemu jest podstawowym obowiązkiem właściciela systemu i osoby autoryzującej dany system. Wdrażanie mechanizmów zabezpieczeń specyficznych dla danego systemu może wprowadzać ryzyko, jeżeli implementacje mechanizmów zabezpieczeń nie są interoperacyjne ze wspólnymi mechanizmami zabezpieczeń. Organizacje mogą wdrożyć zabezpieczenie jako *hybrydowe*, jeżeli jedna część zabezpieczeń jest wspólna (dziedziczna), a druga część jest specyficzna dla danego systemu. Na przykład, organizacja może wdrożyć zabezpieczenie CP-2 przy użyciu predefiniowanego szablonu planu awaryjnego dla wszystkich indywidualnych systemów informatycznych organizacji, dostosowując plan do zastosowań specyficznych dla systemu, tam gdzie jest to właściwe. Podział zabezpieczeń hybrydowych na część wspólną (dziedziczną) i część specyficzną dla systemu może różnić się dla danej organizacji, w zależności od rodzaju zastosowanej technologii informatycznej, podejścia stosowanego przez organizację do zarządzania zabezpieczeniami i przydziału obowiązków. W przypadku, gdy zabezpieczenie jest realizowane jako zabezpieczenie hybrydowe, dostawca zabezpieczeń wspólnych jest odpowiedzialny za zapewnienie realizacji, oceny i monitorowania *wspólnej części zabezpieczeń hybrydowych,* a właściciel systemu jest odpowiedzialny za zapewnienie realizacji, oceny i monitorowania części zabezpieczeń hybrydowych odnoszących się do *specyficznego systemu*. Zabezpieczenia zaimplementowane jako zabezpieczenia hybrydowe,

mogą wprowadzać ryzyko, jeżeli odpowiedzialność za wykonanie i bieżące zarządzanie wspólną i specyficzną dla systemu częścią zabezpieczeń nie jest jednoznacznie zdefiniowana.

Określenie właściwego podejścia do realizacji zabezpieczeń (tj. wspólnych, hybrydowych lub specyficznych dla danego systemu) jest uzależnione od sytuacji. Podejścia do realizacji zabezpieczeń nie można określić jako wspólnego, hybrydowego lub specyficznego dla danego systemu jedynie w oparciu o opis zabezpieczeń. Określenie podejścia do realizacji zabezpieczeń może prowadzić do znacznych oszczędności w organizacji w zakresie kosztów realizacji i oceny oraz bardziej spójnego stosowania zabezpieczeń w całej organizacji. Zazwyczaj identyfikacja metody implementacji zabezpieczeń jest prosta. Jednakże, wdrożenie wymaga odpowiedniego planowania i koordynacji.

Planowanie podejścia wdrożeniowego zabezpieczeń (tj. wspólne, hybrydowe lub specyficzne dla systemu) najlepiej jest przeprowadzać na wczesnym etapie cyklu życia systemu i koordynować je z podmiotami zapewniającymi zabezpieczenia [NSC 800-37]. Podobnie, jeśli zabezpieczenie ma być dziedziczne, wymagana jest koordynacja z podmiotem dokonującym podziału obowiązków, aby zapewnić, że zabezpieczenie spełnia jego potrzeby. Jest to szczególnie ważne ze względu na charakter parametrów zabezpieczeń. Jednostka dziedzicząca nie może zakładać, że zabezpieczenia są takie same i ograniczają odpowiednie ryzyka dla systemu tylko dlatego, że identyfikatory zabezpieczeń (np. AC-1) są takie same. Istotne jest zbadanie parametrów zabezpieczeń (np. operacji przydzielania lub wyboru) przy określaniu, czy zabezpieczenie wspólna jest odpowiednie do ograniczenia ryzyka specyficznego dla systemu.

2.4. ŚRODKI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Wybór i wdrożenie środków bezpieczeństwa i ochrony prywatności odzwierciedlają cele programów bezpieczeństwa informacji i prywatności oraz sposób, w jaki programy te zarządzają własnym ryzykiem. W zależności od okoliczności, te cele i zagrożenia mogą być niezależne lub nakładać się na siebie. Programy bezpieczeństwa informacji są odpowiedzialne za ochronę informacji i systemów informatycznych przed nieautoryzowanym dostępem, użyciem, ujawnieniem, zakłóceniem, modyfikacją lub zniszczeniem (tzn.

nieautoryzowaną działalnością lub nieprawidłowym zachowaniem systemu) w celu zapewnienia poufności, integralności i dostępności. Programy te są również odpowiedzialne za zarządzanie ryzykiem bezpieczeństwa i zapewnienie zgodności z obowiązującymi wymogami bezpieczeństwa. Programy ochrony prywatności są odpowiedzialne za zarządzanie ryzykiem osób fizycznych związanym z tworzeniem, gromadzeniem, wykorzystywaniem, przetwarzaniem, przechowywaniem, utrzymaniem, rozpowszechnianiem, ujawnianiem lub usuwaniem (zwanych łącznie *przetwarzaniem*) danych osobowych oraz za zapewnienie zgodności z obowiązującymi wymogami ochrony prywatności.[32] W przypadku, gdy system przetwarza dane osobowe, program bezpieczeństwa informacji i program ochrony prywatności są współodpowiedzialne za zarządzanie zagrożeniami dla bezpieczeństwa tych danych. Ze względu na nakładanie się na siebie obowiązków, zabezpieczenia, które organizacje wybierają do zarządzania tymi zagrożeniami bezpieczeństwa, będą zasadniczo takie same, niezależnie od tego, czy zostaną określone, jako środki bezpieczeństwa lub ochrony prywatności w zestawie minimalnych zabezpieczeń, czy w planach programu lub systemu.

Mogą również wystąpić okoliczności, w których wybór i/lub wdrożenie zabezpieczeń lub zabezpieczeń rozszerzonych wpływa na zdolność programu do osiągnięcia jego celów i zarządzania odpowiednim ryzykiem. W części poświęconej omawianiu zabezpieczeń należy zwrócić uwagę na specyficzne aspekty bezpieczeństwa i/lub prywatności, tak aby organizacje mogły wziąć te względy pod uwagę, ponieważ określają one najbardziej efektywną metodę wdrożenia zabezpieczeń. Jednakże rozważania te nie są wyczerpujące.

Na przykład, organizacja może wybrać opcję AU-3 (Zawartość rejestrów audytu) w celu wsparcia monitorowania nieautoryzowanego dostępu do zasobów informatycznych, które

[32] Programy ochrony prywatności mogą również uwzględniać ryzyko dla osób fizycznych, które może wynikać z ich interakcji z systemami wewnętrznymi, w przypadku gdy przetwarzanie danych osobowych może mieć mniejszy wpływ niż oddziaływanie, jakie ma system, na zachowanie lub działalność osób fizycznych. Takie skutki stanowiłyby ryzyko dla indywidualnych autonomii, a organizacje mogą być zmuszone do podjęcia stosownych kroków w celu zarządzania tym ryzykiem, oprócz ryzyka związanego z bezpieczeństwem i prywatnością informacji.

nie obejmują danych osobowych. Ponieważ potencjalna utrata poufności zasobu informacyjnego nie ma wpływu na prywatność, głównym czynnikiem decydującym o wyborze zabezpieczeń są cele bezpieczeństwa. Jednak wdrożenie zabezpieczeń w odniesieniu do monitorowania nieautoryzowanego dostępu może wiązać się z przetwarzaniem danych dotyczących danych osobowych, co może spowodować zagrożenie dla prywatności i wpłynąć na cele programu ochrony prywatności. Sekcja *Omówienie* w AU-3 zawiera rozważania na temat zagrożeń dla prywatności, pozwalające organizacji uwzględnić te rozważania, ponieważ określają one najlepszy sposób wdrożenia zabezpieczeń.

Dodatkowo można wybrać zabezpieczenie rozszerzone AU-3(3) {Ograniczenie elementów danych osobowych umożliwiających identyfikację} w celu wsparcia zarządzania tymi zagrożeniami dla prywatności.

Ze względu na permutacje w relacji pomiędzy bezpieczeństwem informacji i celami programu ochrony prywatności, a zarządzaniem ryzykiem, istnieje potrzeba ścisłej współpracy pomiędzy programami w celu wybrania i wdrożenia odpowiednich zabezpieczeń systemów informatycznych przetwarzających informacje z danych osobowych. Organizacje analizują, w jak promować i sformalizować współpracę między tymi dwoma programami, aby zapewnić osiągnięcie celów obu dziedzin i odpowiednio zarządzać ryzykiem.[33]

2.5. ZAUFANIE I WIARYGODNOŚĆ

Zaufanie do systemów, ich komponentów i usług systemowych jest ważną częścią strategii zarządzania ryzykiem opracowanych przez organizacje.[34] *Zaufanie*, w tym kontekście, oznacza zdolność do spełnienia wszelkich oczekiwań, które mogą być wymagane od komponentu, podsystemu, systemu, sieci, aplikacji, misji, funkcji biznesowej, przedsiębiorstwa lub innego podmiotu.[35] Wymagania w zakresie zaufania mogą obejmować

[33] Zasoby wspierające współpracę w zakresie bezpieczeństwa informacji i programów ochrony prywatności są dostępne pod adresem https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[34] [NIST SP 800-160] zawiera wytyczne dotyczące inżynierii bezpieczeństwa systemów i stosowania zasad projektowania bezpieczeństwa w celu uzyskania wiarygodnych systemów.

[35] Patrz: [NEUM04].

atrybuty rzetelności, niezawodności, wydajności, odporności, bezpieczeństwa, ochrony, prywatności i zdolności przetrwania w szeregu potencjalnych przeciwności losu w postaci zakłóceń, zagrożeń, gróźb i ryzyka utraty prywatności. Skuteczne mierniki zaufania mają znaczenie tylko wtedy, gdy wymagania są kompletne, dobrze zdefiniowane i mogą być dokładnie ocenione.

Dwa podstawowe pojęcia, które wpływają na zaufanie do systemów, to *funkcjonalność* i *wiarygodność. Funkcjonalność* definiowana jest w kategoriach bezpieczeństwa i ochrony prywatności, funkcji, mechanizmów, usług, procedur i architektur wdrażanych w ramach systemów i programów organizacyjnych oraz środowisk, w których te systemy i programy działają. *Wiarygodność* jest miarą pewności, że funkcjonalność systemu jest wdrażana prawidłowo, działa zgodnie z założeniami i daje pożądany rezultat w odniesieniu do spełnienia wymogów bezpieczeństwa i ochrony prywatności systemu - tym samym posiada zdolność do dokładnej mediacji i egzekwowania ustanowionych polityk bezpieczeństwa i ochrony prywatności.

Ogólnie rzecz biorąc, zadanie polegające na zapewnieniu znaczącej pewności, że system prawdopodobnie zrobi to, czego się od niego oczekuje, może być wzmocnione przez techniki, które upraszczają lub zawężają analizę, na przykład poprzez zwiększenie poziomu dokładności w zakresie architektury systemu, projektowania oprogramowania, specyfikacji, rodzaju kodu i zarządzania konfiguracją. Środki bezpieczeństwa i ochrony prywatności dotyczą funkcjonalności i wiarygodności. Niektóre elementy zabezpieczeń koncentrują się przede wszystkim na funkcjonalności, podczas gdy inne na zapewnieniu wiarygodności. Niektóre zabezpieczenia mogą obsługiwać funkcjonalność i wiarygodność.

Organizacje mogą wybrać zabezpieczenia powiązane z wiarygodnością, które pozwalają zdefiniować działania związane z rozwojem systemu, wygenerować dowody dotyczące funkcjonalności i zachowania systemu oraz prześledzić ich powiązanie z elementami systemu, które zapewniają taką funkcjonalność lub wykazują takie zachowanie. Dowody te są wykorzystywane do uzyskania stopnia pewności, że system spełnia określone wymagania dotyczące bezpieczeństwa i ochrony prywatności przy jednoczesnym wspieraniu misji

i funkcji biznesowych organizacji. Zabezpieczenia powiązane z wiarygodnością są zidentyfikowane w tabelach podsumowujących zabezpieczenia w Załączniku C.

DOWÓD WPROWADZENIA ZABEZPIECZEŃ

Podczas wyboru i wdrażania zabezpieczeń, ważne jest, aby organizacje rozważyły dowody (np. artefakty, dokumentację), które będą potrzebne do wsparcia obecnych i przyszłych ocen zabezpieczeń. Takie oceny pomagają określić, czy zabezpieczenia są wdrażane prawidłowo, czy działają zgodnie z założeniami i czy spełniają wymogi polityki bezpieczeństwa i ochrony prywatności, dostarczając upoważnionym osobom istotnych informacji do podejmowania świadomych decyzji *opartych na ocenie ryzyka.*

ROZDZIAŁ TRZECI ZABEZPIECZENIA

PODSTAWOWE ŚRODKI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI ORAZ ZABEZPIECZENIA ROZSZERZONE

Niniejszy katalog środków bezpieczeństwa i ochrony prywatności zapewnia środki bezpieczeństwa systemów, organizacji i osób fizycznych. Zabezpieczenia mają na celu ułatwienie zarządzania ryzykiem i zapewnienie zgodności z obowiązującymi przepisami, rozporządzeniami wykonawczymi, dyrektywami, zasadami i normami. Z nielicznymi wyjątkami, środki bezpieczeństwa i ochrony prywatności zawarte w katalogu są neutralne pod względem zasad, technologii i branży, co oznacza, że koncentrują się na podstawowych środkach niezbędnych do ochrony informacji i prywatności osób fizycznych w całym cyklu życia informacji. Chociaż, że środki bezpieczeństwa i ochrony prywatności są w dużej mierze neutralne pod względem zasad, technologii i sektora, nie oznacza to, że zabezpieczenia te są niezależne od zasad, technologii i branży. Zrozumienie zasad, technologii i branży jest konieczne, aby zabezpieczenia były odpowiednie podczas ich wdrażania. Stosowanie katalogu zabezpieczeń neutralnych pod względem zasad, technologii i branży ma wiele zalet i zachęca on organizacje do:

- Skoncentrowania się na funkcjach i możliwościach związanych z bezpieczeństwem i ochroną prywatności, które są niezbędne do osiągnięcia misji i sukcesu biznesowego oraz do ochrony informacji i prywatności osób, niezależnie od technologii stosowanych w systemach organizacyjnych;
- Przeanalizowania każdego środka bezpieczeństwa i ochrony prywatności pod kątem możliwości zastosowania go w konkretnych technologiach, środowiskach działania, misji i funkcjach biznesowych oraz społecznościach będących przedmiotem zainteresowania; oraz
- Określania zasad bezpieczeństwa i ochrony prywatności, jako część procesu dostosowywania zabezpieczeń, które mają zmienne parametry.

W nielicznych przypadkach, w których konkretne technologie są przywoływane w zabezpieczeniach, organizacje są przestrzegane, że potrzeba zarządzania zagrożeniami dla

bezpieczeństwa i ochrony prywatności może wykraczać poza wymogi pojedynczego zabezpieczenia związanego z daną technologią. Dodatkowe potrzebne środki ochrony są uzyskiwane z innych zabezpieczeń podanych w katalogu. Narodowe Standardy Cyberbezpieczeństwa zawierają wskazówki dotyczące wyboru środków bezpieczeństwa i ochrony prywatności, które zmniejszają ryzyko dla konkretnych technologii i zastosowań sektorowych, w tym inteligentnych sieci, chmur obliczeniowych, opieki zdrowotnej, usług mobilnych, przemysłowych systemów zabezpieczeń i urządzeń Internetu rzeczy (IoT).[36] Publikacje NIST są przytaczane jako odniesienia mające zastosowanie do konkretnych zabezpieczeń zawartych w podrozdziałach 3.1 - 3.20 tej publikacji.

Ocenia się, że środki bezpieczeństwa i ochrony prywatności w katalogu z czasem ulegną zmianie w miarę wycofywania, poprawiania i dodawania nowych zabezpieczeń. Aby utrzymać stabilność planów bezpieczeństwa i ochrony prywatności, zabezpieczenia nie są przenumerowywane za każdym razem, gdy są wycofywane. Przeciwnie, oznaczenia zabezpieczeń, które zostały wycofane, są utrzymywane w katalogu zabezpieczeń dla celów historycznych. Zabezpieczenia mogą być wycofane z różnych powodów, w tym, gdy funkcja lub zdolność zapewniona przez zabezpieczenie została włączona do innego zabezpieczenia, zabezpieczenie jest redundantne do istniejącego innego zabezpieczenia lub zabezpieczenie jest uważane za już zbędne lub nieskuteczne.

Nowe zabezpieczenia są regularnie opracowywane z wykorzystaniem informacji o zagrożeniach i podatności na zagrożenia oraz informacji o taktyce, technikach i procedurach stosowanych przez przeciwników. Ponadto nowe środki bezpieczeństwa są opracowywane w oparciu o lepsze zrozumienie sposobu ograniczania zagrożeń bezpieczeństwa informacji systemów i organizacji oraz ryzyka dla prywatności osób fizycznych wynikającego z przetwarzania informacji. Wreszcie, nowe mechanizmy bezpieczeństwa są opracowywane w oparciu o nowe lub zmieniające się wymagania zawarte w prawie, zarządzeniach, regulacjach, zasadach, standardach lub wytycznych.

[36] Na przykład, [NIST SP 800-82] zawiera wytyczne dotyczące zarządzania ryzykiem i wyboru zabezpieczeń w przemysłowych systemach sterowania ICS.

Proponowane modyfikacje zabezpieczeń są dokładnie analizowane podczas każdego cyklu weryfikacji, biorąc pod uwagę potrzebę stabilności zabezpieczeń oraz potrzebę reagowania na zmieniające się technologie, zagrożenia, słabe punkty, rodzaje ataków i metody badań. Celem tych modyfikacji jest dostosowanie zmieniającego się w czasie poziomu bezpieczeństwa i ochrony prywatności informacji do potrzeb organizacji i osób fizycznych.

KATEGORIA AC – KONTROLA DOSTĘPU

AC-1 POLITYKA I PROCEDURY

Zabezpieczenie podstawowe:

Należy:

a. Opracowywanie, dokumentowanie i rozpowszechnianie w [*Realizacja: personel lub role określone przez organizację*]*:*

   1. [*Wybór (jeden lub więcej): poziom organizacji; poziom misji/procesu biznesowego; poziom systemu*] zasady kontroli dostępu, która:

      (a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami; oraz

      (b) Jest zgodna z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi; oraz

   2. Procedur ułatwiających wdrożenie zasad kontroli dostępu i powiązanych zabezpieczeń dostępu;

b. Wyznaczanie [*Realizacja: osoba wyznaczony przez organizację*] do zarządzania opracowywaniem, dokumentowaniem i upowszechnianiem polityki i procedur kontroli dostępu; oraz

c. Przeglądanie i aktualizowanie bieżącej:

   1. Polityki zabezpieczeń dostępu z [Realizacja: *częstotliwość określona przez organizację*] i następujących [*Realizacja: zdarzenia określone przez organizację*]; oraz

   2. Procedur dotyczących zabezpieczeń dostępu z [Realizacja: *częstotliwość określona przez organizację*] i następujących [*Realizacja: zdarzenia określone przez organizację*].

Omówienie: Polityka i procedury w zakresie kontroli dostępu dotyczą zabezpieczeń w kategorii *Kontrola dostępu* (AC), które są wdrażane w ramach systemów i organizacji. Strategia zarządzania ryzykiem jest ważnym czynnikiem przy tworzeniu takich polityk i procedur. Polityki i procedury przyczyniają się do zapewnienia bezpieczeństwa i ochrony prywatności. Dlatego ważne jest, aby programy bezpieczeństwa i ochrony prywatności były opracowywane wspólnie przy kształtowaniu polityki i procedur kontroli dostępu. Polityki i procedury dotyczące programów bezpieczeństwa i ochrony prywatności na poziomie organizacji są ogólnie rzecz biorąc preferowane i mogą eliminować potrzeby tworzenia polityk i procedur specyficznych dla danej misji lub systemu. Polityka może być włączona, jako część ogólnej polityki bezpieczeństwa i ochrony prywatności lub reprezentowana przez wiele polityk odzwierciedlających złożony charakter organizacji. Procedury mogą być ustanowione dla programów bezpieczeństwa i ochrony prywatności, dla misji lub procesów biznesowych oraz dla systemów, jeśli to konieczne. Procedury opisują sposób wdrażania zasad lub zabezpieczeń i mogą być skierowane do osoby lub roli, która jest przedmiotem procedury. Procedury mogą być udokumentowane w planach bezpieczeństwa i ochrony prywatności systemu w jednym lub kilku oddzielnych dokumentach.

Zdarzenia, które mogą spowodować konieczność aktualizacji polityki i procedur kontroli dostępu, obejmują wyniki oceny lub audytu, incydenty lub naruszenia bezpieczeństwa, lub zmiany w przepisach prawa, zarządzeniach, dyrektywach, rozporządzeniach, zasadach, standardach i wytycznych.

Oświadczenie o wprowadzeniu zabezpieczeń nie jest równoznaczne z ustanowieniem polityki lub procedury organizacyjnej.

Zabezpieczenia powiązane: IA-1, PM-9, PM-24, PS-8, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [NIST SP 800-12], [NIST SP 800-30], [NIST SP 800-39], [NIST SP 800-100], [IR 7874].

AC-2 ZARZĄDZANIE KONTAMI

Zabezpieczenie podstawowe:

Należy:

a. Określić i udokumentować rodzaje kont dozwolonych i szczególnie zabronionych do użytku w ramach systemu;

b. Przydzielić zarządzających systemem kont;

c. Wymagać [*Realizacja: warunki i kryteria określone przez organizację*] dotyczące przynależności do grupy i roli;

d. Ustanowić:

   1. Autoryzowanych użytkowników systemu;

   2. Przynależność do grupy i roli; oraz

   3. Uprawnienia dostępu (tj. przywileje) oraz [*Realizacja: atrybuty zdefiniowane przez organizację (w razie potrzeby)*] dla każdego konta;

e. Wymagać zatwierdzenia przez [*Realizacja: personel lub role zdefiniowane przez organizację*] wniosków o utworzenia konta;

f. Tworzyć, włączać, modyfikować, wyłączać i usuwać konta zgodnie z [*Realizacja: polityka określona przez organizację, procedury, warunki wstępne i kryteria*];

g. Monitorować korzystanie z kont;

h. Powiadomić zarządzających systemem kont i [*Realizacja: personel określony przez organizację lub role*] w okresie:

   1. [*Realizacja: okres czasu określony przez organizację*], gdy konta nie są już wymagane;

   2. [*Realizacja: okres czasu określony przez organizację*], kiedy użytkownicy zostają zwolnieni lub przeniesieni; oraz

3. [*Realizacja: zdefiniowany przez organizację okres czasu*], kiedy użycie systemu lub potrzeba wiedzy koniecznej (*ang. need-to-know*) zmienia się dla danej osoby;

i. Dokonywać autoryzacji dostępu do systemu na podstawie:

1. Ważnego upoważnienia do dostępu;
2. Zamierzonego celu użycia systemu; oraz
3. [*Realizacja: atrybuty zdefiniowane przez organizację (w razie potrzeby)*]*;*

j. Dokonywać przeglądu kont pod kątem zgodności z wymogami zarządzania kontem [*Realizacja: częstotliwość określona przez organizację*]*;*

k. Ustanowić i wdrożyć proces zmiany współdzielonych lub grupowych kont zatwierdzający uwierzytelnianie kont (jeśli zostały one wdrożone) w przypadku usunięcia osób z grupy; oraz

l. Ujednolicić procesy zarządzania kontami z procesami zwalniania i przenoszenia pracowników.

Omówienie: Przykłady typów kont systemowych obejmują konta indywidualne, współdzielone, grupowe, systemowe, gości, anonimowe, awaryjne, deweloperskie, tymczasowe i serwisowe. Identyfikacja upoważnionych użytkowników systemu oraz określenie uprawnień dostępu odzwierciedlają wymagania innych zabezpieczeń w planie bezpieczeństwa. Użytkownicy wymagający uprawnień administracyjnych na kontach systemowych są dodatkowo kontrolowani przez personel organizacyjny odpowiedzialny za zatwierdzanie takich kont i uprzywilejowany dostęp, w tym właściciela systemu, właściciela misji lub firmy, personel ds. bezpieczeństwa informacji organizacji lub inspektora ochrony danych. Rodzaje kont, których używanie organizacje mogą chcieć zakazać ze względu na zwiększone ryzyko, obejmują konta wspólne, grupowe, awaryjne, anonimowe, tymczasowe i dla gości.

W przypadku, gdy dostęp obejmuje dane osobowe, programy bezpieczeństwa współpracują z personelem zajmującym się w organizacji prywatnością (ochroną

danych osobowych) w celu ustalenia szczególnych warunków członkostwa w grupie i roli; określają autoryzowanych użytkowników, członkostwa w grupie i roli oraz uprawnienia dostępu do każdego konta; oraz tworzą, dostosowują lub usuwają konta systemowe zgodnie z zasadami organizacyjnymi. Zasady mogą zawierać takie informacje, jak data wygaśnięcia konta lub inne czynniki, które powodują wyłączenie konta. Organizacje mogą zdefiniować uprawnienia dostępu lub inne atrybuty według konta, typu konta lub kombinacji tych dwóch. Przykłady innych atrybutów wymaganych do autoryzacji dostępu obejmują ograniczenia dotyczące pory dnia, dnia tygodnia oraz miejsca pochodzenia. Definiując inne atrybuty konta systemowego, organizacje biorą pod uwagę wymagania systemowe oraz wymagania misji/biznesu. Brak uwzględnienia tych czynników może mieć wpływ na dostępność systemu.

Konta tymczasowe i awaryjne są przeznaczone do użytku krótkoterminowego. Organizacje zakładają konta tymczasowe w ramach normalnych procedur aktywacji konta, gdy istnieje potrzeba utworzenia konta krótkoterminowego bez konieczności natychmiastowej aktywacji konta. Organizacje zakładają konta awaryjne w odpowiedzi na sytuacje kryzysowe i potrzebę szybkiej aktywacji konta. W związku z tym aktywacja konta awaryjnego może ominąć normalne procesy autoryzacji konta. Kont awaryjnych i tymczasowych nie należy mylić z kontami rzadko używanymi, w tym z kontami logowania lokalnego, używanymi do zadań specjalnych lub gdy zasoby sieciowe są niedostępne (mogą być również nazywane kontami ostatniej szansy). Takie konta pozostają dostępne i nie podlegają terminom automatycznego wyłączenia lub usunięcia. Warunki wyłączania lub dezaktywacji kont obejmują przypadki, gdy nie są już wymagane konta wspólne/grupowe, awaryjne lub tymczasowe oraz gdy osoby fizyczne są przenoszone lub zwalniane. Zmiana autoryzacji udostępnionych / grupowych kont uwierzytelniających w momencie opuszczenia grupy ma na celu zapewnienie, że byli członkowie grupy nie zachowają dostępu do konta udostępnionego lub konta grupy. Niektóre rodzaje kont systemowych mogą wymagać specjalistycznego szkolenia.

Zabezpieczenia powiązane: AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-24, AU-2, AU-12, CM-5, IA-2, IA-4, IA-5, IA-8, MA-3, MA-5, PE-2, PL-4, PS-2, PS-4, PS-5, PS-7, PT-2, PT-3, SC-7, SC-12, SC-13, SC-37.

Zabezpieczenia rozszerzone:

(1) ZARZĄDZANIE KONTAMI | AUTOMATYCZNE ZARZĄDZANIE KONTEM SYSTEMU

Wsparcie zarządzania kontami systemowymi za pomocą [***Realizacja: organizacyjnie zdefiniowane mechanizmy automatyczne***]**.**

Omówienie: Zautomatyzowane zarządzanie kontami systemowymi obejmuje wykorzystanie automatycznych mechanizmów do tworzenia, włączania, modyfikowania, wyłączania i usuwania kont; powiadamianie osób zarządzających kontami o utworzeniu, włączeniu, zmodyfikowaniu, wyłączeniu lub usunięciu konta albo o zakończeniu lub przeniesieniu użytkowników; monitorowanie wykorzystania konta systemowego; oraz zgłaszanie nietypowego wykorzystania konta systemowego. Zautomatyzowane mechanizmy mogą obejmować wewnętrzne funkcje systemu oraz powiadomienia e-mail, telefoniczne i tekstowe.

Zabezpieczenia powiązane: Brak.

(2) ZARZĄDZANIE KONTAMI | AUTOMATYCZNE ZARZĄDZANIE KONTEM CZASOWYM | AWARYJNYM

Automatycznie [***Wybór: usunąć; wyłączyć***] **konta tymczasowe i awaryjne po** [***Realizacja: okres czasu określony przez organizację dla każdego typu konta***]**.**

Omówienie: Zarządzanie kontami tymczasowymi i awaryjnymi obejmuje usuwanie lub wyłączanie takich kont automatycznie po upływie wcześniej określonego czasu, a nie według uznania administratora systemu. Automatyczne usuwanie lub wyłączanie kont zapewnia bardziej spójną realizację tych czynności.

Zabezpieczenia powiązane: Brak.

(3) ZARZĄDZANIE KONTAMI | WYŁĄCZANIE KONT

Wyłączyć konta w ciągu [***Realizacja: okres czasu określony przez organizację***]**, które:**

(a) Wygasły;

(b) Nie są już kojarzone z użytkownikiem (procesem) lub osobą;

(c) Naruszają politykę organizacyjną; lub

(d) Były nieaktywne przez [***Realizacja: okres czasu określony przez organizację***]**.**

Omówienie: Wyłączenie wygasłych, nieaktywnych lub w inny sposób niezgodnych z przeznaczeniem kont wspiera koncepcję najmniejszych uprawnień i najmniejszej funkcjonalności, które zmniejszają powierzchnię ataku systemu.

Zabezpieczenia powiązane: Brak.

(4) ZARZĄDZANIE KONTAMI | AUTOMATYCZNE DZIAŁANIA AUDYTOWE

Automatyczny audyt tworzenia, modyfikacji, włączania, wyłączania i usuwania konta.

Omówienie: Zapisy z audytu zarządzania kontem są definiowane zgodnie z AU-2 oraz przeglądane, analizowane i raportowane zgodnie z AU-6.

Zabezpieczenia powiązane: AU-2, AU-6.

(5) ZARZĄDZANIE KONTAMI | WYLOGOWANIE PRZEZ UŻYTKOWNIKA PO OKREŚLONYM OKRESIE NIEAKTYWNOŚCI

Należy wymagać, aby użytkownicy wylogowali się po upływie [***Realizacja: określony przez organizację okres oczekiwanego braku aktywności lub opis czasu wylogowania***] **spodziewanej nieaktywności.**

Omówienie: Wylogowanie z nieaktywności jest oparte na zachowaniu lub polityce i wymaga od użytkowników podjęcia fizycznych działań w celu wylogowania się, gdy spodziewają się dłużej nieaktywności przez określony czas. Automatyczne

egzekwowanie wylogowania z nieaktywności jest regulowane przez zabezpieczenie AC-11.

Zabezpieczenia powiązane: AC-11.

(6) ZARZĄDZANIE KONTAMI | DYNAMICZNE ZARZĄDZANIE UPRAWNIENIAMI

Należy wdrożyć [Realizacja: *zdefiniowane przez organizację możliwości dynamicznego zarządzania uprawnieniami*].

Omówienie: W przeciwieństwie do podejść do kontroli dostępu, które wykorzystują statyczne konta i predefiniowane uprawnienia użytkowników, podejścia dynamicznej kontroli dostępu opierają się na decyzjach dotyczących kontroli dostępu w czasie rzeczywistym, umożliwianych przez dynamiczne zarządzanie uprawnieniami, takimi jak zabezpieczenie dostępu oparta na atrybutach. Podczas gdy tożsamość użytkownika pozostaje stosunkowo stała w czasie, uprawnienia użytkowników zmieniają się zazwyczaj częściej w zależności od bieżącej misji lub wymagań biznesowych oraz potrzeb operacyjnych organizacji. Przykładem dynamicznego zarządzania uprawnieniami jest natychmiastowe odebranie uprawnień użytkownikom, w przeciwieństwie do żądania, aby użytkownicy kończyli i wznawiali sesje w celu odzwierciedlenia zmian w uprawnieniach. Dynamiczne zarządzanie uprawnieniami może również obejmować mechanizmy, które zmieniają uprawnienia użytkowników w oparciu o dynamiczne reguły, w przeciwieństwie do edycji konkretnych profili użytkowników. Przykładem może być automatyczne dostosowywanie uprawnień użytkowników, jeśli pracują oni poza swoim normalnym czasem pracy, jeśli zmieniają się ich funkcje pracy lub zadania, lub jeśli systemy są obciążone lub w sytuacjach awaryjnych. Dynamiczne zarządzanie uprawnieniami obejmuje efekty zmian uprawnień, na przykład w przypadku zmiany kluczy szyfrujących używanych do komunikacji.

Zabezpieczenia powiązane: AC-16.

(7) ZARZĄDZANIE KONTAMI | UPRZYWILEJOWANE KONTA UŻYTKOWNIKÓW

(a) Tworzenie i zarządzanie kontami uprzywilejowanych użytkowników zgodnie z [***Wybór: schemat dostępu oparty na rolach; schemat dostępu oparty na atrybutach***]**;**

(b) Monitorowanie przydziałów uprzywilejowanych ról lub atrybutów;

(c) Monitorowanie zmian w rolach lub atrybutach; oraz

(d) Cofanie dostępu, gdy przypisanie uprzywilejowanej roli lub atrybutu nie jest już właściwe.

Omówienie: Uprzywilejowane role to zdefiniowane organizacyjnie role przypisane do osób, które pozwalają tym osobom na wykonywanie pewnych funkcji istotnych z punktu widzenia bezpieczeństwa, do których wykonywania zwykli użytkownicy nie są uprawnieni. Uprawnienia obejmują zarządzanie kluczami, zarządzanie kontami, administrację bazami danych, administrację systemem i siecią oraz administrację i obsługę stron internetowych. Schemat dostępu oparty na rolach porządkuje dozwolony dostęp do systemu i uprawnienia w role. Natomiast schemat dostępu oparty na atrybutach określa dozwolony dostęp do systemu oraz uprawnienia na podstawie atrybutów.

Zabezpieczenia powiązane: Brak.

(8) ZARZĄDZANIE KONTAMI | DYNAMICZNE ZARZĄDZANIE KONTEM

Dynamiczne tworzenie, aktywowanie, zarządzanie i dezaktywowanie [***Realizacja: konta systemowe zdefiniowane przez organizację***]**.**

Omówienie: Podejścia do dynamicznego tworzenia, aktywowania, zarządzania i dezaktywacji kont systemowych polegają na automatycznej obsłudze w czasie rzeczywistym kont podmiotów, które wcześniej nie były znane. Organizacje planują dynamiczne zarządzanie, tworzenie, aktywację i dezaktywację kont systemowych poprzez tworzenie relacji zaufania, reguł biznesowych oraz mechanizmów

z odpowiednimi uprawnieniami do zatwierdzania powiązanych uprawnień i przywilejów.

Zabezpieczenia powiązane: AC-16.

(9) ZARZĄDZANIE KONTAMI | OGRANICZENIA W KORZYSTANIU Z KONT WSPÓLNYCH I GRUPOWYCH

Zezwolenie na korzystanie tylko z kont wspólnych i grupowych, które spełniają [***Realizacja: organizacyjnie określone warunki ustanawiania kont wspólnych i grupowych***]**.**

Omówienie: Przed wydaniem zezwolenia na korzystanie ze wspólnych lub grupowych kont, organizacje rozważają zwiększone ryzyko wynikające z braku rozliczalności takich kont.

Zabezpieczenia powiązane: Brak.

(10) ZARZĄDZANIE KONTAMI | ZMIANA POŚWIADCZANIA UPRAWNIEŃ KONTA WSPÓLNEGO I GRUPOWEGO

[Wycofane: Włączone do AC-2k].

(11) ZARZĄDZANIE KONTAMI | WARUNKI UŻYTKOWANIA

Egzekwowanie [***Realizacja: okoliczności określone przez organizację i/lub warunki użytkowania***] **dla [Realizacja: *konta systemowe określone przez organizację*].**

Omówienie: Określanie i egzekwowanie warunków użytkowania pomaga egzekwować zasadę najmniejszych uprawnień, zwiększyć odpowiedzialność użytkownika i umożliwić skuteczne monitorowanie konta. Monitorowanie konta obejmuje alarmy generowane w przypadku, gdy konto jest wykorzystywane z naruszeniem parametrów organizacyjnych. Organizacje mogą opisać konkretne warunki lub okoliczności, w jakich można korzystać z kont systemowych, np.

ograniczając korzystanie z nich do określonych dni tygodnia, pór dnia lub określonych okresów czasu.

Zabezpieczenia powiązane: Brak.

(12) ZARZĄDZANIE KONTAMI | MONITOROWANIE KONT POD WZGLĘDEM NIETYPOWYCH ZASTOSOWAŃ

(a) Monitorowanie kont systemowych pod względem [***Realizacja: nietypowe użycie zdefiniowane przez organizację***]***;*** **oraz**

(b) Zgłaszanie nietypowego korzystania z kont systemowych do [***Realizacja: personel lub role zdefiniowane przez organizację***]**.**

Omówienie: Użycie nietypowe obejmuje dostęp do systemów o określonych porach dnia lub z miejsc, które nie są zgodne z normalnymi wzorcami użycia poszczególnych osób. Monitorowanie nietypowego użytkowania może ujawnić nieuczciwe zachowanie osób lub trwający atak. Monitorowanie kont może nieumyślnie stwarzać zagrożenie dla prywatności, ponieważ dane zbierane w celu zidentyfikowania nietypowego użytkowania mogą ujawnić wcześniej nieznane informacje o zachowaniu osób. Organizacje oceniają i dokumentują zagrożenia dla prywatności związane z monitorowaniem kont pod kątem nietypowego użytkowania w ramach oceny wpływu na prywatność oraz dokonują ustaleń zgodnych z ich programem ochrony prywatności.

Zabezpieczenia powiązane: AU-6, AU-7, CA-7, IR-8, SI-4.

(13) ZARZĄDZANIE KONTAMI | WYŁĄCZANIE KONT DOSTĘPOWYCH UŻYTKOWNIKOM WYSOKIEGO RYZYKA

Wyłączyć konta osób fizycznych w ciągu [***Realizacja: zdefiniowany przez organizację okres czasu***] **od momentu wykrycia** [***Realizacja: zdefiniowany przez organizację istotny czynnik ryzyka***]**.**

Omówienie: Użytkownicy, którzy stanowią znaczące zagrożenie dla bezpieczeństwa i/lub prywatności, to osoby, w stosunku do których wiarygodne

dowody wskazują na zamiar wykorzystania autoryzowanego dostępu do systemów w celu wyrządzenia szkody lub przez których przeciwnicy wyrządzą szkodę. Szkody takie obejmują negatywny wpływ na działalność organizacji, aktywa organizacyjne, osoby prywatne, inne organizacje lub Państwo. Ścisła koordynacja pomiędzy administratorami systemów, personelem prawnym, ds. zasobów ludzkich i personelem zatwierdzającymi ma zasadnicze znaczenie w przypadku wyłączania kont systemowych osób wysokiego ryzyka.

Zabezpieczenia powiązane: AU-6, SI-4.

Referencje: [NIST SP 800-162], [NIST SP 800-178], [NIST SP 800-192].

AC-3 EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU

Zabezpieczenie podstawowe: Egzekwowanie zatwierdzonych zezwoleń na logiczny dostęp do informacji i zasobów systemowych zgodnie z obowiązującymi zasadami kontroli dostępu.

Omówienie: Zasady kontroli dostępu reguluje dostęp pomiędzy aktywnymi jednostkami lub podmiotami (tj. użytkownikami lub procesami działającymi w imieniu użytkowników,) a pasywnymi jednostkami lub obiektami (tj. urządzeniami, plikami, zapisami, domenami) w systemach organizacyjnych. Poza egzekwowaniem autoryzowanego dostępu na poziomie systemu i uznaniem, że w systemach może znajdować się wiele aplikacji i usług wspierających realizację misji i funkcji biznesowych, na poziomie aplikacji i usług mogą być również stosowane mechanizmy egzekwowania dostępu w celu zapewnienia większego bezpieczeństwa i ochrony prywatności informacji. W przeciwieństwie do logicznych kontroli dostępu, które są wdrażane w ramach systemu, fizyczne kontrole dostępu są uwzględniane w zabezpieczeniach w kategorii ochrony fizycznej i środowiskowej (PE).

Zabezpieczenia powiązane: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AC- 24, AC-25, AT-2, AT-3, AU-9, CA-9, CM-5, CM-11, IA-2, IA-5, IA-6, IA-7, IA-11, MA-3, MA-4, MA-5, MP-4, PM-2, PS-3, PT-2, PT-3, SA-17, SC-2, SC-3, SC-4, SC-12, SC-13, SC-28, SC-31, SC-34, SI-4, SI-8.

Zabezpieczenia rozszerzone:

(1) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | OGRANICZONY DOSTĘP DO FUNKCJI UPRZYWILEJOWANYCH

[Wycofane: Włączone do AC-6].

(2) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | PODWÓJNA AUTORYZACJA

Egzekwowanie podwójnej autoryzacji dla [***Realizacja: zdefiniowanych przez organizację poleceń uprzywilejowanych i/lub innych zdefiniowanych przez organizację działań***]**.**

Omówienie: Podwójna autoryzacja, znana również jako dwuosobowe zabezpieczenie, zmniejsza ryzyko związane z zagrożeniami wewnętrznymi. Mechanizmy podwójnej autoryzacji wymagają zgody dwóch upoważnionych osób do ich wykonania. Aby zmniejszyć ryzyko zmowy, organizacje powinny rozważyć rotację obowiązków związanych z podwójną autoryzacją. Organizacje biorą pod uwagę ryzyko związane z wdrożeniem mechanizmów podwójnej autoryzacji, gdy natychmiastowa reakcja jest konieczna dla zapewnienia bezpieczeństwa publicznego i środowiskowego.

Zabezpieczenia powiązane: CP-9, MP-6.

(3) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | OBOWIĄZKOWA KONTROLA DOSTĘPU

Egzekwowanie [***Realizacja: zdefiniowana przez organizację obowiązkowa polityka kontroli dostępu***] ***w*** **odniesieniu do zbioru objętych nią podmiotów i obiektów określonych w tej polityce oraz miejsca, w którym zasada ta jest realizowana:**

(a) Jest jednolicie egzekwowana w odniesieniu do wszystkich objętych nią podmiotów i obiektów w ramach systemu;

(b) Określa, że podmiot, któremu przyznano dostęp do informacji, jest zobowiązany do nie wykonywania żadnego z poniższych działań;

(1) Przekazywania informacji nieupoważnionym podmiotom lub obiektom;

(2) Przyznawania swoich przywilejów innym podmiotom;

(3) Zmiany jakiegokolwiek atrybutu bezpieczeństwa (określonego przez zasady) podmiotów, obiektów, systemów lub komponentów systemu;

(4) Wyboru atrybutów bezpieczeństwa i wartości atrybutów (określonych przez zasady), które mają być powiązane z nowo utworzonymi lub zmodyfikowanymi obiektami; oraz

(5) Zmiany zasad regulujących kontrolę dostępu; oraz

(c) Określa, że podmiotom zaufanym [Realizacja: *podmioty określone przez organizację*] mogą być wyraźnie przyznane [*Realizacja: uprawnienia określone przez organizację*] w taki sposób, że nie są one ograniczone przez żaden określony podzbiór (lub wszystkie) powyższych ograniczeń.

Omówienie: Obowiązkowa kontrola dostępu to rodzaj nie uznaniowej (nakazowej) kontroli dostępu. Polityka obowiązkowej kontroli dostępu ogranicza działania, jakie podmioty mogą podejmować w związku z informacjami uzyskanymi z obiektów, do których już uzyskały dostęp. Zapobiega to przekazywaniu informacji przez podmioty nieupoważnionym podmiotom i obiektom. Polityka obowiązkowej kontroli dostępu ogranicza działania, które podmioty mogą podejmować w związku z propagowaniem uprawnień kontroli dostępu; to znaczy, że podmiot z uprawnieniami nie może przekazać tych uprawnień innym podmiotom. Polityka jest jednolicie egzekwowana na wszystkich podmiotach i obiektach, nad którymi system ma zabezpieczenie. W przeciwnym razie polityka kontroli dostępu może być obchodzona. Egzekwowanie to jest zapewnione przez implementację zgodną z koncepcją monitora referencyjnego opisaną w zabezpieczeniu AC-25. Polityka ta jest ograniczona przez system (tzn. po przekazaniu informacji poza zabezpieczenie systemu mogą być wymagane dodatkowe środki w celu zapewnienia, że ograniczenia dotyczące informacji pozostają w mocy).

Zaufanym podmiotom opisanym powyżej przyznaje się przywileje zgodne z koncepcją najmniejszych przywilejów (patrz: AC-6). Zaufanym podmiotom przyznawane są jedynie minimalne uprawnienia niezbędne do zaspokojenia misji/ potrzeb biznesowych organizacji w związku z powyższą polityką. Zabezpieczenie ma największe zastosowanie, gdy istnieje uprawnienie, które ustanawia politykę dostępu do kontrolowanych informacji jawnych lub informacji wrażliwych, a niektórzy użytkownicy systemu nie są upoważnieni do dostępu do wszystkich takich informacji znajdujących się w systemie. Obowiązkowa kontrola dostępu może funkcjonować w połączeniu z uznaniową kontrolą dostępu

opisaną w zabezpieczeniu rozszerzonym AC-3(4). Podmiot, którego działanie jest ograniczone przez zasady obowiązkowej kontroli dostępu, może nadal działać w ramach mniej rygorystycznych ograniczeń określonych w AC-3(4), ale zasady obowiązkowej kontroli dostępu mają pierwszeństwo przed mniej rygorystycznymi ograniczeniami określonymi w AC-3(4). Na przykład, podczas gdy polityka obowiązkowej kontroli dostępu nakłada ograniczenie, które uniemożliwia podmiotowi przekazanie informacji innemu podmiotowi działającemu na innym poziomie wpływu lub klasyfikacji, AC-3(4) zezwala podmiotowi na przekazanie informacji innemu podmiotowi działającemu na tym samym poziomie wpływu lub klasyfikacji, co podmiot. Przykłady polityki obowiązkowej kontroli dostępu obejmują politykę Bell-LaPadula w zakresie ochrony poufności informacji oraz politykę Biba w zakresie ochrony integralności informacji.

Zabezpieczenia powiązane: SC-7.

(4) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | UZNANIOWA KONTROLA DOSTĘPU

Egzekwowanie [***Realizacja: zdefiniowana przez organizację polityka uznaniowej kontroli dostępu***] **w odniesieniu do zbioru objętych nią podmiotów i obiektów określonych w polityce, a także w przypadku, gdy polityka określa, że podmiot, któremu przyznano dostęp do informacji, może wykonać jedną lub więcej z poniższych czynności:**

(a) Przekazać informacje innym podmiotom lub obiektom;

(b) Przyznać swoje przywileje innym podmiotom;

(c) Zmienić atrybuty zabezpieczeń podmiotów, obiektów, systemu lub jego komponentów

(d) Wybrać atrybuty bezpieczeństwa, które mają być powiązane z nowo utworzonymi lub zmienionymi obiektami; lub

(e) Zmienić zasady regulujące kontrolę dostępu.

Omówienie: Podczas wdrażania polityki uznaniowej kontroli dostępu, podmioty nie są ograniczane co do tego, jakie działania mogą podjąć w związku z informacjami, do których już uzyskały dostęp. Podmioty, którym przyznano dostęp do informacji, nie są zatem pozbawione możliwości przekazania informacji innym podmiotom lub obiektom (tj. podmioty mają swobodę w przekazywaniu informacji). Uznaniowa kontrola dostępu może działać w połączeniu z obowiązkową kontrolą dostępu opisaną w zabezpieczeniach rozszerzonych AC-3(3) i AC-3(15). Podmiot, którego działanie jest ograniczone przez zasady obowiązkowej kontroli dostępu, może nadal działać w ramach mniej rygorystycznych ograniczeń uznaniowej kontroli dostępu. W związku z tym, podczas gdy AC-3(3) nakłada ograniczenia, które uniemożliwiają podmiotowi przekazywania informacji innemu podmiotowi działającemu na innym poziomie wpływu lub klasyfikacji, AC-3(4) zezwala podmiotowi na przekazanie informacji innemu podmiotowi na tym samym poziomie wpływu lub klasyfikacji. Polityka ta jest ograniczona przez system. Po przekazaniu informacji poza zabezpieczenie systemu mogą być wymagane dodatkowe środki w celu zapewnienia, że ograniczenia te pozostają w mocy. Podczas gdy tradycyjne definicje uznaniowej kontroli dostępu wymagają kontroli dostępu opartej na tożsamości, ograniczenie to nie jest wymagane w przypadku tego konkretnego zastosowania uznaniowej kontroli dostępu.

Zabezpieczenia powiązane: Brak.

(5) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | INFORMACJE DOTYCZĄCE BEZPIECZEŃSTWA

Zapobieganie dostępowi do [***Realizacja: zdefiniowanych przez organizację informacji istotnych z punktu widzenia bezpieczeństwa***] **z wyjątkiem sytuacji, w których system znajduje się w bezpiecznym stanie nieoperacyjnym.**

Omówienie: Informacje istotne dla bezpieczeństwa to informacje zawarte w systemach, które mogą potencjalnie wpływać na działanie funkcji

bezpieczeństwa lub świadczenie usług w zakresie bezpieczeństwa w sposób, który mógłby doprowadzić do niewdrożenia polityki bezpieczeństwa i ochrony prywatności systemu lub do rozdzielenia kodu i danych. Informacje istotne dla bezpieczeństwa obejmują listy kontroli dostępu, zasady filtrowania routerów lub zapór sieciowych, parametry konfiguracyjne usług bezpieczeństwa oraz informacje dotyczące zarządzania kluczami kryptograficznymi. Bezpieczne, nieoperacyjne stany systemu obejmują czasy, w których systemy nie wykonują zadań lub nie przetwarzają danych związanych z działalnością biznesową organizacji, np. gdy system jest wyłączony z eksploatacji w celu konserwacji, rozruchu, rozwiązywania problemów lub wyłączenia.

Zabezpieczenia powiązane: CM-6, SC-39.

(6) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | OCHRONA INFORMACJI UŻYTKOWNIKA I SYSTEMU

[Wycofane: Włączone do MP-4 i SC-28].

(7) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | KONTROLA DOSTĘPU OPARTA NA ROLI

Egzekwowanie zasady kontroli dostępu opartej na rolach w odniesieniu do zdefiniowanych podmiotów i obiektów oraz kontroli dostępu w oparciu o [*Realizacja: role zdefiniowane przez organizację i użytkownicy upoważnieni do pełnienia takich ról*].

Omówienie: Kontrola dostępu oparta na roli (*ang. Role based access control - RBAC*) to polityka kontroli dostępu, która wymusza dostęp do obiektów i funkcji systemu w oparciu o zdefiniowaną rolę (tj. funkcję pracy) podmiotu. Organizacje mogą tworzyć określone role w oparciu o funkcje zadań i uprawnienia (tj. przywileje) do wykonywania niezbędnych operacji w systemach związanych z funkcjami zdefiniowanymi przez organizację. Gdy użytkownicy są przypisani do określonych ról, dziedziczą uprawnienia lub przywileje zdefiniowane dla tych ról. RBAC upraszcza administrowanie uprawnieniami organizacji, ponieważ uprawnienia nie są przypisane bezpośrednio do każdego użytkownika (których

może być duża liczba), lecz są nabywane poprzez przypisanie ról. RBAC może również zwiększyć ryzyko związane z prywatnością i bezpieczeństwem, jeśli osoby przypisane do danej roli uzyskają dostęp do informacji wykraczający poza to, czego potrzebują do wspierania misji organizacji lub funkcji biznesowych. RBAC może być wdrożony, jako obowiązkowa lub uznaniowa forma kontroli dostępu. W przypadku organizacji wdrażających RBAC z obowiązkową kontrolą dostępu, wymogi zawarte w AC-3(3) określają zakres podmiotów i obiektów objętych polityką.

Zabezpieczenia powiązane: Brak.

(8) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | COFNIĘCIE ZEZWOLEŃ NA DOSTĘP

Egzekwowanie cofnięcia uprawnień dostępu wynikających ze zmian w atrybutach bezpieczeństwa podmiotów i obiektów w oparciu o [***Realizacja: zasady określone przez organizację określające czas cofnięcia uprawnień dostępu***]**.**

Omówienie: Zasady cofania dostępu mogą się różnić w zależności od rodzaju cofniętego dostępu. Na przykład, jeżeli podmiot (tj. użytkownik lub proces działający w imieniu użytkownika) zostanie usunięty z grupy, dostęp może zostać cofnięty dopiero przy następnym otwarciu obiektu lub przy kolejnej próbie dostępu do obiektu. Cofnięcie na podstawie zmian etykiet zabezpieczających może stać się skuteczne natychmiast. Organizacje zapewniają alternatywne sposoby natychmiastowego cofnięcia zezwoleń, jeśli systemy nie mogą zapewnić takiej możliwości i konieczne jest natychmiastowe unieważnienie zezwolenia.

Zabezpieczenia powiązane: Brak.

(9) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | KONTROLOWANE UDOSTĘPNIENIE INFORMACJI

Udostępnianie informacji poza systemem tylko wtedy, gdy:

(a) Odbiorca [***Realizacja: system zdefiniowany przez organizację lub składnik systemu***] **zapewnia** [***Realizacja: zabezpieczenia zdefiniowane przez organizację***]**; oraz**

(b) [***Realizacja: zabezpieczenia określone przez organizację***] **są wykorzystywane do sprawdzania adekwatności informacji przeznaczonych do udostępnienia (jeżeli istnieją podstawy prawne do udostępniania informacji).**

Omówienie: Organizacje mogą bezpośrednio chronić informacje tylko wtedy, gdy znajdują się one w systemie. Dodatkowe zabezpieczenia mogą być konieczne w celu zapewnienia, że informacje organizacyjne są odpowiednio chronione po ich przekazaniu poza system. W sytuacjach, gdy system nie jest w stanie określić adekwatności ochrony zapewnianej przez podmioty zewnętrzne, jako środek łagodzący, organizacje proceduralnie określają, czy systemy zewnętrzne zapewniają odpowiednie zabezpieczenia. Środki stosowane do określenia adekwatności zabezpieczeń zapewnianej przez systemy zewnętrzne obejmują przeprowadzanie okresowych ocen (inspekcji/testów), zawieranie umów pomiędzy organizacją a jej odpowiednikami lub inny proces. Środki stosowane przez podmioty zewnętrzne w celu ochrony otrzymywanych informacji nie muszą być takie same jak te stosowane przez organizację, ale stosowane środki powinny być wystarczające do zapewnienia spójnej oceny polityki bezpieczeństwa i ochrony prywatności w celu ochrony informacji i prywatności osób.

Kontrolowane udostępnianie informacji wymaga, aby systemy wdrożyły środki techniczne lub proceduralne w celu zatwierdzenia informacji przed udostępnieniem ich zewnętrznym systemom. Na przykład, jeżeli system przekazuje informacje do systemu kontrolowanego przez inną organizację, stosuje się środki techniczne w celu sprawdzenia, czy atrybuty bezpieczeństwa i ochrony prywatności związane z eksportowanymi informacjami są odpowiednie dla systemu otrzymującego. Alternatywnie, jeżeli system przekazuje informacje do drukarki w przestrzeni kontrolowanej przez organizację, można zastosować

środki proceduralne zapewniające, że tylko upoważnione osoby uzyskają dostęp do drukarki.

Zabezpieczenia powiązane: CA-3, PT-7, PT-8, SA-9, SC-16.

(10) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | NADZOROWANE OBEJŚCIE MECHANIZMÓW KONTROLI DOSTĘPU

Zastosowanie audytowanego obejścia mechanizmów automatycznej kontroli dostępu w ramach [Realizacja: *warunki określone przez organizację*] przez [*Realizacja: role określone przez organizację*].

Omówienie: W pewnych sytuacjach, np. gdy istnieje zagrożenie dla życia ludzkiego lub zdarzenie zagrażające zdolności organizacji do wykonywania krytycznych misji lub funkcji biznesowych, może być konieczne wprowadzenie funkcji nadrzędnej dla mechanizmów kontroli dostępu (nadzorowane obejście mechanizmów kontroli dostępu). Warunki obejścia są określane przez organizacje i stosowane tylko w tych ograniczonych okolicznościach. Zdarzenia audytowe zdefiniowane są w zabezpieczeniu AU-2. Zapisy audytów są generowane w zabezpieczeniu AU-12.

Zabezpieczenia powiązane: AU-2, AU-6, AU-10, AU-12, AU-14.

(11) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | OGRANICZENIE DOSTĘPU DO OKREŚLONYCH RODZAJÓW INFORMACJI

Ograniczanie dostępu do repozytoriów danych zawierających [*Realizacja: typy informacji zdefiniowane przez organizację*].

Omówienie: Ograniczenie dostępu do określonych informacji ma na celu zapewnienie elastyczności w zakresie kontroli dostępu do określonych typów informacji w ramach systemu. Na przykład dostęp oparty na rolach mógłby być stosowany w celu umożliwienia dostępu tylko do określonego rodzaju informacji umożliwiających identyfikację osoby w ramach bazy danych, a nie w celu umożliwienia dostępu do bazy danych w całości. Inne przykłady obejmują

ograniczenie dostępu do kluczy kryptograficznych, informacji o uwierzytelnianiu i wybranych informacji systemowych.

Zabezpieczenia powiązane: CM-8, CM-12, CM-13, PM-5.

(12) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | ZAPEWNIENIE I EGZEKWOWANIE DOSTĘPU DO APLIKACJI

(a) Wymaganie od aplikacji zapewnienia, w ramach procesu instalacji, niezbędnego dostępu do następujących aplikacji i funkcji systemowych: [*Realizacja*: *aplikacje i funkcje systemowe zdefiniowane przez organizację*];

(b) Zapewnienie mechanizmu egzekwowania prawa w celu zapobiegania nieupoważnionemu dostępowi; oraz

(c) Zatwierdzanie zmian dostępu po przeprowadzeniu wstępnej instalacji aplikacji.

Omówienie: Zapewnienie i egzekwowanie uprawnień aplikacji dostępowych jest związane z aplikacjami, które muszą uzyskać dostęp do istniejących aplikacji i funkcji systemowych, w tym kontaktów użytkowników, globalnych systemów pozycjonowania, kamer, klawiatur, mikrofonów, sieci, telefonów lub innych plików.

Zabezpieczenia powiązane: CM-7.

(13) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | KONTROLA DOSTĘPU NA PODSTAWIE ATRYBUTÓW

Egzekwowanie zasady kontroli dostępu opartej na atrybutach w odniesieniu do zdefiniowanych podmiotów i obiektów oraz kontroli dostępu w oparciu o [*Realizacja: atrybuty zdefiniowane przez organizację w celu uzyskania uprawnień dostępu*].

Omówienie: Zabezpieczenie dostępu oparta na atrybutach to polityka kontroli dostępu, która ogranicza dostęp do systemu autoryzowanym użytkownikom na podstawie określonych atrybutów organizacyjnych (np. funkcja pracy,

tożsamość), atrybutów działania (np. czytanie, pisanie, usuwanie), atrybutów środowiskowych (np. pora dnia, lokalizacja) oraz atrybutów zasobów (np. klasyfikacja dokumentu). Organizacje mogą tworzyć reguły oparte na atrybutach i uprawnieniach (np. przywilejach) do wykonywania niezbędnych operacji w systemach skojarzonych z atrybutami i regułami zdefiniowanymi przez organizację. W przypadku przypisania użytkowników do atrybutów zdefiniowanych w zasadach lub regułach kontroli dostępu opartych na atrybutach, mogą oni zostać przydzieleni do systemu z odpowiednimi uprawnieniami lub dynamicznie uzyskać dostęp do chronionego zasobu. Zabezpieczenie dostępu oparta na atrybutach może być wdrożone, jako obowiązkowa lub uznaniowa forma kontroli dostępu. W przypadku wdrożenia obowiązkowej kontroli dostępu, wymagania zawarte w zabezpieczeniu rozszerzonym AC-3(3) określają katalog podmiotów i obiektów objętych polityką.

Zabezpieczenia powiązane: Brak.

(14) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | DOSTĘP INDYWIDUALNY

Dostarczanie [***Realizacja: mechanizmy zdefiniowane przez organizację***] ***w*** **celu umożliwienia osobom dostępu do następujących elementów ich danych osobowych:** [***Realizacja: elementy określone przez organizację***]**.**

Omówienie: Dostęp indywidualny daje osobom możliwość wglądu w dane osobowe przechowywane w aktach organizacyjnych, niezależnie od ich formatu. Dostęp pomaga osobom zrozumieć, w jaki sposób przetwarzane są ich dane osobowe. Może on również pomóc osobom w zapewnieniu, że ich dane są poprawne. Mechanizmy dostępu mogą obejmować formularze wniosków i interfejsy aplikacji. Mogą być zlokalizowane w systemach powiadomień o rejestrach oraz na stronach internetowych organizacji. Dostęp do niektórych rodzajów rejestrów może być nie możliwy (np. w przypadku rejestrów organów ścigania, organy mogą być zwolnione z obowiązku ujawnienia w ramach dostępu publicznego) lub mogą wymagać pewnych poziomów zapewnienia

uwierzytelnienia. Personel organizacyjny powinien konsultować się z osobami odpowiedzialnymi za prywatność i doradztwo prawne, celem określenia odpowiednich mechanizmów i prawa lub ograniczania dostępu.

Zabezpieczenia powiązane: IA-8, PM-22, PM-20, PM-21, PT-6.

(15) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | UZNANIOWA I OBOWIĄZKOWA KONTROLA DOSTĘPU

(a) Egzekwowanie [***Realizacja: zdefiniowana przez organizację obowiązkowa polityka kontroli dostępu***] **w odniesieniu do zestawu objętych nią podmiotów i obiektów określonych w tej polityce; oraz**

(b) Egzekwowanie [***Realizacja: zdefiniowana przez organizację uznaniowa polityka kontroli dostępu***] **w odniesieniu do zestawu objętych nią podmiotów i obiektów określonych w tej polityce.**

Omówienie: Jednoczesne wdrożenie obowiązkowej zasady kontroli dostępu oraz uznaniowej zasady kontroli dostępu może zapewnić dodatkową ochronę przed nieautoryzowanym wykonaniem kodu przez użytkowników lub procesy działające w ich imieniu. Pomaga to zapobiec sytuacji, w której pojedynczy zagrożony użytkownik lub proces naruszyłby cały system.

Zabezpieczenia powiązane: SC-2, SC-3, AC-4.

Referencje: [PRIVACT], [OMB A-130], [NIST SP 800-57-1], [NIST SP 800-57-2], [NIST SP 800-57-3], [NIST SP 800-162], [NIST SP 800-178], [IR 7874].

AC-4 EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI

Zabezpieczenie podstawowe: Egzekwowanie zatwierdzonych uprawnień do kontroli przepływu informacji w ramach systemu oraz pomiędzy połączonymi systemami w oparciu o [*Realizacja: zasady kontroli przepływu informacji określone przez organizację*].

Omówienie: Kontrola przepływu informacji określa, gdzie informacje mogą być przesyłane w obrębie danego systemu oraz pomiędzy systemami (w przeciwieństwie do tego, kto ma dostęp do informacji), a także bez względu na to, kto ma później dostęp do tych informacji. Ograniczenia kontroli przepływu obejmują blokowanie zewnętrznego ruchu, który rzekomo pochodzi z wewnątrz organizacji, uniemożliwienie przekazywania informacji kontrolowanych do Internetu, ograniczenie żądań internetowych, które nie pochodzą z wewnętrznego serwera proxy, oraz ograniczenie przekazywania informacji między organizacjami w oparciu o struktury danych i treści. Przesyłanie informacji między organizacjami może wymagać zawarcia umowy określającej sposób egzekwowania przepływu informacji (patrz: zabezpieczenie CA-3). Przesyłanie informacji pomiędzy systemami w domenach bezpieczeństwa lub prywatności o różnych zasadach bezpieczeństwa lub prywatności stwarza ryzyko, że takie transfery naruszą jedną lub więcej reguł bezpieczeństwa lub prywatności domeny. W takich sytuacjach właściciele informacji/osoby odpowiedzialne za ochronę danych udzielają wskazówek w wyznaczonych punktach egzekwowania polityki pomiędzy połączonymi systemami. Organizacje powinny rozważyć narzucenie konkretnych rozwiązań architektonicznych w celu egzekwowania określonych polityk bezpieczeństwa i ochrony prywatności. Egzekwowanie obejmuje zakaz przekazywania informacji pomiędzy połączonymi systemami (tj. zezwalanie tylko na dostęp), weryfikowanie uprawnień pisemnych przed przyjęciem informacji z innej domeny bezpieczeństwa lub prywatności albo połączonego systemu, stosowanie mechanizmów sprzętowych do egzekwowania jednokierunkowego przepływu informacji oraz wdrażanie zaufanych mechanizmów

zmiany klasyfikacji w celu zmiany atrybutów i etykiet bezpieczeństwa lub prywatności.

Organizacje powszechnie stosują politykę kontroli przepływu informacji i wprowadzają mechanizmy kontroli przepływ informacji między wyznaczonymi źródłami i miejscami przeznaczenia w ramach systemów oraz między połączonymi systemami. Kontrola przepływu informacji bazuje na podstawie charakterystyki informacji i/lub ścieżce komunikacyjnej. Egzekwowanie kontroli przepływu informacji występuje na przykład w urządzeniach brzegowych, które wykorzystują zestawy reguł lub ustanawiają ustawienia konfiguracyjne ograniczające usługi systemowe, zapewniają możliwość filtrowania pakietów w oparciu o informacje z nagłówka lub zapewniają możliwość filtrowania komunikatów w oparciu o treść komunikatu. Organizacje biorą również pod uwagę wiarygodność mechanizmów filtrowania i/lub kontroli (tj. sprzętu, oprogramowania sprzętowego i aplikacji), które są kluczowe dla egzekwowania przepływu informacji. Zabezpieczenia rozszerzone AC-4(3) do AC-4(32) dotyczą przede wszystkim potrzeb rozwiązań między domenowych, które skupiają się na bardziej zaawansowanych technikach filtrowania, dogłębnej analizie i silniejszych mechanizmach egzekwowania przepływu informacji wdrożonych w produktach między domenowych, takich jak zabezpieczenia o wysokim stopniu wiarygodności. Takie możliwości nie są na ogół dostępne w rozwiązaniach komercyjnych. Egzekwowanie przepływu informacji ma również zastosowanie do zabezpieczeń transferu ruchu (np. routingu i DNS).

Zabezpieczenia powiązane: AC-3, AC-6, AC-16, AC-17, AC-19, AC-21, AU-10, CA-3, CA-9, CM-7, PL-9, PM-24, SA-17, SC-4, SC-7, SC-16, SC-31.

Zabezpieczenia rozszerzone:

(1) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | BEZPIECZEŃSTWO OBIEKTÓW I ATRYBUTY PRYWATNOŚCI

Wykorzystanie [Realizacja: *atrybuty bezpieczeństwa i ochrony prywatności zdefiniowane przez organizację*] związane z [*Realizacja: informacje*

zdefiniowane przez organizację, źródła i obiekty docelowe] **do egzekwowania** [***Realizacja: reguły kontroli przepływu informacji zdefiniowane przez organizację***] **jako podstawy do podejmowania decyzji dotyczących kontroli przepływu informacji.**

Omówienie: Mechanizmy egzekwowania reguł dotyczących przepływu informacji porównują atrybuty bezpieczeństwa i ochrony prywatności związane z informacjami (tj. zawartość i strukturę danych) oraz obiektami źródłowymi i docelowymi oraz odpowiednio reagują, gdy mechanizmy egzekwowania przepływów napotykają na przepływy informacji, które nie są wyraźnie dozwolone przez politykę przepływu informacji. Na przykład, obiekt informacyjny oznaczony jako *nieklasyfikowany będzie mógł przepływać* do obiektu docelowego oznaczonego jako *nieklasyfikowany,* ale obiekt informacyjny oznaczony jako *klasyfikowany* nie będzie mógł przepływać do obiektu docelowego oznaczonego jako *nieklasyfikowany*. Zbiór danych osobowych może być oznaczony ograniczeniami dotyczącymi łączenia z innymi typami zbiorów danych, a tym samym nie będzie mógł przepływać do zastrzeżonego zbioru danych. Atrybuty bezpieczeństwa i ochrony prywatności mogą również obejmować adresy źródłowe i docelowe stosowane w zaporach sieciowych filtrujących transmisję danych. Egzekwowanie przepływu z wykorzystaniem jednoznacznych atrybutów bezpieczeństwa lub prywatności może być wykorzystywane na przykład do kontrolowania uwalniania niektórych rodzajów informacji.

Zabezpieczenia powiązane: Brak.

(2) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | PRZETWARZANIE DOMEN

Wykorzystanie chronionych domen przetwarzania do egzekwowania [***Realizacja: zasady kontroli przepływu informacji określone przez organizację***] **jako podstawy do podejmowania decyzji dotyczących kontroli przepływu.**

Omówienie: Chronione domeny przetwarzania w systemach to przestrzenie przetwarzania, które mają kontrolowane interakcje z innymi przestrzeniami

przetwarzania, umożliwiające kontrolę przepływu informacji pomiędzy tymi przestrzeniami oraz do/z obiektów informatycznych. Chronione domeny przetwarzania mogą być zapewnione, na przykład, poprzez wdrożenie egzekwowania reguł dotyczących domen i typów. W egzekwowaniu domen i typów procesy systemowe są przypisane do domen, informacje są identyfikowane według typów, a przepływy informacji są kontrolowane na podstawie dozwolonego dostępu do informacji (tj. określonego według domeny i typu), dozwolonej sygnalizacji pomiędzy domenami oraz dozwolonych przejść procesów do innych domen.

Zabezpieczenia powiązane: SC-39.

(3) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | DYNAMICZNA KONTROLA PRZEPŁYWU INFORMACJI

Egzekwowanie [***Realizacja: zasady kontroli przepływu informacji określone przez organizację***]**.**

Omówienie: Polityka organizacyjna dotycząca dynamicznej kontroli przepływu informacji obejmuje dopuszczenie lub niedopuszczenie do przepływu informacji w oparciu o zmieniające się warunki lub względy misyjne lub operacyjne. Zmieniające się warunki obejmują zmiany w zakresie tolerancji ryzyka wynikające ze zmian w dostępności przekazu potrzeb misyjnych lub biznesowych, zmiany w środowisku zagrożeń oraz wykrywanie potencjalnie szkodliwych lub niekorzystnych zdarzeń.

Zabezpieczenia powiązane: SI-4.

(4) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | KONTROLA PRZEPŁYWU ZASZYFROWANYCH INFORMACJI

Zapobieganie omijaniu przez zaszyfrowane informacje [***Realizacja: mechanizmy kontroli przepływu informacji określone przez organizację***] **poprzez** [***Wybór (jeden lub więcej): odszyfrowanie informacji; zablokowanie przepływu***

zaszyfrowanych informacji; zakończenie sesji komunikacyjnych usiłujących przekazać zaszyfrowane informacje; [***Realizacja: procedura lub metoda określona przez organizację***]]***.***

Omówienie: Mechanizmy kontroli przepływu obejmują sprawdzanie treści, filtry polityki bezpieczeństwa oraz identyfikatory typów danych. Termin szyfrowanie obejmuje także dane zakodowane nierozpoznane przez mechanizmy filtrujące.

Zabezpieczenia powiązane: SI-4.

(5) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | WBUDOWANE RODZAJE DANYCH

Egzekwowanie [***Realizacja: ograniczenia określone przez organizację***] **osadzania typów danych w ramach innych typów danych.**

Omówienie: Wbudowywanie typów danych w inne typy danych może skutkować zmniejszeniem skuteczności kontroli przepływu. Osadzanie typów danych obejmuje wstawianie plików, jako obiektów do innych plików oraz używanie skompresowanych lub zarchiwizowanych typów danych, które mogą zawierać wiele osadzonych typów danych. Ograniczenia dotyczące osadzania typów danych uwzględniają poziomy osadzania i zakazują poziomów osadzania typów danych, które wykraczają poza możliwości narzędzi kontrolnych.

Zabezpieczenia powiązane: Brak.

(6) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | METADANE

Egzekwowanie kontroli przepływu informacji w oparciu o [***Realizacja: metadane zdefiniowane przez organizację***]**.**

Omówienie: Metadane to informacje, które opisują charakterystykę danych. Metadane mogą zawierać metadane strukturalne opisujące struktury danych lub metadane opisowe opisujące zawartość danych. Egzekwowanie dopuszczalnych przepływów informacji w oparciu o metadane umożliwia prostszą i bardziej efektywną kontrolę przepływu. Organizacje biorą pod uwagę wiarygodność

metadanych w zakresie dokładności danych (tj. wiedzy o poprawności wartości metadanych w odniesieniu do danych), integralności danych (tj. ochrony przed nieautoryzowanymi zmianami metadanych) oraz powiązania metadanych z wagą danych (tj. stosowania wystarczająco silnych technik wiązania z odpowiednim zabezpieczeniem).

Zabezpieczenia powiązane: AC-16, SI-7.

(7) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | MECHANIZMY PRZEPŁYWU JEDNOKIERUNKOWEGO

Egzekwowanie jednokierunkowego przepływu informacji poprzez sprzętowe mechanizmy kontroli przepływu.

Omówienie: Mechanizmy jednokierunkowego przepływu mogą być również określane jako sieć jednokierunkowa, jednokierunkowa brama bezpieczeństwa lub dioda danych. Mechanizmy jednokierunkowego przepływu mogą być stosowane w celu uniemożliwienia eksportu danych z domeny lub systemu o większym wpływie lub klasyfikacji, zezwalając jednocześnie na import danych z domen lub systemów o mniejszym wpływie lub niesklasyfikowanych.

Zabezpieczenia powiązane: Brak.

(8) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | FILTRY POLITYKI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

(a) Egzekwowanie kontroli przepływu informacji przy użyciu [Realizacja: *filtry bezpieczeństwa zdefiniowane przez organizację lub filtry polityki prywatności*] jako podstawy do podejmowania decyzji dotyczących kontroli przepływu dla [*Realizacja: przepływ informacji zdefiniowany przez organizację*]; oraz

(b) *Wybór (jeden lub więcej): Blokada; Zerwanie; Modyfikacja; Kwarantanna*] danych po niepowodzeniu działania filtra zgodnie z [*Realizacja: zdefiniowana przez organizację polityka bezpieczeństwa lub prywatności*].

Omówienie: Zdefiniowane przez organizację filtry bezpieczeństwa lub polityki prywatności mogą dotyczyć struktur i treści danych. Na przykład, filtry bezpieczeństwa lub polityki prywatności dla struktur danych mogą sprawdzać maksymalną długość plików, maksymalne rozmiary pól i typy danych/ plików (dla danych ustrukturyzowanych i nieustrukturyzowanych). Filtry bezpieczeństwa lub polityki prywatności dla zawartości danych mogą sprawdzać konkretne słowa, wyliczone wartości lub zakresy wartości danych, a także zawartość ukrytą. Dane ustrukturyzowane pozwalają na interpretację zawartości danych przez aplikacje. Dane nieustrukturyzowane odnoszą się do informacji cyfrowych bez struktury danych lub ze strukturą danych, która nie ułatwia opracowania zestawów reguł mających na celu uwzględnienie wpływu lub poziomu klasyfikacji informacji przekazywanych przez dane lub decyzje dotyczące egzekwowania prawa w zakresie przepływu danych. Dane nieustrukturyzowane składają się z obiektów zawierających mapy bitowe, które z natury nie są oparte na języku (tj. pliki graficzne, wideo lub audio) oraz z obiektów tekstowych, które są oparte na językach pisanych lub drukowanych. Organizacje mogą wdrożyć więcej niż jeden filtr bezpieczeństwa lub polityki prywatności, aby spełnić cele kontroli przepływu informacji.

Zabezpieczenia powiązane: Brak.

(9) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | OCENA PRZEZ UPRAWNIONĄ OSOBĘ

Stosowanie oceny dopuszczalności przepływu przez uprawnioną osobę [***Realizacja: przepływ informacji określony przez organizację***] ***pod*** **następującymi warunkami:** [***Realizacja: warunki określone przez organizację***]**.**

Omówienie: Organizacje definiują filtry bezpieczeństwa lub polityki prywatności dla wszystkich sytuacji, w których możliwe jest podjęcie decyzji o automatycznej kontroli przepływu. Jeżeli podjęcie w pełni zautomatyzowanej decyzji w zakresie kontroli przepływu nie jest możliwe, wówczas zamiast lub jako uzupełnienie

zautomatyzowanego filtrowania polityki bezpieczeństwa lub prywatności można zastosować przegląd przez uprawnioną osobę. Weryfikacja ludzka może być również stosowana, jeśli organizacje uznają to za konieczne.

Zabezpieczenia powiązane: Brak.

(10) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | WŁĄCZANIE I WYŁĄCZANIE FILTRÓW BEZPIECZEŃSTWA LUB POLITYKI PRYWATNOŚCI

Zapewnienie uprawnionym administratorom możliwości włączania i wyłączania [Realizacja: *filtry bezpieczeństwa lub polityki prywatności zdefiniowane przez organizację*] pod następującymi warunkami: [Realizacja: *warunki określone przez organizację*].

Omówienie: Na przykład, jeśli pozwala na to autoryzacja systemu, administratorzy mogą włączyć filtry bezpieczeństwa lub polityki prywatności, aby uwzględnić zatwierdzone typy danych. Administratorzy mają również możliwość wyboru filtrów, które są wykonywane w odniesieniu do konkretnego przepływu danych w oparciu o rodzaj przesyłanych danych, źródłowe i docelowe domeny bezpieczeństwa oraz inne funkcje związane z bezpieczeństwem lub prywatnością, w zależności od potrzeb.

Zabezpieczenia powiązane: Brak.

(11) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | KONFIGURACJA FILTRÓW BEZPIECZEŃSTWA LUB POLITYKI PRYWATNOŚCI

Zapewnienie uprawnionym administratorom możliwości konfiguracji [Realizacja: *filtry bezpieczeństwa lub polityki prywatności zdefiniowane przez organizację*] w celu obsługi różnych polityk bezpieczeństwa lub prywatności.

Omówienie: Dokumentacja powinna zawierać szczegółowe informacje na temat konfigurowania filtrów bezpieczeństwa lub polityki prywatności. Na przykład, administratorzy mogą skonfigurować filtry bezpieczeństwa lub polityki prywatności, aby zawierały listę nieodpowiednich słów, które mechanizmy

bezpieczeństwa lub polityki prywatności sprawdzają zgodnie z definicjami podanymi przez organizacje.

Zabezpieczenia powiązane: Brak.

(12) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | IDENTYFIKATORY TYPÓW DANYCH

Przy przesyłaniu informacji pomiędzy różnymi domenami bezpieczeństwa należy używać [***Realizacja: identyfikatory typu danych zdefiniowane przez organizację***] **do weryfikacji danych istotnych dla decyzji dotyczących przepływu informacji.**

Omówienie: Identyfikatory typów danych obejmują nazwy plików, typy plików, podpisy plików lub tokeny oraz szereg wewnętrznych podpisów plików lub tokenów. Systemy pozwalają na przesyłanie danych wyłącznie w sposób zgodny ze specyfikacją formatu typu danych. Identyfikacja i weryfikacja typów danych opiera się na określonych specyfikacjach związanych z każdym dozwolonym formatem danych. Sama nazwa pliku i numer nie są wykorzystywane do identyfikacji typów danych. Zawartość jest weryfikowana składniowo i semantycznie w stosunku do swojej specyfikacji, aby zapewnić, że jest to właściwy typ danych.

Zabezpieczenia powiązane: Brak.

(13) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | DEKOMPOZYCJA INFORMACJI NA ODPOWIEDNIE PODSKŁADNIKI

Przy przekazywaniu informacji pomiędzy różnymi domenami bezpieczeństwa należy rozłożyć informacje na [***Realizacja: zdefiniowane przez organizację odpowiednie subkomponenty***] **w celu poddania ich mechanizmom egzekwowania polityki bezpieczeństwa.**

Omówienie: Dekompozycja informacji, przed przekazaniem, na istotne dla polityki bezpieczeństwa części składowe ułatwia podejmowanie decyzji

dotyczących źródła, miejsca przeznaczenia, certyfikatów, klasyfikacji, załączników i innych elementów różnicujących, związanych z bezpieczeństwem lub prywatnością. Mechanizmy egzekwowania polityki stosują zasady filtrowania, zabezpieczeń i/lub sanityzacji w odniesieniu do istotnych dla polityki części składowych informacji w celu ułatwienia egzekwowania przepływu przed przekazaniem takich informacji do różnych domen bezpieczeństwa.

Zabezpieczenia powiązane: Brak.

(14) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | POLITYKA STOSOWANIA FILTRÓW BEZPIECZEŃSTWA LUB OCHRONY PRYWATNOŚCI

Podczas przesyłania informacji pomiędzy różnymi domenami bezpieczeństwa, należy wdrożyć [***Realizacja: filtry bezpieczeństwa zdefiniowane przez organizację lub filtry polityki prywatności***] **wymagając w pełni określonych formatów, które ograniczają strukturę i zawartość danych.**

Omówienie: Struktura danych i ograniczenia dotyczące treści zmniejszają zakres potencjalnie złośliwych lub nieakceptowanych treści w operacjach między domenowych. Filtry bezpieczeństwa lub polityki prywatności, które ograniczają struktury danych, obejmują ograniczanie rozmiarów plików i długości pól. Filtry zasad dotyczących zawartości danych obejmują formaty kodowania zestawów znaków, ograniczanie pól danych znaków wyłącznie do znaków alfanumerycznych, zakaz stosowania znaków specjalnych oraz zatwierdzanie struktur schematów.

Zabezpieczenia powiązane: Brak.

(15) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | WYKRYWANIE INFORMACJI NIEAKCEPTOWANYCH

Przy przekazywaniu informacji pomiędzy różnymi domenami bezpieczeństwa należy zbadać informacje pod kątem obecności [Realizacja: *zdefiniowane przez organizację informacje jako nieakceptowalne*] i zakazać przekazywania takich

informacji zgodnie z [***Realizacja: zdefiniowana przez organizację polityka bezpieczeństwa lub prywatności***]**.**

Omówienie: Nieakceptowalne informacje obejmują złośliwy kod, informacje, które nie nadają się do uwolnienia z sieci źródłowej lub kod wykonywalny, który może zakłócić lub uszkodzić usługi lub systemy w sieci docelowej.

Zabezpieczenia powiązane: SI-3.

(16) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | PRZEKAZYWANIE INFORMACJI POMIĘDZY SYSTEMAMI

[Wycofane: Włączone do AC-4].

(17) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | UWIERZYTELNIANIE DOMEN

Unikalna identyfikacja i uwierzytelnianie punktów źródłowych i docelowych przez [***Wybór (jeden lub więcej): organizacja; system; aplikacja; usługa; osoba***] **w celu przekazywania informacji.**

Omówienie: Atrybucja (przypisanie danego działania do konkretnego podmiotu) jest krytycznym elementem koncepcji bezpieczeństwa i ochrony prywatności operacji. Umiejętność identyfikacji punktów źródłowych i docelowych przy przepływie informacji w systemach pozwala na rekonstrukcję przebiegu zdarzeń i zachęca do przestrzegania zasad poprzez przypisywanie naruszeń zasad do konkretnych organizacji lub osób. Skuteczne uwierzytelnianie domen wymaga, aby etykiety systemów rozróżniały systemy, organizacje i osoby zaangażowane w przygotowywanie, wysyłanie, otrzymywanie lub rozpowszechnianie informacji.

Atrybucja pozwala również organizacjom na lepsze utrzymanie ciągłości przetwarzania danych osobowych, ponieważ dane te przepływają przez systemy, co może ułatwić śledzenie zgód, a także korygowanie, usuwanie lub uzyskiwanie dostępu do danych otrzymywanych od tych osób.

Zabezpieczenia powiązane: IA-2, IA-3, IA-9.

(18) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | POWIAZANIE ATRYBUTÓW BEZPIECZEŃSTWA

[Wycofane: Włączone do AC-16].

(19) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | UWIERZYTELNIANIE METADANYCH

Podczas przesyłania informacji pomiędzy różnymi domenami bezpieczeństwa, należy wdrożyć [***Realizacja: filtry bezpieczeństwa zdefiniowane przez organizację lub filtry polityki prywatności***] **dotyczące metadanych.**

Omówienie: Wszystkie informacje (w tym metadane i dane, do których odnoszą się metadane) podlegają filtrowaniu i kontroli. Niektóre organizacje dokonują rozróżnienia między metadanymi, a zawartością danych (tj. tylko tych danych, do których odnoszą się metadane). Inne organizacje nie dokonują takiego rozróżnienia i uznają metadane i dane, do których odnoszą się metadane, za część ładunku danych.

Zabezpieczenia powiązane: Brak.

(20) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | ZATWIERDZONE ROZWIĄZANIA BEZPIECZEŃSTWA

Stosowanie [***Realizacja: zdefiniowanych przez organizację rozwiązań w zatwierdzonych konfiguracjach***] **do kontroli przepływu** [***Realizacja: zdefiniowanych przez organizację informacji***] **pomiędzy domenami bezpieczeństwa.**

Omówienie: Organizacje definiują zatwierdzone rozwiązania i konfiguracje w polityce i wytycznych dotyczących różnych domen bezpieczeństwa, zgodnie z rodzajami przepływu informacji pomiędzy różnymi kategoriami klasyfikacji.

Zabezpieczenia powiązane: Brak.

(21) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | FIZYCZNA LUB LOGICZNA SEPARACJA PRZEPŁYWÓW INFORMACJI

Logiczne lub fizyczne rozdzielenie przepływów informacji przy użyciu [***Realizacja: zdefiniowanych przez organizację mechanizmów i/lub technik***] **w celu osiągnięcia** [***Realizacja: zdefiniowanego przez organizację wymaganego rozdzielenia według typów informacji***]**.**

Omówienie: Egzekwowanie rozdzielenia przepływów informacji związanych z określonymi typami danych może wzmocnić ochronę poprzez zapewnienie, że informacje nie są mieszane podczas tranzytu oraz poprzez umożliwienie kontroli przepływu za pomocą ścieżek transmisji, które nie są osiągalne w inny sposób. Rodzaje informacji, które można rozdzielić, obejmują przychodzący i wychodzący ruch sieciowy, żądania usług i odpowiedzi na nie oraz informacje o różnym wpływie na bezpieczeństwo lub różnych poziomach klasyfikacji.

Zabezpieczenia powiązane: SC-32.

(22) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | TYLKO DOSTĘP

Zapewnienie dostępu z jednego urządzenia do platform obliczeniowych, aplikacji lub danych znajdujących się w wielu różnych domenach bezpieczeństwa, przy jednoczesnym uniemożliwieniu przepływu informacji pomiędzy różnymi domenami bezpieczeństwa.

Omówienie: System zapewnia użytkownikom możliwość dostępu do każdej z podłączonych domen bezpieczeństwa, nie dostarczając żadnych mechanizmów pozwalających użytkownikom na przesyłanie danych lub informacji pomiędzy różnymi domenami bezpieczeństwa. Przykładem rozwiązania opartego wyłącznie na dostępie jest terminal, który zapewnia użytkownikom dostęp do informacji o różnych klauzulach bezpieczeństwa przy jednoczesnym zachowaniu ich odrębności.

Zabezpieczenia powiązane: Brak.

(23) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | MODYFIKACJA INFORMACJI, KTÓRYCH NIE MOŻNA UDOSTĘPNIAĆ

Podczas przesyłania informacji pomiędzy różnymi domenami bezpieczeństwa należy zmodyfikować informacje, które nie mogą zostać udostępnione, poprzez wdrożenie [***Realizacja: działanie modyfikacyjne zdefiniowane przez organizację***]**.**

Omówienie: Modyfikacja informacji, które nie są udostępniane, może pomóc w zapobieganiu wyciekowi danych lub atakowi, gdy informacje są przenoszone między zabezpieczonymi domenami. Działania modyfikacyjne obejmują maskowanie, permutację, zmianę, usuwanie lub poprawki.

Zabezpieczenia powiązane: Brak.

(24) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | WEWNĘTRZNY ZNORMALIZOWANY FORMAT

Podczas przesyłania informacji pomiędzy różnymi domenami bezpieczeństwa, należy przetworzyć przychodzące dane do wewnętrznego, znormalizowanego formatu i odtworzyć je tak, aby były zgodne z zamierzoną specyfikacją.

Omówienie: Przekształcanie danych w znormalizowane formy jest jednym z najbardziej efektywnych mechanizmów powstrzymywania złośliwych ataków i różnorodnych typów eksfiltracji danych.

Zabezpieczenia powiązane: Brak.

(25) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | SANITYZACJA DANYCH

Podczas przesyłania informacji pomiędzy różnymi domenami bezpieczeństwa, należy oczyścić dane, aby zminimalizować [***Wybór (jedno lub więcej): dostarczanie złośliwej zawartości, nadzorowanie i zabezpieczanie przed złośliwym kodem, rozszerzenie złośliwego kodu i danych zakodowanych w steganografii; wyciek wrażliwych informacji***] ***zgodnie z*** **[Realizacja:** ***polityka określona przez organizację*****]].**

Omówienie: Sanityzacja danych to proces nieodwracalnego usunięcia lub zniszczenia danych zapisanych na urządzeniu pamięci (np. na dysku twardym, pamięci flash/dyskach półprzewodnikowych, urządzeniach przenośnych, płytach CD i DVD) lub w formie wydruku.

Zabezpieczenia powiązane: MP-6.

(26) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | AUDYT DZIAŁAŃ FILTRUJĄCYCH

Podczas przesyłania informacji pomiędzy różnymi domenami bezpieczeństwa, rejestrować i audytować działania i wyniki filtrowania treści filtrowanych informacji.

Omówienie: Filtrowanie treści jest procesem sprawdzania informacji, ponieważ przepływa ona przez rozwiązania między domenowe, określając, czy informacje te spełniają wcześniej określone zasady. Akcje filtrowania zawartości i wyniki działań filtrujących są rejestrowane w odniesieniu do poszczególnych wiadomości, aby zapewnić, że zostały zastosowane właściwe działania filtrujące. Raporty filtrowania zawartości są wykorzystywane do pomocy w rozwiązywaniu problemów poprzez, na przykład, określenie, dlaczego zawartość wiadomości została zmodyfikowana i/lub dlaczego proces filtrowania zakończył się niepowodzeniem. Zdarzenia audytowe są zdefiniowane w zabezpieczeniu AU-2. Zapisy audytowe generowane są w zabezpieczeniu AU-12.

Zabezpieczenia powiązane: AU-2, AU-3, AU-12.

(27) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | REDUNDANTNE / NIEZALEŻNE MECHANIZMY FILTRACJI

Podczas przesyłania informacji pomiędzy różnymi domenami bezpieczeństwa, należy wdrożyć rozwiązania filtrowania treści, które zapewniają redundantne i niezależne mechanizmy filtrowania dla każdego typu danych.

Omówienie: Filtrowanie treści jest procesem sprawdzania informacji, ponieważ przepływa ona przez rozwiązanie między domenowe i określa, czy informacje spełniają wcześniej określone zasady. Redundantne i niezależne filtrowanie zawartości eliminuje pojedynczy punkt niepowodzenia systemu filtrowania. Niezależność jest definiowana, jako implementacja filtra treści, który wykorzystuje inną bazę kodową i obsługujące ją biblioteki (np. dwa filtry JPEG wykorzystujące biblioteki JPEG różnych producentów) oraz wiele niezależnych procesów systemowych.

Zabezpieczenia powiązane: Brak.

(28) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | KASKADOWY FILTR TREŚCI

Podczas przesyłania informacji pomiędzy różnymi domenami bezpieczeństwa należy wdrożyć kaskadowy filtr liniowy treści, który jest egzekwowany za pomocą uznaniowych i obowiązkowych kontroli dostępu.

Omówienie: Filtrowanie treści jest procesem sprawdzania informacji przenikającej przez rozwiązania między domenowe i określa, czy informacje te spełniają wcześniej określone zasady. Użycie kaskadowych filtrów liniowych zawartości zapewnia, że procesy filtrowania są nieobejściowe i zawsze wywoływane. Ogólnie rzecz biorąc, zastosowanie architektur wykorzystujących filtrowanie równoległe do filtrowania zawartości treści pojedynczego typu danych niesie ze sobą problemy z obejściem i brakiem możliwości wywołania.

Zabezpieczenia powiązane: Brak.

(29) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | SILNIKI ARANŻACJI FILTROWANIA

Podczas przesyłania informacji pomiędzy różnymi domenami bezpieczeństwa, należy stosować silniki filtrujące zawartość, aby zapewnić, że:

(a) Mechanizmy filtrowania treści skutecznie realizują wykonywanie filtrowania bez błędów; oraz

(b) Czynności w zakresie filtrowania zawartości występują we właściwej kolejności i są zgodne z [***Realizacja: polityka określona przez organizację***]**.**

Omówienie: Filtrowanie treści to proces sprawdzania informacji w trakcie przechodzenia przez rozwiązanie między domenowe i określania, czy informacje te spełniają wcześniej zdefiniowaną politykę bezpieczeństwa. Aparat aranżacji (orkiestracji) koordynuje sekwencjonowanie czynności (ręczne i automatyczne) w procesie filtrowania treści. Błędy są definiowane, jako anomalie działania lub nieoczekiwane zakończenie procesu filtrowania treści. To nie to samo, co filtr powodujący przenikanie zawartości z powodu niezgodności z zasadami. Raporty z filtrowania zawartości są powszechnie stosowanym mechanizmem zapewniającym, że oczekiwane działania filtrujące zostaną pomyślnie zakończone.

Zabezpieczenia powiązane: Brak.

(30) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | MECHANIZMY FILTRUJĄCE WYKORZYSTUJĄCE PROCESY WIELEKROTNE

Podczas przesyłania informacji pomiędzy różnymi domenami bezpieczeństwa, należy wdrożyć mechanizmy filtrowania treści przy użyciu wielu procesów.

Omówienie: Zastosowanie wielu procesów do wdrożenia mechanizmów filtrowania treści zmniejsza prawdopodobieństwo wystąpienia pojedynczego punktu awarii.

Zabezpieczenia powiązane: Brak.

(31) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | ZAPOBIEGANIE PRZENOSZENIU NIEWŁAŚCIWYCH TREŚCI

Podczas przesyłania informacji pomiędzy różnymi domenami bezpieczeństwa, należy zapobiegać przenoszeniu niesprawdzonych treści do domeny odbiorczej.

Omówienie: Zawartość, która nie została sprawdzona podczas filtrowania, może uszkodzić system, jeśli zostanie przeniesiona do domeny odbiorczej.

Zabezpieczenia powiązane: Brak.

(32) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | WYMOGI DOTYCZĄCE PROCESU PRZEKAZYWANIA INFORMACJI

Podczas przesyłania informacji pomiędzy różnymi domenami bezpieczeństwa, proces, który przenosi informacje pomiędzy kaskadami filtracyjnymi:

(a) Nie filtruje treści wiadomości;

(b) Weryfikuje metadane filtrujące;

(c) Zapewnia, że zawartość związana z weryfikacją metadanych została pomyślnie poddana filtrowaniu; oraz

(d) Przekazuje zawartość do docelowego filtra kaskadowego.

Omówienie: Procesy przekazujące informacje pomiędzy kaskadami filtracyjnymi mają minimalną złożoność i stosowną funkcjonalność, aby zapewnić ich prawidłowe działanie.

Zabezpieczenia powiązane: Brak.

Referencje: [NIST SP 800-160-1], [NIST SP 800-162], [NIST SP 800-178], [IR 8112].

AC-5 ROZDZIAŁ OBOWIĄZKÓW

Zabezpieczenie podstawowe:

a. Określenie i udokumentowanie [*Realizacja: określone organizacyjnie obowiązki osób wymagających rozdzielenia obowiązków*]; oraz

b. Zdefiniowanie uprawnień dostępu do systemu w celu wsparcia rozdzielenia obowiązków.

Omówienie: Rozdzielenie obowiązków dotyczy możliwości nadużywania autoryzowanych przywilejów i pomaga zmniejszyć ryzyko nieuczciwej działalności bez stosowania zmowy. Rozdzielenie obowiązków obejmuje podział zadań lub funkcji biznesowych i funkcji wsparcia pomiędzy różne osoby lub role, prowadzenie funkcji wsparcia systemu z różnymi osobami oraz zapewnienie, że pracownicy ochrony, którzy administrują funkcjami kontroli dostępu, nie będą również administrować funkcjami audytu. Ponieważ rozdzielenie obowiązków może obejmować obszary systemów i aplikacji, przy opracowywaniu polityki rozdzielenia obowiązków organizacje biorą pod uwagę całość systemów i komponentów systemowych. Podział obowiązków jest egzekwowany poprzez działania w zakresie zarządzania kontami w zabezpieczeniu AC-2, mechanizmami kontroli dostępu w AC-3 oraz działaniami w zakresie zarządzania tożsamością zawartymi w zabezpieczeniach IA-2, IA-4 i IA-12.

Zabezpieczenia powiązane: AC-2, AC-3, AC-6, AU-9, CM-5, CM-11, CP-9, IA-2, IA-4, IA-5, IA-12, MA-3, MA-5, PS-2, SA-8, SA-17.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

AC-6 ZASADA WIEDZY KONIECZNEJ

Zabezpieczenie podstawowe: Stosowanie zasadę wiedzy koniecznej (jak najmniejszych uprawnień), zezwalając tylko na autoryzowane dostępy użytkownikom (lub procesom działającym w ich imieniu), które są niezbędne do realizacji przydzielonych zadań organizacyjnych.

Omówienie: Organizacje stosują zasadę wiedzy koniecznej w zakresie przydzielonych obowiązków i konkretnych systemów. Zasada wiedzy koniecznej jest również stosowana w odniesieniu do procesów systemowych, zapewniając dostęp do systemów i funkcjonowanie procesów na poziomie uprawnień nie wyższym niż niezbędny do realizacji misji organizacji lub funkcji biznesowych. Organizacje uznają tworzenie dodatkowych procesów, ról i kont za niezbędne do uzyskania najmniejszych uprawnień. Organizacje stosują zasadę wiedzy koniecznej w zakresie tworzenia, wdrażania i eksploatacji systemów organizacyjnych.

Zabezpieczenia powiązane: AC-2, AC-3, AC-5, AC-16, CM-5, CM-11, PL-2, PM-12, SA-8, SA-15, SA-17, SC-38.

Zabezpieczenia rozszerzone:

(1) ZASADA WIEDZY KONIECZNEJ | UPOWAŻNIONY DOSTĘP DO FUNKCJI BEZPIECZEŃSTWA

Autoryzacja dostępu dla [***Realizacja: osoby lub role zdefiniowane przez organizację***] **do*:***

(a) [***Realizacja: funkcje bezpieczeństwa zdefiniowane przez organizację (wdrożone w sprzęcie, oprogramowaniu i oprogramowaniu układowym)***]***;*** **oraz**

(b) [Realizacja: ***informacje dotyczące bezpieczeństwa zdefiniowane przez organizację*****].**

Omówienie: Funkcje bezpieczeństwa obejmują zakładanie kont systemowych, konfigurowanie autoryzacji dostępu (tj. uprawnień, przywilejów), konfigurowanie

ustawień dla zdarzeń, które mają być kontrolowane oraz ustalanie parametrów wykrywania włamań. Informacje istotne dla bezpieczeństwa obejmują reguły filtrowania routerów lub zapór sieciowych, parametry konfiguracyjne usług bezpieczeństwa, informacje o zarządzaniu kluczami kryptograficznymi oraz listy kontroli dostępu. Upoważnieni pracownicy obejmują administratorów bezpieczeństwa, administratorów systemów, personel ds. bezpieczeństwa systemów, programistów systemów i innych uprzywilejowanych użytkowników.

Zabezpieczenia powiązane: AC-17, AC-18, AC-19, AU-9, PE-2.

(2) ZASADA WIEDZY KONIECZNEJ | NIEUPRZYWILEJOWANY DOSTĘP DO FUNKCJI NIEZWIĄZANYCH Z BEZPIECZEŃSTWEM

Wymóg, aby użytkownicy kont (lub ról) systemowych z dostępem do [***Realizacja: zdefiniowane przez organizację funkcje bezpieczeństwa lub informacje istotne dla bezpieczeństwa***] **korzystali z nieuprzywilejowanych kont lub ról przy dostępie do funkcji niezwiązanych z bezpieczeństwem.**

Omówienie: Wymóg korzystania z nieuprzywilejowanych kont w przypadku dostępu do funkcji niezwiązanych z bezpieczeństwem ogranicza ujawnienie w przypadku korzystania z uprzywilejowanych kont lub ról. Włączenie ról odnosi się do sytuacji, w których organizacje wdrażają zasady kontroli dostępu, takie jak zabezpieczenie dostępu oparta na rolach, oraz w których zmiana roli zapewnia taki sam stopień pewności przy zmianie uprawnień dostępu dla użytkownika i procesów działających w jego imieniu, jaki zapewniłaby zmiana między kontem uprzywilejowanym, a nieuprzywilejowanym.

Zabezpieczenia powiązane: AC-17, AC-18, AC-19, PL-4.

(3) ZASADA WIEDZY KONIECZNEJ | DOSTĘP SIECIOWY DO UPRZYWILEJOWANYCH POLECEŃ

Zezwolenie na dostęp do sieci [***Realizacja: zdefiniowanych przez organizację poleceń uprzywilejowanych***] **tylko dla** [***Realizacja: zdefiniowanych przez***

organizację istotnych potrzeb operacyjnych] **i udokumentowanie uzasadnienia tego dostępu w planie bezpieczeństwa systemu.**

Omówienie: Dostęp sieciowy to dowolny dostęp poprzez połączenie sieciowe, realizowane w miejsce dostępu lokalnego (w którym użytkownik jest fizycznie obecny przy urządzeniu).

Zabezpieczenia powiązane: AC-17, AC-18, AC-19.

(4) ZASADA WIEDZY KONIECZNEJ | ODDZIELNE DOMENY PRZETWARZANIA

Udostępnienie oddzielnych domen przetwarzania w celu umożliwienia bardziej precyzyjnego przydzielania uprawnień użytkownikom.

Omówienie: Udostępnienie oddzielnych domen przetwarzania w celu dokładniejszego przydzielania uprawnień użytkownikom obejmuje: wykorzystanie technik wirtualizacji umożliwiających dodatkowe uprawnienia użytkownikom w obrębie maszyny wirtualnej przy jednoczesnym ograniczeniu uprawnień do innych maszyn wirtualnych lub do bazowej maszyny fizycznej; wdrożenie oddzielnych domen fizycznych; oraz zastosowanie mechanizmów separacji domen sprzętowych lub programowych.

Zabezpieczenia powiązane: AC-4, SC-2, SC-3, SC-30, SC-32, SC-39.

(5) ZASADA WIEDZY KONIECZNEJ | UPRZYWILEJOWANE KONTA

Ograniczanie w systemie uprzywilejowanych kont do [Realizacja: *personel lub role zdefiniowane przez organizację*].

Omówienie: Konta uprzywilejowane, w tym konta superużytkowników, są zwykle opisywane, jako administrator systemu dla różnych typów komercyjnych systemów operacyjnych dostępnych w sprzedaży. Ograniczenie uprzywilejowanych kont do określonego personelu lub ról uniemożliwia zwykłemu użytkownikowi dostęp do uprzywilejowanych informacji lub funkcji. Organizacje mogą dokonać rozróżnienia w stosowaniu ograniczania uprzywilejowanych kont między dozwolonymi uprawnieniami dla kont lokalnych

i dla kont domenowych, pod warunkiem, że zachowują możliwość kontrolowania konfiguracji systemu pod kątem kluczowych parametrów i w innych przypadkach, gdy jest to konieczne, do wystarczającego ograniczenia ryzyka.

Zabezpieczenia powiązane: IA-2, MA-3, MA-4.

(6) ZASADA WIEDZY KONIECZNEJ | UPRZYWILEJOWANY DOSTĘP PRZEZ UŻYTKOWNIKÓW NIEORGANIZACYJNYCH

Zakazać uprzywilejowanego dostępu do systemu przez użytkowników niebędącym pracownikami (współpracownikami) organizacji.

Omówienie: Użytkownik organizacyjny to pracownik lub osoba uznana przez organizację za posiadającą równoważny status pracownika. Użytkownikami organizacyjnymi są wykonawcy, zaproszeni badacze lub osoby wyszczególnione w innych organizacjach. Użytkownik niebędący użytkownikiem organizacyjnym to użytkownik, który nie jest pracownikiem (współpracownikiem) organizacji. Zasady i procedury przyznawania równorzędnego statusu pracowników osobom fizycznym obejmują zasadę wiedzy koniecznej, obywatelstwo i stosunek do organizacji.

Zabezpieczenia powiązane: AC-18, AC-19, IA-2, IA-8.

(7) ZASADA WIEDZY KONIECZNEJ | PRZEGLĄD UPRAWNIEŃ UŻYTKOWNIKA

(a) Przeglądanie z częstotliwością [***Realizacja: częstotliwość zdefiniowana przez organizację***] **uprawnień przypisanych do** [***Realizacja: role lub klasy użytkowników zdefiniowane przez organizację***] **w celu potwierdzenia potrzeby takich uprawnień; oraz**

(b) Przeniesienie lub usunięcie uprawnień, jeśli to konieczne, w celu właściwego odzwierciedlenia misji organizacji i potrzeb biznesowych.

Omówienie: Potrzeba posiadania określonych uprawnień przez użytkownika może z czasem ulec zmianie, aby odzwierciedlić zmiany w misji i funkcjach biznesowych organizacji, środowiskach działania, technologiach lub zagrożeniach

związanych z działalnością organizacji. Niezbędny jest okresowy przegląd przydzielonych uprawnień użytkownikowi w celu ustalenia, czy przesłanki do ich nadania pozostają aktualne. Jeśli nie da się tego ponownie zweryfikować, organizacje podejmują odpowiednie działania naprawcze.

Zabezpieczenia powiązane: CA-7.

(8) ZASADA WIEDZY KONIECZNEJ | POZIOMY UPRAWNIEŃ DO WYKONYWANIA KODU

Uniemożliwianie uruchamiania poniższego oprogramowania na wyższych poziomach uprawnień niż użytkownicy uruchamiający oprogramowanie: [Realizacja: *oprogramowanie zdefiniowane przez organizację*].

Omówienie: W pewnych sytuacjach aplikacje lub programy muszą być wykonywane z podwyższonymi uprawnieniami, aby mogły wykonywać wymagane funkcje. Jednakże, w zależności od funkcjonalności i konfiguracji oprogramowania, jeżeli uprawnienia wymagane do wykonania są na wyższym poziomie niż uprawnienia przydzielone organizacyjnym użytkownikom wywołującym takie aplikacje lub programy, użytkownicy ci mogą pośrednio uzyskać większe uprawnienia niż te, które zostały im przydzielone.

Zabezpieczenia powiązane: Brak.

(9) ZASADA WIEDZY KONIECZNEJ | KONTROLA WYKORZYSTANIA UPRZYWILEJOWANYCH FUNKCJI

Rejestrowanie wykonywania funkcji uprzywilejowanych.

Omówienie: Nadmierne korzystanie z uprzywilejowanych funkcji, umyślne lub nieumyślne, przez upoważnionych użytkowników lub przez nieupoważnione podmioty zewnętrzne, które naruszyły konta systemowe, jest poważnym i ciągłym problemem i może mieć istotny negatywny wpływ na organizacje. Rejestrowanie i analizowanie korzystania z funkcji uprzywilejowanych jest jednym ze sposobów na wykrycie takiego nadużycia, a tym samym na ograniczenie ryzyka

związanego z zagrożeniami wewnętrznymi i zaawansowanym zagrożeniem trwałym (*ang. advanced persistent threat - APT*)[37].

Zabezpieczenia powiązane: AU-2, AU-3, AU-12.

(10) ZASADA WIEDZY KONIECZNEJ | ODMOWA WYKONYWANIA PRZEZ NIEUPRZYWILEJOWANYCH UŻYTKOWNIKÓW UPRZYWILEJOWANYCH FUNKCJI

Uniemożliwianie nieuprzywilejowanym użytkownikom korzystanie z uprzywilejowanych funkcji.

Omówienie: Do uprzywilejowanych funkcji należą: wyłączanie, obchodzenie lub zmienianie wdrożonych środków bezpieczeństwa lub ochrony prywatności, zakładanie kont systemowych, przeprowadzanie sprawdzania integralności systemu oraz administrowanie działaniami związanymi z zarządzaniem kluczami kryptograficznymi. Użytkownicy nieuprzywilejowani to osoby, które nie posiadają odpowiednich uprawnień. Do uprzywilejowanych funkcji, które wymagają ochrony przed nieuprzywilejowanymi użytkownikami, należą mechanizmy wykrywania i zapobiegania włamaniom lub mechanizmy ochrony przed złośliwym kodem.

Zapobieganie wykonywaniu przez nieuprzywilejowanych użytkowników uprzywilejowanych funkcji jest egzekwowane przez zabezpieczenie AC-3.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

[37] Cyberprzestępcy wybierają sobie na ofiarę jeden konkretny podmiot, np. instytucję lub przedsiębiorstwo. W tym konkretnym podmiocie, po wstępnej inwigilacji, bardzo często wybierają jedną konkretną osobę, która stanie się wektorem ataku i posłuży do tego, by na starannie wyselekcjonowanej ofierze zarobić możliwie jak najwięcej.

AC-7 NIEUDANE PRÓBY LOGOWANIA

Zabezpieczenie podstawowe:

a. Egzekwowanie limitu [Realizacja: *wielkość zdefiniowana przez organizację*] następujących po sobie nieważnych prób logowania przez użytkownika podczas [*Realizacja: okres czasu zdefiniowany przez organizację*]; oraz

b. Automatycznie [*Wybór (jeden lub więcej): zablokować konto lub węzeł dla* [*Realizacja: okres czasu określony przez organizację*]; *zablokować konto lub węzeł do czasu uwolnienia przez administratora; opóźnić następny monit o zalogowanie na* [*Realizacja: algorytm opóźnienia określony przez organizację*]; *powiadomić administratora systemu; podjąć inne* [*Realizacja: czynność określona przez organizację*]] w przypadku przekroczenia maksymalnej liczby nieudanych prób.

Omówienie: Potrzeba ograniczania nieudanych prób logowania i podejmowania dalszych stosownych działań w przypadku przekroczenia maksymalnej liczby prób ma zastosowanie niezależnie od tego, czy logowanie odbywa się za pośrednictwem połączenia lokalnego czy sieciowego. Ze względu na możliwość odmowy usługi, automatyczne blokady inicjowane przez systemy są zazwyczaj tymczasowe i automatycznie zwalniane po wcześniej określonym, zdefiniowanym przez organizację okresie czasu. W przypadku wyboru algorytmu opóźniającego, organizacje mogą stosować różne algorytmy dla konkretnych komponentów systemu w oparciu o możliwości tych komponentów. Odpowiedzi na nieudane próby logowania mogą być zaimplementowane na poziomie systemu operacyjnego i aplikacji. Zdefiniowane przez organizację działania, które mogą być podejmowane po przekroczeniu dozwolonej liczby następujących po sobie nieudanych prób logowania, obejmują: nakłanianie użytkownika do udzielenia odpowiedzi na specyficzne (niejawne) pytania weryfikacyjne (oprócz podania nazwy użytkownika i hasła), wywołanie trybu blokady z ograniczonymi możliwościami użytkownika (zamiast pełnej blokady), umożliwienie użytkownikom logowanie się

tylko z określonych adresów IP, wymaganie CAPTCHA[38] w celu zapobiegania atakom automatycznym lub zastosowanie profili użytkowników takich jak lokalizacja, pora dnia, adres IP, urządzenie lub adres MAC (*ang. Media Access Control*). Jeśli w celu zapewnienia dostępności automatyczna blokada systemu lub wykonanie algorytmu opóźniającego nie jest zaimplementowane, organizacje rozważają połączenie innych działań, które pomogą zapobiec brutalnym atakom z użyciem siły. Ponadto, organizacje mogą poprosić użytkowników o odpowiedź na specyficzne pytania weryfikujace, zanim liczba dozwolonych nieudanych prób logowania zostanie przekroczona. Automatyczne odblokowanie konta po określonym czasie jest z reguły niedozwolone. Wyjątki mogą być jednak wymagane ze względu na misję operacyjną lub potrzebę organizacji.

Zabezpieczenia powiązane: AC-2, AC-9, AU-2, AU-6, IA-5.

Zabezpieczenia rozszerzone:

(1) NIEUDANE PRÓBY LOGOWANIA | AUTOMATYCZNE ZAMKNIĘCIE KONTA

[Wycofane: Włączone do AC-7].

(2) NIEUDANE PRÓBY LOGOWANIA | USUWANIE INFORMACJI Z URZĄDZEŃ PRZENOŚNYCH

Czyszczenie lub wymazywanie informacji z [Realizacja: *urządzenia przenośne określone przez organizację*] *w* oparciu o [*Realizacja: wymagania i techniki czyszczenia lub kasowania określone przez organizację*] po następujących po sobie, nieudanych próbach logowania urządzenia [Realizacja: *ilość określona przez organizację*].

Omówienie: Urządzenie przenośne jest urządzeniem obliczeniowym o niewielkich rozmiarach, które może być przenoszone przez pojedynczą osobę; jest

[38] CAPTCHA *(ang. Completely Automated Public Turing test to tell Computers and Humans Apart)* –rodzaj techniki stosowanej, jako zabezpieczenie na stronach www, celem której jest dopuszczenie do przesłania danych tylko wypełnionych przez człowieka.

przeznaczone do działania bez fizycznego podłączenia do systemu (połączenie sieciowe); posiada lokalne, nieusuwalne lub usuwalne miejsce przechowywania danych; oraz zawiera niezależne źródło zasilania. Czyszczenie lub kasowanie urządzenia dotyczy wyłącznie urządzeń przenośnych, dla których określona jest przez organizację liczba nieudanych logowań. Logowanie przeprowadzane jest do urządzenia przenośnego, a nie do jakiegokolwiek konta w urządzeniu. Udane logowanie do kont w urządzeniach przenośnych powoduje wyzerowanie liczby nieudanych logowań. Czyszczenie lub wymazywanie może być zbędne, jeśli informacje na urządzeniu są chronione za pomocą wystarczająco silnych mechanizmów szyfrujących.

Zabezpieczenia powiązane: AC-19, MP-5, MP-6.

(3) NIEUDANE PRÓBY LOGOWANIA | OGRANICZANIE PRÓB LOGOWANIA BIOMETRYCZNEGO

Ograniczyć liczbę nieudanych prób logowania biometrycznego do [***Realizacja: liczba prób definiowana przez organizację***]**.**

Omówienie: Biometria ma charakter probabilistyczny. Na zdolność do skutecznego uwierzytelniania może wpływać wiele czynników, w tym dopasowanie wydajności i mechanizmy wykrywania ataków wykorzystujących techniki prezentacji. Organizacje wybierają odpowiednią liczbę prób podejmowanych przez użytkowników w oparciu o zdefiniowane organizacyjnie czynniki.

Zabezpieczenia powiązane: IA-3.

(4) NIEUDANE PRÓBY LOGOWANIA | UŻYCIE ALTERNATYWNEGO CZYNNIKA UWIERZYTELNIANIA

(a) Zezwolenie na użycie [***Realizacja: zdefiniowanych przez organizację czynników uwierzytelniających***]**, które różnią się od podstawowych**

czynników uwierzytelniających, po przekroczeniu liczby zdefiniowanych przez organizację kolejnych nieważnych prób logowania; oraz

(b) Egzekwowanie limitu [Realizacja: *liczba zdefiniowany przez organizację*] kolejnych nieważnych prób logowania poprzez wykorzystanie przez użytkownika czynników alternatywnych w czasie [***Realizacja: okres czasu zdefiniowany przez organizację***]**.**

Omówienie: Zastosowanie alternatywnych czynników uwierzytelniających wspiera cel dostępności i pozwala użytkownikowi, który został przypadkowo zablokowany, na użycie dodatkowych czynników uwierzytelniających w celu ominięcia blokady.

Zabezpieczenia powiązane: IA-3.

Referencje: [NSC 800-63], [NIST SP 800-124].

AC-8 POWIADOMIENIE O ZASADACH UŻYCIA SYSTEMU

Zabezpieczenie podstawowe:

a. Wyświetlanie [*Realizacja: zdefiniowany przez organizację system używania komunikatu powiadamiającego lub bannera*] użytkownikom przed udzieleniem dostępu do systemu, który zapewnia informacje o prywatności i bezpieczeństwie zgodne z obowiązującymi przepisami prawa, rozporządzeniami, dyrektywami, rozporządzeniami, zasadami, standardami i wytycznymi, oraz potwierdza, że:

   1. Użytkownicy mają dostęp do systemu organizacji;
   2. Korzystanie z systemu może być monitorowane, rejestrowane i poddawane audytowi;
   3. Nieupoważnione korzystanie z systemu jest zabronione i podlega sankcjom karnym i cywilnym; oraz
   4. Korzystanie z systemu oznacza zgodę na monitorowanie i nagrywanie;

b. Zachowywanie komunikatów powiadamiania lub baneru na ekranie do czasu, aż użytkownicy potwierdzą warunki użytkowania i podejmą wyraźne działania w celu zalogowania się lub uzyskania dalszego dostępu do systemu; oraz

c. W systemach publicznie dostępnych:

   1. System wyświetlania wykorzystuje informacje [*Realizacja: warunki zdefiniowane przez organizację*], przed udzieleniem dalszego dostępu do publicznie dostępnego systemu;
   2. System wyświetla ewentualne referencje monitorowania, rejestrowania lub audytu, które są zgodne z zasadami ochrony prywatności dla takich systemów, które generalnie zakazują tych działań; oraz
   3. Załączany jest opis dozwolonych zastosowań systemu.

Omówienie: Powiadomienia o użyciu systemu mogą być realizowane za pomocą komunikatów lub banerów ostrzegawczych wyświetlanych przed zalogowaniem się

do systemu. Powiadomienia o użyciu systemu są wykorzystywane wyłącznie w celu uzyskania dostępu poprzez interfejsy logowania wyłącznie przez osoby. Powiadomienia nie są wymagane, gdy nie istnieją interfejsy logowania przeznaczone wyłącznie dla ludzi. W oparciu o ocenę ryzyka organizacje rozważają, czy do uzyskania dostępu do aplikacji lub innych zasobów systemowych po wstępnym zalogowaniu się do sieci, potrzebne jest dodatkowe powiadomienie o wykorzystaniu systemu, czy też nie. Organizacje rozważają wykorzystanie komunikatów lub banerów z powiadomieniami wyświetlanych w wielu językach w zależności od potrzeb organizacji i danych demograficznych użytkowników systemu. Organizacje mogą konsultować się z inspektorem ochrony danych w celu uzyskania informacji dotyczących komunikatów o ochronie prywatności oraz działem prawnym lub jego odpowiednikiem organizacyjnym w celu dokonania przeglądu prawnego i zatwierdzenia treści banerów ostrzegawczych.

Zabezpieczenia powiązane: AC-14, PL-4, SI-4.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

AC-9 POWIADOMIENIE O POPRZEDNIM ZALOGOWANIU

Zabezpieczenie podstawowe: Po pomyślnym zalogowaniu się do systemu system powinien powiadomić użytkownika o dacie i godzinie ostatniego (poprzedniego) logowania.

Omówienie: Powiadomienie o poprzednim logowaniu ma zastosowanie do dostępu do systemu za pomocą interfejsów użytkownika oraz dostępu do systemów, który występuje w innych typach architektur. Informacja o ostatnim udanym logowaniu pozwala użytkownikowi rozpoznać, czy podana data i godzina są zgodne z ostatnim dostępem użytkownika.

Zabezpieczenia powiązane: AC-7, PL-4.

Zabezpieczenia rozszerzone:

(1) POWIADOMIENIE O POPRZEDNIM ZALOGOWANIU | NIEUDANE LOGOWANIE

Powiadomienie użytkownika, po udanym zalogowaniu, o liczbie nieudanych prób logowania od ostatniego udanego logowania.

Omówienie: Informacja o liczbie nieudanych prób logowania od ostatniego udanego logowania pozwala użytkownikowi rozpoznać, czy liczba nieudanych prób logowania jest zgodna z rzeczywistą liczbą prób logowania użytkownika.

Zabezpieczenia powiązane: Brak.

(2) POWIADOMIENIE O POPRZEDNIM ZALOGOWANIU | UDANE I NIEUDANE LOGOWANIE

Powiadomienie użytkownika, po udanym logowaniu, o liczbie [***Wybór: udane logowanie; nieudane próby logowania; oba przypadki***] **podczas** [***Realizacja: okres czasu określony przez organizację***]**.**

Omówienie: Informacja o liczbie udanych i nieudanych prób logowania w określonym czasie pozwala użytkownikowi rozpoznać, czy liczba i rodzaje prób logowania są zgodne z rzeczywistymi próbami logowania użytkownika.

Zabezpieczenia powiązane: Brak.

(3) POWIADOMIENIE O POPRZEDNIM ZALOGOWANIU | POWIADOMIENIE O ZMIANACH W KONCIE

Powiadomić użytkownika, po pomyślnym zalogowaniu, o zmianach w [Realizacja: *cechy lub parametry konta użytkownika związane z bezpieczeństwem zdefiniowanym przez organizację*] podczas [*Realizacja: okres czasu zdefiniowany przez organizację*].

Omówienie: Informacje o zmianach w koncie dotyczące bezpieczeństwa konta w określonym okresie czasu pozwalają użytkownikom rozpoznać, czy zmiany zostały dokonane bez ich wiedzy.

Zabezpieczenia powiązane: Brak.

(4) POWIADOMIENIE O POPRZEDNIM ZALOGOWANIU | DODATKOWE INFORMACJE DOTYCZĄCE LOGOWANIA

Po pomyślnym zalogowaniu poinformuj użytkownika o następujących dodatkowych informacjach: [***Realizacja: informacje dodatkowe zdefiniowane przez organizację***]**.**

Omówienie: Organizacje mogą określić dodatkowe informacje, które należy podać użytkownikom podczas logowania, w tym lokalizację ostatniego logowania. Lokalizację użytkownika definiuje się jako informacje, które mogą być określone przez systemy, takie jak adresy protokołu internetowego (IP), z których nastąpiło

logowanie w sieci, powiadomienia o lokalnych logowaniach lub identyfikatory urządzeń.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

AC-10 KONTROLA ILOŚCI JEDNOCZESNYCH SESJI

Zabezpieczenie podstawowe: Ograniczanie liczby równoległych sesji dla każdego konta [*Realizacja: konto zdefiniowane przez organizację i/lub typ konta*] do [*Realizacja: liczba równoczesnych sesji zdefiniowana przez organizację*].

Omówienie: Organizacje mogą określić maksymalną liczbę jednoczesnych sesji dla kont systemowych globalnie, według typu konta, według konta lub dowolnej jego kombinacji. Na przykład, organizacje mogą ograniczyć liczbę jednoczesnych sesji dla administratorów systemów lub innych osób pracujących w szczególnie wrażliwych domenach lub aplikacjach o znaczeniu krytycznym. Kontrola jednoczesnych sesji dotyczy ilości równoczesnych sesji dla kont systemowych. Nie dotyczy ona jednak jednoczesnych sesji pojedynczych użytkowników za pośrednictwem wielu kont systemowych.

Zabezpieczenia powiązane: SC-23.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

AC-11 BLOKADA URZĄDZENIA

Zabezpieczenie podstawowe:

a. Zapobieganie dalszemu dostępowi do systemu poprzez [*Wybór (jeden lub więcej): inicjowanie blokady urządzeń po* [*Realizacja: określony przez organizację okres czasu*] *braku aktywności; wymaganie od użytkownika zainicjowania blokady urządzeń przed pozostawieniem systemu bez nadzoru*]; oraz

b. Utrzymywanie blokady urządzenia, dopóki użytkownik nie przywróci dostępu przy użyciu ustalonych procedur identyfikacji i uwierzytelniania.

Omówienie: Blokady urządzeń są tymczasowymi działaniami podejmowanymi w celu uniemożliwienia logicznego dostępu do systemów organizacyjnych, gdy użytkownicy kończą pracę i oddalają się od najbliższego otoczenia tych systemów, ale nie chcą się wylogować ze względu na tymczasowy charakter ich nieobecności. Blokady urządzeń mogą być realizowane na poziomie systemu operacyjnego lub na poziomie aplikacji. Blokada zbliżeniowa może być wykorzystana do zainicjowania blokady urządzenia (np. za pomocą urządzenia z funkcją Bluetooth lub klucza sprzętowego). Blokada urządzenia inicjowana przez użytkownika jest oparta na zachowaniu lub zasadach i jako taka wymaga od użytkownika podjęcia działań fizycznych w celu zainicjowania blokady urządzenia. Blokady urządzeń nie są akceptowalnym substytutem wylogowania się z systemów, np. gdy organizacje wymagają od użytkowników wylogowania się na koniec dnia roboczego.

Zabezpieczenia powiązane: AC-2, AC-7, IA-11, PL-4.

Zabezpieczenia rozszerzone:

(1) BLOKADA URZĄDZENIA | WYGASZACZ EKRANU

Informacje wcześniej widoczne na ekranie zastępowane są wygaszaczem ekranu ukazującym publicznie dostępny obraz.

Omówienie: Wygaszacz ekranu ukrywający wcześniej widoczne na ekranie informacje, może zawierać statyczne lub dynamiczne obrazy, takie jak wzory

używane z wygaszaczami ekranu, obrazy fotograficzne, stałe kolory, zegar, wskaźnik żywotności baterii, lub pusty ekran z zastrzeżeniem, że kontrolowane informacje jawne nie są wyświetlane.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

AC-12 ZAKOŃCZENIE SESJI

Zabezpieczenie podstawowe: Automatyczne zakończenie sesji użytkownika po [*Realizacja: warunki zdefiniowane przez organizację, lub wywołanie zdarzeń wymagających rozłączenia sesji*].

Omówienie: Zakończenie sesji odnosi się do zakończenia sesji logicznych inicjowanych przez użytkownika (w przeciwieństwie do zabezpieczenia SC-10, które odnosi się do zakończenia połączeń sieciowych związanych z sesjami komunikacyjnymi, tj. rozłączenia sieci). Sesja logiczna (dla dostępu lokalnego, sieciowego i zdalnego) jest inicjowana zawsze, gdy użytkownik (lub proces działający w jego imieniu) uzyskuje dostęp do systemu organizacyjnego. Takie sesje użytkowników mogą być zakończone bez przerywania sesji sieciowych. Zakończenie sesji kończy wszystkie procesy związane z sesją logiczną użytkownika z wyjątkiem tych procesów, które zostały specjalnie utworzone przez użytkownika (tj. właściciela sesji), w celu kontynuowania po zakończeniu sesji. Warunki lub zdarzenia wyzwalające, które wymagają automatycznego zakończenia sesji, obejmują określone przez organizację okresy braku aktywności użytkownika, ukierunkowane reakcje na określone rodzaje zdarzeń lub ograniczenia czasowe w użytkowaniu systemu.

Zabezpieczenia powiązane: MA-4, SC-10, SC-23.

Zabezpieczenia rozszerzone:

(1) ZAKOŃCZENIE SESJI | WYLOGOWANIE INICJOWANE PRZEZ UŻYTKOWNIKA

Zapewnienie możliwości wylogowania w przypadku sesji komunikacyjnych inicjowanych przez użytkownika za każdym razem, gdy do uzyskania dostępu do [***Realizacja: zasoby informacyjne zdefiniowane przez organizację***] **wykorzystywane jest uwierzytelnianie.**

Omówienie: Zasoby informacyjne, do których użytkownicy uzyskują dostęp poprzez uwierzytelnienie, obejmują lokalne stacje robocze, bazy danych oraz chronione hasłem strony internetowe lub usługi internetowe.

Zabezpieczenia powiązane: Brak.

(2) ZAKOŃCZENIE SESJI | KOMUNIKAT O ZAKOŃCZENIU SESJI (WYLOGOWANIU)

Wyświetlanie użytkownikom jednoznacznego komunikatu o wylogowaniu, wskazującego na zakończenie uwierzytelnionych sesji komunikacyjnych.

Omówienie: Po zakończeniu uwierzytelnionych sesji uzyskanych w celu dostępu do Internetu, można wyświetlać komunikaty o wylogowaniu. Jednak w przypadku niektórych typów sesji, w tym sesji z protokołem przesyłania plików (FTP), przed zakończeniem sesji systemy zazwyczaj wysyłają wiadomości o wylogowaniu, jako wiadomości końcowe.

Zabezpieczenia powiązane: Brak.

(3) ZAKOŃCZENIE SESJI | KOMUNIKAT OSTRZEGAWCZY O PRZEKROCZENIU LIMITU CZASU

Wyświetlanie użytkownikom jednoznacznego komunikatu wskazującego, że sesja zakończy się w [***Realizacja: czas określony przez organizację do końca sesji***]**.**

Omówienie: W celu zwiększenia użyteczność, należy powiadomić użytkowników o zbliżającym się zakończeniu sesji i zasugerować do kontynuowania sesji. Czas zakończenia aktywnej sesji jest oparty na parametrach zdefiniowanych w zabezpieczeniu podstawowym AC-12.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

AC-13 NADZÓR I PRZEGLĄD KONTROLI DOSTĘPU

[Wycofane: Włączone do AC-2 i AU-6].

AC-14 DZIAŁANIA DOZWOLONE BEZ IDENTYFIKACJI LUB UWIERZYTELNIENIA

Zabezpieczenie podstawowe:

a. Identyfikacja [*Realizacja: zdefiniowanych przez organizację działań użytkownika*], które mogą być wykonywane w systemie bez identyfikacji lub uwierzytelnienia, zgodnie z misją organizacji i funkcjami biznesowymi; oraz

b. Udokumentowanie i przedstawienie uzasadnienia w planie bezpieczeństwa systemu działania użytkowników niewymagające identyfikacji lub uwierzytelnienia.

Omówienie: Określone działania użytkownika mogą być dozwolone bez identyfikacji lub uwierzytelniania, jeśli organizacje ustalą, że identyfikacja i uwierzytelnianie nie są wymagane dla określonych działań użytkownika. Organizacje mogą zezwolić na ograniczoną liczbę działań użytkowników bez identyfikacji lub uwierzytelniania, w tym, gdy osoby korzystają z publicznych stron internetowych lub innych publicznie dostępnych systemów, gdy osoby korzystają z telefonów komórkowych do odbierania połączeń lub gdy odbierane są faksy. Organizacje identyfikują działania, które zazwyczaj wymagają identyfikacji lub uwierzytelnienia, ale mogą, w pewnych okolicznościach, pozwolić na ominięcie mechanizmów identyfikacji lub uwierzytelniania. Takie obejścia mogą mieć miejsce, na przykład, za pomocą fizycznego przełącznika sterowanego programowo, który nakazuje obejście funkcji logowania i jest chroniony przed przypadkowym lub niemonitorowanym użyciem. Zezwolenie na działania bez identyfikacji lub uwierzytelniania nie ma zastosowania do sytuacji, w których identyfikacja i uwierzytelnianie miały już miejsce i nie jest wymagane ich powtarzanie, ale do sytuacji, w których identyfikacja i uwierzytelnianie nie miały jeszcze miejsca. Organizacje mogą zdecydować, że nie zezwalają na działania użytkownika, które mogą być wykonywane w systemach organizacyjnych

bez identyfikacji i uwierzytelniania, a zatem wartość *Przypisanie* w pkt. a. zabezpieczenia AC-14 może być opisana jako "Brak".

Zabezpieczenia powiązane: AC-8, IA-2, PL-2.

Zabezpieczenia rozszerzone: Brak.

(1) DZIAŁANIA DOZWOLONE BEZ IDENTYFIKACJI LUB UWIERZYTELNIANIA | NIEZBĘDNE ZASTOSOWANIA

[Wycofane: Włączone do AC-14].

Referencje: Brak.

AC-15 ZNAKOWANIE AUTOMATYCZNE

[Wycofane: Włączone do MP-3].

AC-16 ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Zabezpieczenie podstawowe:

a. Zapewnienie środków umożliwiających powiązanie [Realizacja: *zdefiniowanych* przez *organizację typów atrybutów bezpieczeństwa i ochrony prywatności*] z [*Realizacja: zdefiniowane przez organizację wartości atrybutów bezpieczeństwa i ochrony prywatności*] w odniesieniu do informacji przechowywanych, przetwarzanych i/lub przekazywanych;

b. Upewnienie się, że skojarzenia atrybutów są tworzone i zachowywane wraz z informacjami;

c. Ustalenie następujących dozwolonych atrybutów dotyczących bezpieczeństwa i ochrony prywatności na podstawie atrybutów zdefiniowanych w zabezpieczeniu rozszerzonym AC-16a dla [*Realizacja: systemy zdefiniowane przez organizację*]: [*Realizacja: atrybuty dotyczące bezpieczeństwa i ochrony prywatności zdefiniowane przez organizację*];

d. Określenie następujących dozwolonych wartości lub zakresów dla każdego z ustalonych atrybutów: [*Realizacja: zdefiniowane przez organizację wartości lub zakresy atrybutów dla ustalonych atrybutów*];

e. Audytowanie zmian w atrybutach; oraz

f. Przeglądanie [*Realizacja: atrybuty bezpieczeństwa i ochrony prywatności zdefiniowane przez organizację*] *pod* kątem możliwości zastosowania, z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*].

Omówienie: Informacje są reprezentowane wewnętrznie w systemach za pomocą abstrakcji znanych, jako struktury danych. Wewnętrzne struktury danych mogą reprezentować różne rodzaje podmiotów, zarówno aktywnych jak i pasywnych. Jednostki aktywne, nazywane również *podmiotami,* są zazwyczaj związane z osobami, urządzeniami lub procesami działającymi w imieniu osób fizycznych. Jednostki pasywne, zwane również *obiektami,* są zazwyczaj związane ze strukturami

danych, takimi jak rekordy, bufory, tabele, pliki, potoki międzyprocesowe i porty komunikacyjne. Atrybuty bezpieczeństwa, będące formą metadanych, są abstrakcjami, które reprezentują podstawowe właściwości lub cechy jednostek aktywnych i pasywnych w odniesieniu do ochrony informacji. Atrybuty ochrony prywatności, które mogą być używane niezależnie lub w połączeniu z atrybutami bezpieczeństwa, reprezentują podstawowe właściwości lub cechy jednostek aktywnych lub pasywnych w odniesieniu do zarządzania informacjami umożliwiającymi identyfikację osób. Atrybuty mogą być w sposób wyraźny lub domyślny powiązane z informacjami zawartymi w systemach organizacyjnych lub komponentach systemu.

Atrybuty mogą być związane z aktywnymi jednostkami (tj. podmiotami), które mogą wysyłać lub odbierać informacje, powodować przepływ informacji między obiektami lub zmieniać stan systemu. Atrybuty te mogą być również powiązane z pasywnymi jednostkami (tj. obiektami), które zawierają lub odbierają informacje. Powiązanie atrybutów z podmiotami i obiektami przez system jest określane jako wiązanie i obejmuje ustawienie wartości atrybutu oraz typu atrybutu.
Atrybuty, w powiązaniu z danymi lub informacjami, umożliwiają egzekwowanie polityki bezpieczeństwa i ochrony prywatności w zakresie kontroli dostępu i kontroli przepływu informacji, w tym ograniczeń dotyczących zatrzymywania danych, dozwolonego wykorzystania informacji umożliwiających identyfikację osób oraz identyfikacji informacji osobowych w ramach obiektów danych. Takie egzekwowanie odbywa się poprzez procesy organizacyjne lub funkcje lub mechanizmy systemowe. Techniki wiązania wdrażane przez systemy wpływają na siłę wiązania informacji. Siła wiązania i pewność związana z technikami wiązania odgrywają ważną rolę w zaufaniu, jakim organizacje cieszą się w procesie egzekwowania przepływu informacji. Techniki wiązania mają wpływ na liczbę i stopień dodatkowych przeglądów wymaganych przez organizacje. Treść lub przypisane wartości atrybutów mogą mieć bezpośredni wpływ na zdolność osób do dostępu do informacji o organizacji.

Organizacje mogą definiować typy atrybutów potrzebnych systemom do obsługi misji lub funkcji biznesowych. Istnieje wiele wartości, które mogą być przypisane do atrybutu bezpieczeństwa. Poprzez określenie dozwolonych zakresów i wartości atrybutów, organizacje zapewniają, że wartości atrybutów są znaczące i istotne. Etykietowanie odnosi się do powiązania atrybutów z podmiotami i obiektami reprezentowanymi przez wewnętrzne struktury danych w systemach. Ułatwia to systemowe egzekwowanie polityki bezpieczeństwa informacji i ochrony prywatności. Oznaczenia obejmują klasyfikację informacji zgodnie z wymogami prawnymi i wymogami zgodności (np. ściśle tajne, tajne, poufne, zastrzeżone, jawne), poziom wpływu informacji; informacje o aktywach o wysokiej wartości, zezwolenia dostępu, narodowość; ochronę cyklu życia danych (tj. szyfrowanie i retencja danych), zezwolenia na przetwarzanie informacji umożliwiających identyfikację osób, w tym indywidualną zgodę na przetwarzanie informacji umożliwiających identyfikację osób, oraz przynależność do wykonawcy. Powiązanym pojęciem z etykietowaniem jest znakowanie. Znakowanie odnosi się do skojarzenia atrybutów z obiektami w formie czytelnej dla człowieka i wyświetlanej na nośnikach systemowych. Znakowanie umożliwia ręczne, proceduralne lub procesowe egzekwowanie polityki bezpieczeństwa informacji i ochrony prywatności. Etykiety bezpieczeństwa i ochrony prywatności mogą mieć taką samą wartość jak oznakowanie nośników (np. ściśle tajne, tajne, poufne, zastrzeżone, jawne). Patrz MP-3 (Oznakowanie nośników).

Zabezpieczenia powiązane: AC-3, AC-4, AC-6, AC-21, AC-25, AU-2, AU-10, MP-3, PE-22, PT-2, PT-3, PT-4, SC-11, SC-16, SI-12, SI-18.

Zabezpieczenia rozszerzone:

(1) ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | DYNAMICZNE KOJARZENIE ATRYBUTÓW

Dynamicznie kojarzy atrybuty bezpieczeństwa i ochrony prywatności z [***Realizacja: zdefiniowane przez organizację podmioty i obiekty***] ***zgodnie z*** **następującą polityką bezpieczeństwa i ochrony prywatności**

tworzenia i łączenia informacji: [***Realizacja: zdefiniowana przez organizację polityka bezpieczeństwa i ochrony prywatności***]**.**

Omówienie: Dynamiczne kojarzenie atrybutów jest właściwe zawsze, gdy charakterystyka bezpieczeństwa lub prywatności informacji zmienia się w czasie. Atrybuty mogą się zmieniać ze względu na kwestie agregacji informacji (tj. cechy poszczególnych elementów danych różnią się od połączonych elementów), zmiany w indywidualnych uprawnieniach dostępu (tj. przywilejach), zmiany w kategorii bezpieczeństwa informacji lub zmiany w polityce bezpieczeństwa lub ochrony prywatności. Atrybuty mogą również zmieniać się w zależności od sytuacji.

Zabezpieczenia powiązane: Brak.

(2) ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | ZMIANY WARTOŚCI ATRYBUTÓW PRZEZ UPOWAŻNIONE OSOBY

Zapewnienie upoważnionym osobom (lub procesom działającym w imieniu osób) możliwości zdefiniowania lub zmiany wartości powiązanych atrybutów bezpieczeństwa i ochrony prywatności.

Omówienie: Zawartość lub przypisane wartości atrybutów mogą mieć bezpośredni wpływ na zdolność osób do dostępu do informacji organizacyjnych. Dlatego ważne jest, aby systemy były w stanie ograniczyć, do uprawnionych osób, możliwość tworzenia lub modyfikowania atrybutów.

Zabezpieczenia powiązane: Brak.

(3) ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | UTRZYMANIE KOJARZENIA ATRYBUTÓW PRZEZ SYSTEM INFORMATYCZNY

Utrzymywanie kojarzenia i integralności [Realizacja: atrybuty *bezpieczeństwa i ochrony prywatności zdefiniowane przez organizację*] z [Realizacja: *podmioty i obiekty zdefiniowane przez organizację*].

Omówienie: Utrzymanie kojarzenia i integralności atrybutów bezpieczeństwa i ochrony prywatności podmiotów i przedmiotów z wystarczającą pewnością pomaga zapewnić, że kojarzenie atrybutów może być wykorzystywane, jako podstawa zautomatyzowanych reguł działania. Integralność określonych elementów, takich jak pliki konfiguracyjne zabezpieczeń, może być utrzymywana za pomocą mechanizmu monitorowania integralności, który wykrywa anomalie i zmiany odbiegające od "znanych dobrych" poziomów bazowych. Zautomatyzowane działania w ramach polityki obejmują retencję danych, przyznawanie praw dostępu, decyzje dotyczące kontroli przepływu informacji oraz decyzje dotyczące ujawniania informacji.

Zabezpieczenia powiązane: Brak.

(4) ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | KOJARZENIE ATRYBUTÓW PRZEZ AUTORYZOWANY PERSONEL

Zapewnienie możliwości powiązania [Realizacja: *atrybuty bezpieczeństwa i ochrony prywatności zdefiniowane przez organizację*] z [*Realizacja: podmioty i obiekty zdefiniowane przez organizację*] przez uprawnione osoby (lub procesy działające w imieniu osób).

Omówienie: Ogólnie rzecz biorąc, systemy zapewniają uprawnionym użytkownikom możliwość przypisywania atrybutów bezpieczeństwa i ochrony prywatności do zdefiniowanych przez system obiektów (np. użytkowników) i obiektów (np. katalogów, plików i portów). Niektóre systemy oferują dodatkowe możliwości przypisywania przez użytkowników ogólnych atrybutów bezpieczeństwa i ochrony prywatności dodatkowym obiektom (np. plikom, wiadomościom e-mail). Przypisywanie atrybutów przez autoryzowane osoby jest opisane w dokumentacji projektowej. Wsparcie zapewniane przez systemy może obejmować wyświetlanie użytkownikom monitów o wybranie atrybutów bezpieczeństwa i ochrony prywatności, które mają być powiązane z obiektami informacyjnymi, stosowanie automatycznych mechanizmów kategoryzacji

informacji za pomocą atrybutów opartych na zdefiniowanych zasadach lub zapewnienie, że kombinacja wybranych atrybutów bezpieczeństwa lub prywatności jest prawidłowa. Organizacje biorą pod uwagę tworzenie, usuwanie lub modyfikację atrybutów podczas definiowania zdarzeń podlegających audytowi.

Zabezpieczenia powiązane: Brak.

(5) ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | ATRYBUTY BEZPIECZEŃSTWA PREZENTOWANE NA WYŚWIETLACZACH URZĄDZEŃ WYJŚCIOWYCH

Wyświetlanie na każdym obiekcie, w formie czytelnej dla człowieka, atrybutów bezpieczeństwa i ochrony prywatności, które system przesyła do urządzeń wyjściowych w celu identyfikacji [Realizacja: *zdefiniowana przez organizację specjalna instrukcja rozpowszechniania, obsługi lub dystrybucji*] przy użyciu [*Realizacja: zdefiniowana przez organizację, czytelna dla człowieka, standardowa konwencja nazewnicza*].

Omówienie: Systemowe dane wyjściowe zawierają drukowane strony, ekrany lub ich odpowiedniki. Systemowe urządzenia wyjściowe obejmują drukarki, notebooki, wyświetlacze wideo, smartfony, tablety, itp. Aby zminimalizować ryzyko nieuprawnionego ujawnienia informacji (np. podczas przeglądania stron internetowych), urządzenia wyjścia wyświetlają pełne wartości atrybutów po zdjęciu maskowania ich przez użytkownika.

Zabezpieczenia powiązane: Brak.

(6) ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | ZARZĄDZANIE POWIĄZANYMI ATRYBUTAMI

Należy wymagać, aby personel kojarzył i utrzymywał kojarzenie [*Realizacja: atrybuty bezpieczeństwa i ochrony prywatności zdefiniowane przez organizację*] **z [Realizacja: *podmioty i obiekty zdefiniowane przez organizację*]**

zgodnie z [***Realizacja: zasady bezpieczeństwa i ochrony prywatności zdefiniowane przez organizację***]**.**

Omówienie: Utrzymanie skojarzonych atrybutów wymaga od indywidualnych użytkowników (w przeciwieństwie do systemu) przestrzegania kojarzenia zdefiniowanych atrybutów bezpieczeństwa i ochrony prywatności z podmiotami i obiektami.

Zabezpieczenia powiązane: Brak.

(7) ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | INTERPRETACJA WSPÓLNYCH ATRYBUTÓW

Zapewnienie spójnej interpretacji atrybutów bezpieczeństwa i ochrony prywatności przekazywanych pomiędzy rozproszonymi komponentami systemu.

Omówienie: W celu egzekwowania polityki bezpieczeństwa i ochrony prywatności w odniesieniu do wielu komponentów systemów rozproszonych, organizacje zapewniają spójną interpretację atrybutów bezpieczeństwa i ochrony prywatności stosowanych w egzekwowaniu dostępu i decyzjach dotyczących egzekwowania przepływu. Organizacje mogą ustanawiać umowy i procesy, które pomagają zapewnić, że rozproszone komponenty systemu wdrażają atrybuty o spójnej interpretacji w działaniach związanych z automatycznym egzekwowaniem dostępu i egzekwowaniem przepływu.

Zabezpieczenia powiązane: Brak.

(8) ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | TECHNIKI I TECHNOLOGIE WIĄZANIA

Wdrożenie [Realizacja: *techniki i technologie zdefiniowane przez organizację*] w zakresie przypisywania atrybutów bezpieczeństwa i ochrony prywatności do informacji.

Omówienie: Powiązanie atrybutów bezpieczeństwa i ochrony prywatności z informacjami w ramach systemów, jest ważne dla prowadzenia zautomatyzowanych działań w zakresie egzekwowania dostępu i przepływu. Powiązanie takich atrybutów z informacjami (tj. łączenie) można osiągnąć za pomocą technologii i technik, które zapewniają różne poziomy bezpieczeństwa. Na przykład systemy mogą kryptograficznie wiązać atrybuty z informacjami za pomocą podpisów cyfrowych, które obsługują klucze kryptograficzne chronione przez urządzenia sprzętowe (czasami znane, jako sprzętowe źródła zaufania).

Zabezpieczenia powiązane: SC-12, SC-13.

(9) ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | PONOWNY PRZYDZIAŁ ATRYBUTÓW - MECHANIZMY ZMIANY KLASYFIKACJI

Zmiana atrybutów bezpieczeństwa i ochrony prywatności związanych z informacjami tylko poprzez mechanizmy zmiany klasyfikacji zatwierdzone przy użyciu [***Realizacja: techniki lub procedury określone przez organizację***]**.**

Omówienie: Mechanizm zmiany klasyfikacji to zaufany proces uprawniony do zmiany klasyfikacji i oznakowania danych zgodnie ze zdefiniowanymi regułami wyjątków. Zatwierdzone mechanizmy ponownej klasyfikacji są stosowane przez organizacje w celu zapewnienia wymaganego poziomu poświadczenia dla działań związanych z ponownym przypisaniem atrybutów. Zatwierdzenie jest ułatwione poprzez zapewnienie, że mechanizmy zmiany klasyfikacji mają jeden cel i ograniczoną funkcjonalność. Ponieważ zmiany w zakresie bezpieczeństwa i ochrony prywatności mogą mieć bezpośredni wpływ na działania związane z egzekwowaniem polityki, wdrożenie wiarygodnych mechanizmów zmiany klasyfikacji jest konieczne, aby pomóc w zapewnieniu, że mechanizmy te działają w spójnym i prawidłowym trybie.

Zabezpieczenia powiązane: Brak.

(10) ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | KONFIGURACJA ATRYBUTÓW PRZEZ UPOWAŻNIONE OSOBY

Udostępnienie upoważnionym osobom możliwości zdefiniowania lub zmiany typu i wartości atrybutów bezpieczeństwa i ochrony prywatności dostępnych do kojarzenia z podmiotami i obiektami.

Omówienie: Treść lub przypisane wartości atrybutów bezpieczeństwa i ochrony prywatności mogą mieć bezpośredni wpływ na możliwość dostępu osób do informacji organizacyjnych. Dlatego ważne jest, aby systemy były w stanie ograniczyć tylko do uprawnionych osób, możliwość tworzenia lub modyfikowania typu i wartości atrybutów dostępnych do skojarzenia z podmiotami i obiektami.

Zabezpieczenia powiązane: Brak.

Referencje: [OMB A-130], [FIPS 140-3], [FIPS 186-4], [NIST SP 800-162], [NIST SP 800-178].

AC-17 DOSTĘP ZDALNY

Zabezpieczenie podstawowe:

a. Ustanowienie i udokumentowanie ograniczenia w użytkowaniu, wymagań dotyczących konfiguracji/podłączenia oraz wytycznych wdrożeniowych dla każdego dozwolonego typu zdalnego dostępu; oraz

b. Przed zezwoleniem na takie połączenia należy autoryzować każdy rodzaj zdalnego dostępu do systemu.

Omówienie: Dostęp zdalny to dostęp do systemów organizacyjnych (lub procesów działających w imieniu użytkowników), które komunikują się poprzez zewnętrzne sieci, takie jak Internet. Rodzaje dostępu zdalnego obejmują dostęp wdzwaniany (dial-up), szerokopasmowy i bezprzewodowy. Organizacje wykorzystują szyfrowane wirtualne sieci prywatne (VPN) w celu zwiększenia poufności i integralności zdalnych połączeń. Wykorzystanie zaszyfrowanych sieci VPN daje organizacji wystarczającą pewność, że może ona skutecznie traktować takie połączenia jak połączenie w sieci wewnętrznej, jeśli stosowane mechanizmy kryptograficzne są wdrażane zgodnie z obowiązującymi przepisami prawa, rozporządzeniami, dyrektywami, regulacjami, zasadami, standardami i wytycznymi. Jednakże, połączenia VPN tranzytowane są przez sieci zewnętrzne, a szyfrowana sieć VPN nie zwiększa dostępności zdalnych połączeń. Sieci VPN z szyfrowanymi tunelami mogą również wpływać na możliwość odpowiedniego monitorowania sieciowego ruchu komunikacyjnego w poszukiwaniu złośliwego kodu. Zabezpieczenia dostępu zdalnego mają zastosowanie do systemów innych niż publiczne serwery internetowe lub systemy przeznaczone do publicznego dostępu. Autoryzacja każdego typu zdalnego dostępu odbywa się przed zezwoleniem na zdalny dostęp, bez określania konkretnych formatów takiej autoryzacji. Podczas gdy organizacje mogą korzystać z umów o wymianie informacji i bezpieczeństwie połączeń systemowych do zarządzania połączeniami zdalnego dostępu do innych systemów, umowy takie są traktowane, jako część zabezpieczeń CA-3. Egzekwowanie

ograniczeń dostępu w przypadku zdalnego dostępu jest realizowane za pośrednictwem zabezpieczeń AC-3.

Zabezpieczenia powiązane: AC-2, AC-3, AC-4, AC-18, AC-19, AC-20, CA-3, CM-10, IA-2, IA-3, IA-8, MA-4, SE- 17, PL-2, PL-4, SC-10, SC-12, SC-13, SI-4.

Zabezpieczenia rozszerzone:

(1) DOSTĘP ZDALNY | AUTOMATYCZNE MONITOROWANIE I KONTROLA

Stosowanie zautomatyzowanych mechanizmów do monitorowania i kontroli metod zdalnego dostępu.

Omówienie: Monitorowanie i zabezpieczenie metod zdalnego dostępu pozwala organizacjom na wykrywanie ataków i pomoc w zapewnieniu zgodności z zasadami zdalnego dostępu poprzez audytowanie działań w zakresie połączeń zdalnych użytkowników z różnych komponentach systemu, w tym serwerów, notebooków, stacji roboczych, smartfonów i tabletów. Rejestracja audytów zdalnego dostępu jest wymuszona przez zabezpieczenia AU-2. Zdarzenia audytowe są zdefiniowane w zabezpieczeniu rozszerzonym AU-2a.

Zabezpieczenia powiązane: AU-2, AU-6, AU-12, AU-14.

(2) DOSTĘP ZDALNY | OCHRONA POUFNOŚCI I INTEGRALNOŚCI Z WYKORZYSTANIEM SZYFROWANIA

Wdrożenie mechanizmów kryptograficznych w celu ochrony poufności i integralności sesji zdalnego dostępu.

Omówienie: Wirtualne sieci prywatne mogą być wykorzystywane do ochrony poufności i integralności sesji zdalnego dostępu. Transport Layer Security (TLS) jest przykładem protokołu kryptograficznego, który zapewnia całościowe bezpieczeństwo komunikacji w sieci i jest wykorzystywany do komunikacji internetowej i transakcji online.

Zabezpieczenia powiązane: SC-8, SC-12, SC-13.

(3) DOSTĘP ZDALNY | ZARZĄDZANE PUNKTY KONTROLI DOSTĘPU

Udostępnianie dostępu zdalnego wyłącznie poprzez autoryzowane i zarządzane punkty kontroli dostępu do sieci.

Omówienie: Organizacje biorą pod uwagę wymagania inicjatywy Trusted Internet Connections (TIC) [DHS TIC] odnoszące się do zewnętrznych połączeń sieciowych, ponieważ ograniczenie liczby punktów kontroli dostępu, przeznaczonych do zdalnego dostępu, zmniejsza powierzchnie ataku.

Zabezpieczenia powiązane: SC-7.

(4) DOSTĘP ZDALNY | POLECENIA UPRZYWILEJOWANE I DOSTĘP

(a) Zezwolenie na wykonywanie uprzywilejowanych poleceń i dostęp do informacji istotnych z punktu widzenia bezpieczeństwa poprzez dostęp zdalny tylko w formacie, który zapewnia możliwy do oceny dowód oraz na następujące potrzeby: [***Realizacja: potrzeby określone przez organizację***]***;*** **oraz**

(b) Dokumentowanie uzasadnień przydzielania zdalnego dostępu w planie bezpieczeństwa systemu.

Omówienie: Zdalny dostęp do systemów stanowi istotną potencjalną słabość, która może być wykorzystana przez przeciwników. W związku, z tym ograniczenie wykonywania poprzez zdalny dostęp uprzywilejowanych poleceń i udzielania dostępu do informacji istotnych z punktu widzenia bezpieczeństwa, zmniejsza narażenie organizacji oraz podatność na zagrożenia ze strony przeciwników w przypadku stosowania zdalnego dostępu.

Zabezpieczenia powiązane: AC-6, SC-12, SC-13.

(5) DOSTĘP ZDALNY | MONITOROWANIE NIEAUTORYZOWANYCH POŁĄCZEŃ

[Wycofane: Włączone do SI-4].

(6) DOSTĘP ZDALNY | OCHRONA MECHANIZMÓW DOSTĘPU ZDALNEGO

Ochrona informacji o mechanizmach zdalnego dostępu przed nieautoryzowanym użyciem i ujawnieniem.

Omówienie: Zdalny dostęp do informacji organizacyjnych przez podmioty nieorganizacyjne może zwiększyć ryzyko nieautoryzowanego wykorzystania i ujawnienia mechanizmów zdalnego dostępu. Organizacja rozważa włączenie wymagań dotyczących zdalnego dostępu do umów o wymianie informacji z innymi organizacjami, jeśli ma to zastosowanie. Wymagania dotyczące zdalnego dostępu mogą być również zawarte w zasadach zachowania (patrz zabezpieczenie PL-4) i umowach o dostępie (patrz zabezpieczenie PS-6).

Zabezpieczenia powiązane: NA-2, NA-3, PS-6.

(7) DOSTĘP ZDALNY | DODATKOWA OCHRONA DOSTĘPU DO FUNKCJI BEZPIECZEŃSTWA

[Wycofane: Włączone do AC-3(10)]

(8) DOSTĘP ZDALNY | WYŁĄCZANIE NIEZABEZPIECZONYCH PROTOKOŁÓW SIECIOWYCH

[Wycofane: Włączone do CM-7].

(9) DOSTĘP ZDALNY |ODŁĄCZENIE LUB WYŁĄCZENIE DOSTĘPU

Zapewnienie możliwości odłączenia lub wyłączenia zdalnego dostępu do systemu w ciągu [***Realizacja: okres czasu określony przez organizację***]**.**

Omówienie: Szybkość odłączania lub wyłączania systemu zależy od krytyczności misji lub funkcji biznesowych oraz od potrzeby wyeliminowania natychmiastowego lub przyszłego zdalnego dostępu do systemów.

Zabezpieczenia powiązane: Brak.

(10) DOSTĘP ZDALNY | UWIERZYTELNIANIE ZDALNYCH POLECEŃ

Zaimplementowanie [***Realizacja: mechanizmy zdefiniowane przez organizację***] **do uwierzytelniania** [***Realizacja: polecenia zdalne zdefiniowane przez organizację***]**.**

Omówienie: Uwierzytelnianie zdalnych poleceń chroni przed nieautoryzowanymi poleceniami i odtwarzaniem autoryzowanych poleceń. Możliwość uwierzytelniania zdalnych poleceń jest ważna dla systemów zdalnych, dla których utrata, nieprawidłowe działanie, przekierowanie lub wykorzystanie miałyby natychmiastowe lub poważne konsekwencje, takie jak obrażenia ciała, śmierć, uszkodzenie mienia, utrata aktywów o wysokiej wartości, niepowodzenie misji lub funkcji biznesowych, lub narażenie na szwank informacji niejawnych lub kontrolowanych informacji jawnych. Mechanizmy uwierzytelniania zdalnych poleceń zapewniają, że systemy przyjmują i wykonują polecenia w zamierzonej kolejności, wykonują tylko autoryzowane polecenia i odrzucają nieautoryzowane polecenia. Mechanizmy kryptograficzne mogą być wykorzystywane, na przykład, do uwierzytelniania zdalnych poleceń.

Zabezpieczenia powiązane: SC-12, SC-13, SC-23.

Referencje: [NIST SP 800-46], [NIST SP 800-77], [NIST SP 800-113], [NIST SP 800-114], [NIST SP 800-121], [IR 7966].

AC-18 DOSTĘP BEZPRZEWODOWY

Zabezpieczenie podstawowe:

a. Ustalenie wymagań dotyczących konfiguracji, połączeń oraz wytycznych dotyczących wdrażania dla każdego rodzaju dostępu bezprzewodowego; oraz

b. Autoryzacja każdego rodzaju dostępu bezprzewodowego do systemu przed zezwoleniem na dokonanie takiego połączenia.

Omówienie: Technologie bezprzewodowe obejmują sieci mikrofalowe, sieci Packet Radio (ultra-wysokie lub bardzo wysokie częstotliwości), sieci wykorzystujące standard 802.11x oraz Bluetooth. Sieci bezprzewodowe wykorzystują protokoły uwierzytelniania, które zapewniają ochronę autoryzacji i wzajemne uwierzytelnianie.

Zabezpieczenia powiązane: AC-2, AC-3, AC-17, AC-19, CA-9, CM-7, IA-2, IA-3, IA-8, PL-4, SC-40, SC-43, SI-4.

Zabezpieczenia rozszerzone:

(1) DOSTĘP BEZPRZEWODOWY | UWIERZYTELNIANIE ORAZ SZYFROWANIE

Ochrona dostępu bezprzewodowego do systemu za pomocą uwierzytelniania [***Wybór (jeden lub więcej): użytkownicy; urządzenia***] **i szyfrowania.**

Omówienie: Możliwości sieci bezprzewodowych stanowią znaczną potencjalną lukę, która może zostać wykorzystana przez przeciwników. W celu ochrony systemów z punktami dostępu bezprzewodowego, silne uwierzytelnianie użytkowników i urządzeń wraz z silnym szyfrowaniem może zmniejszyć podatność na zagrożenia ze strony przeciwników wykorzystujących technologie bezprzewodowe.

Zabezpieczenia powiązane: SC-8, SC-12, SC-13.

(2) DOSTĘP BEZPRZEWODOWY | MONITOROWANIE POŁĄCZEŃ NIEAUTORYZOWANYCH

[Wycofane: Włączone do SI-4].

(3) DOSTĘP BEZPRZEWODOWY | DEZAKTYWACJA SIECI BEZPRZEWODOWEJ

Przed wydaniem zezwolenia do użycia i wdrożenia należy wyłączyć, jeśli nie są przeznaczone do użytku, funkcje sieci bezprzewodowej włączone do komponenty systemu.

Omówienie: Możliwości sieci bezprzewodowych, które są włączone do komponenty systemu, stanowią znaczącą potencjalną lukę, która może być wykorzystana przez przeciwników. Wyłączenie funkcji sieci bezprzewodowej, gdy nie są one potrzebne do realizacji istotnych zadań lub funkcji organizacyjnych, może zmniejszyć podatność na zagrożenia ze strony przeciwników wykorzystujących technologie bezprzewodowe.

Zabezpieczenia powiązane: Brak.

(4) DOSTĘP BEZPRZEWODOWY | OGRANICZENIE DOKONYWANIA KONFIGURACJI PRZEZ UŻYTKOWNIKÓW

Zidentyfikowanie i autoryzacja użytkowników, którzy mogą samodzielnie konfigurować funkcje sieci bezprzewodowej.

Omówienie: Organizacyjne uprawnienia umożliwiające wybranym użytkownikom konfigurację funkcji sieci bezprzewodowej są egzekwowane częściowo przez mechanizmy egzekwowania dostępu stosowane w systemach organizacyjnych.

Zabezpieczenia powiązane: SC-7, SC-15.

(5) DOSTĘP BEZPRZEWODOWY | POZIOMY MOCY ANTEN / TRANSMISJI

Wybór anten radiowych i kalibracja poziomów mocy nadawania, w celu zmniejszenia prawdopodobieństwa odbioru sygnałów z bezprzewodowych punktów dostępowych poza strefami kontrolowanymi przez organizację.

Omówienie: Działania, które mogą być podjęte w celu ograniczenia nieautoryzowanego korzystania z komunikacji bezprzewodowej poza kontrolowanymi przez organizację strefami, obejmują zmniejszenie mocy transmisji bezprzewodowych, tak, aby ograniczyć niepożądaną emisję sygnału, który może być przechwycony poza fizycznymi strefami kontrolnymi organizacji, stosowanie takich środków jak bezpieczeństwo emisji w celu kontrolowania promieniowania elektromagnetycznego oraz stosowanie anten kierunkowych lub z kształtujących wiązkę, które zmniejszają prawdopodobieństwo, że niepożądani odbiorcy będą w stanie przechwycić sygnały. Przed podjęciem takich działań łagodzących, organizacje mogą przeprowadzać okresowe badania urządzeń bezprzewodowych, w celu zrozumienia profilu częstotliwości radiowych systemów organizacyjnych, jak również innych systemów, które mogą działać w danym obszarze.

Zabezpieczenia powiązane: PE-19.

Referencje: [NIST SP 800-94], [NIST SP 800-97].

AC-19 KONTROLA DOSTĘPU DO URZĄDZEŃ PRZENOŚNYCH

Zabezpieczenie podstawowe:

a. Ustanowienie wymagań dotyczących konfiguracji i połączeń oraz wytycznych dotyczących wdrażania urządzeń przenośnych kontrolowanych przez organizację, w celu uwzględnienia sytuacji, gdy urządzenia takie znajdują się poza obszarami kontrolowanymi przez organizację; oraz

b. Zezwolenie na podłączenie urządzeń przenośnych do systemów organizacyjnych.

Omówienie: Urządzenie przenośne jest urządzeniem komputerowym o niewielkich rozmiarach, tak, że może być z łatwością przenoszone przez jedną osobę; jest przeznaczone do działania bez fizycznego połączenia; posiada lokalny, stały lub wyjmowany magazyn przechowywania danych; oraz zawiera niezależne źródło zasilania. Funkcje urządzenia przenośnego mogą również obejmować komunikację głosową, wbudowane sensory umożliwiające urządzeniu przechwytywanie informacji i/lub wbudowane funkcje synchronizacji danych lokalnych ze zdalnymi lokalizacjami. Przykładem mogą być smartfony i tablety. Urządzenia przenośne są zazwyczaj kojarzone z pojedynczą osobą. Możliwości przetwarzania, przechowywania i przesyłania danych przez urządzenie przenośne mogą być porównywalne lub stanowić jedynie podzbiór systemów notebooków/ komputerów stacjonarnych, w zależności od charakteru i przeznaczenia urządzenia. Ochrona i zabezpieczenie urządzeń przenośnych opiera się na ustalonych zasadach i wymaga od użytkowników podjęcia działań fizycznych w celu ochrony i zabezpieczeń takich urządzeń poza kontrolowanymi obszarami. Obszary kontrolowane to przestrzenie, w których organizacje zapewniają fizyczną lub proceduralną kontrolę w celu spełnienia wymagań ustanowionych dla ochrony informacji i systemów.

Ze względu na dużą różnorodność urządzeń przenośnych o różnych właściwościach i możliwościach, ograniczenia organizacyjne mogą być różne dla różnych klas lub typów takich urządzeń. Ograniczenia w użytkowaniu i szczegółowe wytyczne dotyczące wdrażania urządzeń przenośnych obejmują zarządzanie konfiguracją,

identyfikację urządzeń i uwierzytelnianie, wdrażanie obowiązkowego oprogramowania ochronnego, skanowanie urządzeń w poszukiwaniu złośliwego kodu, aktualizowanie oprogramowania chroniącego przed wirusami, skanowanie w poszukiwaniu krytycznych aktualizacji i poprawek oprogramowania, przeprowadzanie zabezpieczeń integralności podstawowego systemu operacyjnego (i ewentualnie innego oprogramowania rezydującego) oraz wyłączanie nieużywanego hardware-u.

Ograniczenia użytkowania i uprawnienia do łączenia mogą się różnić w zależności od systemu organizacyjnego. Na przykład, organizacja może zezwolić na podłączenie urządzeń przenośnych do swojej sieci i nałożyć zestaw ograniczeń użytkowania, podczas gdy właściciel systemu może wstrzymać zezwolenie na podłączenie urządzeń przenośnych do określonych aplikacji lub nałożyć dodatkowe ograniczenia użytkowania przed zezwoleniem na podłączenie urządzeń przenośnych do systemu. Odpowiednie zabezpieczenia urządzeń przenośnych wykraczają poza wymagania określone w zabezpieczeniu AC-19. Wiele środków bezpieczeństwa dla urządzeń przenośnych znajduje odzwierciedlenie w innych zabezpieczeniach. Środki bezpieczeństwa mogą również w pewnym stopniu nakładać się na siebie w ramach różnych rodzin zabezpieczeń. Zabezpieczenie AC-20 dotyczy urządzeń przenośnych, które nie są kontrolowane przez organizację.

Zabezpieczenia powiązane: AC-3, AC-4, AC-7, AC-11, AC-17, AC-18, AC-20, CA-9, CM 2, CM-6, IA-2, MP-2, MP-4, MP-5, MP-7, PL-4, SC-7, SC-34, SC-43, SI-3, SI-4.

Zabezpieczenia rozszerzone:

(1) KONTROLA DOSTĘPU DO URZĄDZEŃ PRZENOŚNYCH | KORZYSTANIE Z ZAPISYWALNYCH I PRZENOŚNYCH URZĄDZEŃ MAGAZYNUJĄCYCH

[Wycofane: Włączone do MP-7].

(2) KONTROLA DOSTĘPU DO URZĄDZEŃ PRZENOŚNYCH | KORZYSTANIE Z OSOBISTYCH PRZENOŚNYCH URZĄDZEŃ MAGAZYNUJĄCYCH

[Wycofane: Włączone do MP-7].

(3) KONTROLA DOSTĘPU DO URZĄDZEŃ PRZENOŚNYCH | KORZYSTANIE Z OGÓLNODOSTĘPNYCH PRZENOŚNYCH URZĄDZEŃ MAGAZYNUJĄCYCH

[Wycofane: Włączone do MP-7].

(4) KONTROLA DOSTĘPU DO URZĄDZEŃ PRZENOŚNYCH | OGRANICZENIA DOTYCZĄCE INFORMACJI NIEJAWNYCH[39]

(a) Zakazanie używania niesklasyfikowanych urządzeń przenośnych w obiektach zawierających systemy przetwarzające, przechowujące lub przekazujące informacje niejawne; oraz

(b) Egzekwowanie ograniczeń wobec osób upoważnionych do korzystania z niesklasyfikowanych urządzeń przenośnych w obiektach zawierających systemy przetwarzania, przechowywania lub przekazywania informacji niejawnych:

(1) Podłączanie niesklasyfikowanych urządzeń przenośnych do systemów klasyfikowanych jest zabronione;

(2) Podłączanie niesklasyfikowanych urządzeń przenośnych do niesklasyfikowanych systemów wymaga zatwierdzenia przez upoważnioną osobę;

(3) Zabronione jest korzystanie z wewnętrznych lub zewnętrznych modemów lub interfejsów bezprzewodowych w obrębie niesklasyfikowanych urządzeń przenośnych; oraz

[39] Realizowane zgodnie z przepisami ustawy o ochronie informacji niejawnych.

(4) Niejawne urządzenia przenośne i informacje przechowywane na tych urządzeniach podlegają wyrywkowym przeglądom i kontrolom przeprowadzanym przez [***Realizacja: personel ds. bezpieczeństwa informacji wyznaczony przez organizację***]**, a w przypadku wykrycia informacji niejawnych wdrażana jest polityka postępowania z incydentami.**

(c) Ograniczenie możliwość podłączania klasyfikowanych urządzeń przenośnych do systemów klasyfikowanych zgodnie z [***Realizacja: zasady bezpieczeństwa określone przez organizację***]**.**

Omówienie: Brak.

Zabezpieczenia powiązane: CM-8, IR-4.

(5) KONTROLA DOSTĘPU DO URZĄDZEŃ PRZENOŚNYCH | SZYFROWANIE ZAWARTOŚCI CAŁEGO URZĄDZENIA / WYBRANYCH ZASOBÓW URZĄDZENIA

Zastosowanie [***Wybór: szyfrowanie całego urządzenia; szyfrowanie wybranych zasobów urządzenia***] **w celu ochrony poufności i integralności informacji na temat** [***Realizacja: urządzenia mobilne zdefiniowane przez organizację***]**.**

Omówienie: Szyfrowanie wybranych zasobów (kontenera) urządzenia zapewnia bardziej precyzyjne podejście do szyfrowania danych i informacji na urządzeniach przenośnych, w tym szyfrowanie wybranych struktur danych, takich jak pliki, rekordy lub pola.

Zabezpieczenia powiązane: SC-12, SC-13, SC-28.

Referencje: [NIST SP 800-114], [NIST SP 800-124].

AC-20 WYKORZYSTANIE SYSTEMÓW ZEWNĘTRZNYCH

Zabezpieczenie podstawowe:

a. [*Wybór (jeden lub więcej): Ustanowienie* [*Realizacja: zdefiniowanych przez organizację warunków*]*; Określenie* [*Realizacja: zdefiniowanych przez organizację środków bezpieczeństwa, co do których istnieje domniemanie, że zostaną wdrożone w systemach zewnętrznych*]], zgodnych z relacjami współpracy ustanowionymi z innymi organizacjami posiadającymi, obsługującymi i/lub utrzymującymi systemy zewnętrzne, pozwalających upoważnionym osobom na:

   1. Dostęp do systemu organizacji z systemów zewnętrznych; oraz

   2. Przetwarzanie, przechowywanie lub przekazywanie informacji kontrolowanych przez organizację przy użyciu zewnętrznych systemów; lub

b. Zakazanie używania [*Realizacja: zdefiniowanych organizacyjnie typów systemów zewnętrznych*].

Omówienie: Systemy zewnętrzne to systemy, które są wykorzystywane przez organizację, ale nie są częścią jej systemów organizacyjnych i w przypadku których organizacja nie ma bezpośredniej kontroli nad wdrożeniem wymaganych zabezpieczeń lub oceną skuteczności zabezpieczeń. Systemy zewnętrzne obejmują systemy, komponenty lub urządzenia będące własnością prywatną; prywatne urządzenia komputerowe i komunikacyjne w obiektach komercyjnych lub publicznych; systemy będące własnością lub kontrolowane przez organizacje inne organizacje; systemy zarządzane przez wykonawców; oraz systemy informatyczne, które nie są własnością, nie są obsługiwane lub nie znajdują się pod bezpośrednim nadzorem lub władzą organizacji. Systemy zewnętrzne obejmują również systemy będące własnością lub eksploatowane przez inne komponenty w ramach tej samej organizacji oraz systemy wewnątrz organizacji o różnych granicach autoryzacji. Organizacje mają możliwość zakazania korzystania z jakiegokolwiek rodzaju systemów zewnętrznych lub zakazania korzystania z określonych rodzajów systemów zewnętrznych (np. zakazania korzystania z jakiegokolwiek systemu zewnętrznego,

który nie jest własnością organizacji, lub zakazania korzystania z systemów będących własnością prywatną).

W przypadku niektórych systemów zewnętrznych (tj. systemów obsługiwanych przez inne organizacje) relacje oparte na zaufaniu, które zostały ustanowione między tymi organizacjami, a organizacją, z której pochodzą, mogą być takie, że nie są wymagane żadne określone warunki wykorzystywania. Takie systemy nie mogą być uważane za zewnętrzne. Sytuacje takie mają miejsce na przykład wtedy, gdy istnieją wcześniej istniejące umowy o wymianie informacji (domniemane lub ustanowione) zawarte między organizacjami lub gdy takie umowy są określone przez obowiązujące prawo, zarządzenia, dyrektywy, rozporządzenia, zasady lub normy. Do upoważnionych osób zalicza się personel organizacyjny, kontrahentów lub inne osoby posiadające autoryzowany dostęp do systemów organizacyjnych, w stosunku do których organizacje są uprawnione do narzucania określonych zasad postępowania dotyczących dostępu do systemów. Ograniczenia, które organizacje nakładają na upoważnione osoby, nie muszą być jednolite, ponieważ mogą się różnić w zależności od relacji zaufania między organizacjami. Dlatego też podmioty publiczne mogą zdecydować się na nałożenie innych ograniczeń bezpieczeństwa na wykonawców komercyjnych, niż na inne podmioty publiczne.

Systemy zewnętrzne służące do dostępu do interfejsów publicznych systemów organizacyjnych znajdują się poza zakresem zastosowania zabezpieczenia AC-20. Organizacje określają szczegółowe zasady i warunki korzystania z systemów zewnętrznych zgodnie z polityką i procedurami bezpieczeństwa organizacji. Warunki te dotyczą co najmniej określonych typów aplikacji w systemach organizacji, do których można uzyskać dostęp z systemów zewnętrznych oraz najwyższej kategorii bezpieczeństwa informacji, które mogą być przetwarzane, przechowywane lub przekazywane na systemach zewnętrznych. W przypadku braku możliwości ustalenia zasad i warunków z właścicielami systemów zewnętrznych, organizacje mogą nałożyć ograniczenia na personel organizacyjny korzystający z tych systemów zewnętrznych.

Zabezpieczenia powiązane: AC-2, AC-3, AC-17, AC-19, CA-3, PL-2, PL-4, SA-9, SC-7.

Zabezpieczenia rozszerzone:

(1) WYKORZYSTANIE SYSTEMÓW ZEWNĘTRZNYCH | OGRANICZENIA AUTORYZOWANEGO DOSTĘPU

Zezwolenie upoważnionym osobom na korzystanie z zewnętrznego systemu w celu uzyskania dostępu do systemu lub przetwarzania, przechowywania, przekazywania informacji kontrolowanych przez organizację, następuje dopiero po:

(a) Weryfikacji wdrożenia zabezpieczeń systemu zewnętrznego, określonych w polityce bezpieczeństwa i ochrony prywatności organizacji oraz w jej planach bezpieczeństwa i ochrony prywatności; lub

(b) Zawarciu umów o połączeniu sieci / systemów lub obsłudze systemu z jednostką organizacyjną hostującą system zewnętrzny.

Omówienie: Limitowanie autoryzowanego użytkowania rozpoznaje okoliczności, w których osoby korzystające z systemów zewnętrznych mogą potrzebować dostępu do systemów organizacyjnych. Organizacje potrzebują zapewnienia, że systemy zewnętrzne zawierają niezbędne środki bezpieczeństwa, aby nie narażać systemów organizacyjnych na szwank, nie uszkadzać ich lub w inny sposób nie powodować szkody. Weryfikacja, czy wymagane zabezpieczenia zostały wdrożone, może zostać osiągnięta za pomocą zewnętrznych, niezależnych ocen, certyfikatów lub innych środków, w zależności od poziomu zaufania wymaganego przez organizacje.

Zabezpieczenia powiązane: CA-2.

(2) KORZYSTANIE Z SYSTEMÓW ZEWNĘTRZNYCH | PRZENOŚNE URZĄDZENIA MAGAZYNUJĄCE - OGRANICZONE ZASTOSOWANIE

Ograniczenie korzystania w systemach zewnętrznych przez uprawnione osoby z przenośnych urządzeń magazynujących (urządzeń pamięci masowej)

kontrolowanych przez organizację, stosując [***Realizacja: ograniczenia zdefiniowane przez organizację***]**.**

Omówienie: Ograniczenia dotyczące korzystania z kontrolowanych przez organizację przenośnych urządzeń pamięci masowej w systemach zewnętrznych obejmują ograniczenia dotyczące sposobu i warunków korzystania z tych urządzeń.

Zabezpieczenia powiązane: MP-7, SC-41.

(3) KORZYSTANIE Z SYSTEMÓW ZEWNĘTRZNYCH | SYSTEMY NIENALEŻĄCE DO ORGANIZACJI - OGRANICZONE ZASTOSOWANIE

Ograniczenie korzystania z systemów lub komponentów systemu niebędących własnością organizacji w celu przetwarzania, przechowywania lub przekazywania informacji organizacyjnych przy użyciu [***Realizacja: ograniczenia zdefiniowane przez organizację***]**.**

Omówienie: Systemy lub komponenty systemowe niebędące własnością organizacji obejmują systemy lub komponenty systemowe będące własnością innych organizacji, jak również urządzenia będące własnością prywatną. Istnieje potencjalne ryzyko wykorzystania systemów lub komponentów niebędących własnością organizacji. W niektórych przypadkach ryzyko jest wystarczająco duże, aby zakazać takiego wykorzystania (patrz zabezpieczenie rozszerzone AC-20b.). W innych przypadkach korzystanie z takich systemów lub komponentów systemu może być dozwolone, ale w pewien sposób ograniczone. Ograniczenia obejmują wymóg implementacji zatwierdzonych zabezpieczeń przed wydaniem zezwolenia na podłączenie systemów i komponentów niebędących własnością organizacji; ograniczenie dostępu do rodzajów informacji, usług lub aplikacji; wykorzystanie technik wirtualizacji w celu ograniczenia przetwarzania i przechowywania danych jedynie na serwerach lub komponentach systemu dostarczonych przez organizację; oraz wyrażenie zgody na warunki użytkowania. Organizacje konsultują się z działem prawnym w zakresie zagadnień prawnych związanych

z korzystaniem z urządzeń będących własnością prywatną, w tym wymagań dotyczących przeprowadzania analiz procesowych w trakcie czynności dochodzeniowych po zaistnieniu zdarzenia.

Zabezpieczenia powiązane: Brak.

(4) KORZYSTANIE Z SYSTEMÓW ZEWNĘTRZNYCH | SIECIOWE URZĄDZENIA MAGAZYNUJĄCE – ZAKAZ UŻYWANIA

Zakazanie używania [***Realizacja: zdefiniowanych przez organizację sieciowych urządzeń magazynujących (pamięci masowej)***] **w systemach zewnętrznych.**

Omówienie: Sieciowe urządzenia magazynujące dostępne w systemach zewnętrznych obejmują urządzenia pamięci masowej online w publicznych, hybrydowych lub wspólnotowych systemach opartych na chmurze.

Zabezpieczenia powiązane: Brak.

(5) KORZYSTANIE Z SYSTEMÓW ZEWNĘTRZNYCH | PRZENOŚNE URZĄDZENIA MAGAZYNUJĄCE - ZAKAZ UŻYWANIA

Zakazanie używania w systemach zewnętrznych przez uprawnione osoby przenośnych urządzeń magazynujących kontrolowanych przez organizację.

Omówienie: Ograniczenia dotyczące stosowania w systemach zewnętrznych przenośnych urządzeń magazynujących kontrolowanych przez organizację obejmują całkowity zakaz stosowania takich urządzeń. Zakaz takiego stosowania jest egzekwowany za pomocą metod technicznych i/lub metod nietechnicznych (tj. opartych na procesach).

Zabezpieczenia powiązane: MP-7, PL-4, PS-6, SC-41.

Referencje: [FIPS 199], [NIST SP 800-171], [NIST SP 800-172].

AC-21 UDOSTĘPNIANIE INFORMACJI

Zabezpieczenie podstawowe:

a. Umożliwienie autoryzowanym użytkownikom określenia, czy uprawnienia dostępu przydzielone partnerowi, któremu udostępniane są informacje, są zgodne z ograniczeniami dostępu i użytkowania informacji do [*Realizacja: zdefiniowanych przez organizację okoliczności udostępniania informacji, w których wymagana jest zachowanie tajemnicy*]; oraz

b. Stosowanie [*Realizacja: zdefiniowane przez organizację automatyczne mechanizmy lub procesy ręczne*], aby pomóc użytkownikom w podejmowaniu decyzji dotyczących udostępniania informacji i współpracy.

Omówienie: Udostępnianie informacji dotyczy informacji, które mogą być w pewien sposób ograniczone w oparciu o pewne ustalenia formalne lub administracyjne. Przykłady takich informacji obejmują informacje wrażliwe z punktu widzenia umowy, informacje niejawne związane ze specjalnymi programami dostępu lub dziedzinami, informacje uprzywilejowane, informacje zastrzeżone oraz informacje umożliwiające identyfikację osoby. Oceny ryzyka związanego z bezpieczeństwem i prywatnością, jak również obowiązujące prawa, przepisy i polityki mogą stanowić użyteczny wkład w te ustalenia. W zależności od okoliczności, partnerzy udostępniający informacje mogą być określeni na poziomie indywidualnym, grupowym lub organizacyjnym. Informacje mogą być definiowane według zawartości, typu, kategorii bezpieczeństwa lub specjalnego programu lub obszaru dostępu. Ograniczenia dostępu mogą obejmować umowy o zachowaniu poufności (NDA)[40]. Techniki przepływu informacji i atrybuty bezpieczeństwa mogą być stosowane w celu zapewnienia automatycznej pomocy użytkownikom podejmującym decyzje dotyczące udostępniania i współpracy.

[40] Patrz: NSC 7298, Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa.

Zabezpieczenia powiązane: AC-3, AC-4, AC-16, PT-2, PT-7, RA-3, SC-15.

Zabezpieczenia rozszerzone:

(1) UDOSTĘPNIANIE INFORMACJI | AUTOMATYCZNE WSPARCIE DECYZJI

Stosowanie [***Realizacja: określone przez organizację automatyczne mechanizmy***] **w celu egzekwowania decyzji dotyczących udostępniania informacji przez uprawnionych użytkowników na podstawie uprawnień dostępu współpracujących partnerów oraz ograniczeń dostępu do informacji, które mają być udostępniane.**

Omówienie: Zautomatyzowane mechanizmy są wykorzystywane do egzekwowania decyzji dotyczących wymiany informacji.

Zabezpieczenia powiązane: Brak.

(2) UDOSTĘPNIANIE INFORMACJI | WYSZUKIWANIE I ODZYSKIWANIE INFORMACJI

Wdrożenie usług wyszukiwania i odzyskiwania informacji, które egzekwują [Realizacja: *ograniczenia dotyczące udostępniania informacji określone przez organizację*].

Omówienie: Usługi wyszukiwania i odzyskiwania informacji określają zasoby systemu informatycznego istotne z punktu widzenia potrzeb informatycznych.

Zabezpieczenia powiązane: Brak.

Referencje: [OMB A-130], [NIST SP 800-150], [IR 8062].

AC-22 TREŚCI PUBLICZNIE DOSTĘPNE

Zabezpieczenie podstawowe:

a. Wyznaczenie osób upoważnionych do publicznego udostępniania informacji;

b. Szkolenie upoważnionych osób, aby zapewnić, że publicznie dostępne informacje nie zawierają informacji niepublicznych;

c. Dokonywanie przeglądów proponowanej do upublicznienia treści informacji przed ich umieszczeniem w publicznie dostępnym systemie, aby upewnić się, że informacje niepubliczne nie zostały udostępnione; oraz

d. Przeglądanie zawartości upublicznianych treść w publicznie dostępnym systemie pod kątem informacji niepublicznych z częstotliwością [*Realizacja: częstotliwość określona przez organizację*] i usuwanie takich informacji w przypadku ich wykrycia.

Omówienie: Zgodnie z obowiązującymi przepisami prawa, rozporządzeniami wykonawczymi, dyrektywami, politykami, rozporządzeniami, standardami i wytycznymi, społeczeństwo nie jest upoważnione do dostępu do informacji niepublicznych, włącznie z informacjami chronionymi oraz informacjami własnościowymi. Publicznie dostępne treści dotyczą systemów kontrolowanych przez organizację i dostępnych publicznie, zazwyczaj bez identyfikacji lub uwierzytelnienia. Umieszczanie informacji w systemach innych niż organizacyjne (np. na publicznych stronach internetowych, forach i mediach społecznościowych) jest objęte polityką organizacyjną. Podczas gdy organizacje mogą mieć osoby odpowiedzialne za opracowywanie i wdrażanie zasad dotyczących informacji, które mogą być publicznie dostępne, publicznie dostępne treści kierowane są do kierownictwa osób, które udostępniają takie informacje.

Zabezpieczenia powiązane: AC-3, AT-2, AT-3, AU-13.

Zabezpieczenia rozszerzone: Brak.

Referencje: [PRIVACT].

AC-23 OCHRONA PRZED PRZESZUKIWANIEM DANYCH

Zabezpieczenie podstawowe: Stosowanie [Realizacja: *zdefiniowana przez organizację technika zapobiegania i wykrywania inwigilacji danych*] dla [*Realizacja: zdefiniowana przez organizację obiekty przechowywania danych*] w celu wykrywania i ochrony przed nieautoryzowanym przeszukiwaniem danych.

Omówienie: Przeszukiwanie danych jest procesem analitycznym, który próbuje znaleźć korelacje lub wzorce w dużych zbiorach danych w celu pozyskania danych lub wiedzy o podmiocie. Obiekty przechowywania danych obejmują rekordy i pola bazy danych. Informacje wrażliwe mogą być wyselekcjonowane podczas operacji przeszukiwania danych. Jeżeli informacja jest informacją możliwą do zidentyfikowania, może prowadzić do niepożądanych ujawnień dotyczących osób i stwarzać zagrożenie dla prywatności. Przed przystąpieniem do przeszukiwania danych organizacje ustalają, czy takie działania są dozwolone. Organizacje podlegają obowiązującym przepisom prawa, zarządzeniom, dyrektywom, rozporządzeniom lub zasadom, które dotyczą wymogów inwigilacji danych. Personel organizacji konsultuje się w sprawie takich wymogów z inspektorem ochrony danych i radcą prawnym.

Techniki zapobiegania eksploracji danych i wykrywania obejmują ograniczenie liczby i częstotliwości zapytań do baz danych w celu zwiększenia współczynnika pracy niezbędnego do określenia zawartości baz danych, ograniczenie rodzajów odpowiedzi udzielanych na zapytania do baz danych, stosowanie zróżnicowanych technik ochrony prywatności lub szyfrowania homomorficznego oraz powiadamianie personelu w przypadku wystąpienia nietypowych zapytań do baz danych lub dostępu do nich. Ochrona przed przeszukiwaniem danych koncentruje się na ochronie informacji przed eksploracją danych, podczas gdy takie informacje znajdują się w organizacyjnych magazynach danych. W przeciwieństwie do tego środka bezpieczeństwa, zabezpieczenie AU-13 koncentruje się na monitorowaniu informacji organizacyjnych, które mogły zostać wydobyte lub w inny sposób uzyskane z magazynów danych i są dostępne, jako informacje open-source znajdujące się na

zewnętrznych stronach internetowych, takich jak portale społecznościowe lub witryny społecznościowe.

Wymagane jest ustanowienie programu przeciwdziałania zagrożeniom związanym z wykorzystaniem informacji wrażliwych, wykrywania i ograniczania takich zagrożeń, w tym ochrony informacji wrażliwych przed wykorzystaniem, narażeniem na szwank lub innym nieuprawnionym ujawnieniem. Ochrona eksploracji danych wymaga od organizacji określenia odpowiednich technik zapobiegania i wykrywania zbędnych lub nieuprawnionych eksploracji danych. Przeszukiwanie danych może być wykorzystane przez osobę mającą dostęp do informacji wrażliwych w celu zebrania informacji organizacyjnych do celów eksfiltracji danych.

Zabezpieczenia powiązane: PM-12, PT-2.

Zabezpieczenia rozszerzone: Brak.

Referencje: [EO 13587].

AC-24 PRZYZNAWANIE PRAW DOSTĘPU

Zabezpieczenie podstawowe: [*Wybór: ustanowienie procedur; wdrożenie mechanizmów*] w celu zapewnienia, że [*Realizacja: przyznawanie praw dostępu określone przez organizację*] są stosowane do każdego wniosku o dostęp przed potwierdzeniem (udzieleniem) dostępu.

Omówienie: Decyzje o przyznawaniu praw dostępu (zwane również decyzjami autoryzacyjnymi) pojawiają się, gdy informacje o autoryzacji są stosowane do przyznawania określonych dostępów. Natomiast egzekwowanie uprawnień dostępu ma miejsce, gdy systemy egzekwują decyzje kontroli dostępu. O ile powszechne jest, że decyzje kontroli dostępu i egzekwowanie uprawnień dostępu są wdrażane przez tę samą jednostkę, nie jest to wymagane i nie zawsze jest to optymalny wybór implementacji. W przypadku niektórych architektur i systemów rozproszonych, decyzje w zakresie kontroli i egzekwowania dostęp mogą podejmować różne podmioty.

Zabezpieczenia powiązane: AC-2, AC-3.

Zabezpieczenia rozszerzone:

(1) PRZYZNAWANIE PRAW DOSTĘPU | PRZESYŁANIE INFORMACJI O AUTORYZACJI DOSTĘPU

Przesyłanie [Realizacja: *informacje o uprawnieniach dostępu zdefiniowanych przez organizację*] przy użyciu [*Realizacja: systemy zdefiniowane przez organizację*] do [*Realizacja: systemy zdefiniowane przez organizację*], które egzekwują przyznawanie praw dostępu.

Omówienie: Procesy autoryzacji i przyznawanie praw dostępu mogą występować w oddzielnych elementach systemów lub w oddzielnych systemach. W takich przypadkach informacje o autoryzacji są przekazywane w sposób bezpieczny (np. za pomocą mechanizmów kryptograficznych), tak, aby w stosownym czasie można było egzekwować decyzje kontrolne

przeprowadzane w odpowiednich miejscach. W celu wsparcia decyzji dotyczących kontroli dostępu konieczne może być przekazanie w ramach autoryzacji dostępu informacji wspierających atrybuty bezpieczeństwa i ochrony prywatności. Dzieje się tak, ponieważ w systemach rozproszonych istnieją różne decyzje w zakresie kontroli dostępu, które muszą być podejmowane, a różne podmioty podejmują te decyzje w sposób seryjny, z których każdy wymaga tych atrybutów do podjęcia decyzji. Ochrona informacji o autoryzacji dostępu zapewnia, że takie informacje nie mogą być zmieniane, sfałszowane, lub narażone na ujawnienie podczas transmisji.

Zabezpieczenia powiązane: AU-10.

(2) PRZYZNAWANIE PRAW DOSTĘPU | BRAK TOŻSAMOŚCI UŻYTKOWNIKA LUB PROCESU

Egzekwowanie decyzji dotyczących kontroli dostępu w oparciu o [***Realizacja: atrybuty bezpieczeństwa lub prywatności zdefiniowane przez organizację***]**, które nie posiadają tożsamości użytkownika lub procesu działającego w imieniu użytkownika.**

Omówienie: W pewnych sytuacjach ważne jest, aby przyznawanie praw dostępu mogły być podejmowane bez posiadania informacji dotyczących tożsamości użytkowników składających wnioski. Są to na ogół przypadki, w których ochrona prywatności indywidualnych osób ma nadrzędne znaczenie. W innych sytuacjach informacje dotyczące identyfikacji użytkownika po prostu nie są potrzebne do podejmowania decyzji w zakresie kontroli dostępu, a szczególnie w przypadku systemów rozproszonych przekazywanie takich informacji z wymaganym stopniem pewności może być bardzo kosztowne lub trudne do zrealizowania.

Na przykład polityki zabezpieczeń oparte na metodzie MAC, RBAC, ABAC i etykietowaniu mogą nie uwzględniać tożsamości użytkownika jako atrybutu.

Zabezpieczenia powiązane: Brak.

Referencje: [NIST SP 800-162], [NIST SP 800-178].

AC-25 MONITOR REFERENCYJNY

Zabezpieczenie podstawowe: Wdrożenie monitora referencyjnego dla [*Realizacja: zasady kontroli dostępu zdefiniowane przez organizację*], który jest odporny na manipulacje, zawsze przywoływany i na tyle „mało waży", że może być poddany analizie i testom, których kompletność można zapewnić.

Omówienie: Monitor referencyjny to zestaw wymogów projektowych dotyczących mechanizmu zatwierdzania referencji, który jako kluczowy element systemu operacyjnego narzuca politykę kontroli dostępu w odniesieniu do wszystkich podmiotów i przedmiotów. Mechanizm weryfikacji referencji jest zawsze przywoływany, zabezpieczony przed ingerencją osób niepowołanych i na tyle mały objętościowo, że może być poddany analizie i testom, których kompletność można zapewnić (tj. zweryfikować). Informacje są przedstawiane wewnętrznie w ramach systemów za pomocą abstrakcji znanych, jako struktury danych. Wewnętrzne struktury danych mogą reprezentować różne rodzaje podmiotów, zarówno aktywnych, jak i pasywnych. Jednostki aktywne, zwane również podmiotami, są związane z osobami, urządzeniami lub procesami działającymi w imieniu osób fizycznych. Jednostki pasywne, zwane również obiektami, są związane ze strukturami danych, takimi jak rekordy, bufory, porty komunikacyjne, tabele, pliki i przepływy międzyprocesowe. Monitory referencyjne egzekwują zasady kontroli dostępu, które ograniczają dostęp do obiektów w oparciu o tożsamość podmiotów lub grup, do których podmioty te należą. System egzekwuje politykę kontroli dostępu w oparciu o zasady ustanowione przez tę politykę. Zabezpieczona przed manipulacją właściwość monitora referencyjnego uniemożliwia zidentyfikowanym przeciwnikom narażenie na szwank funkcjonowania mechanizmu walidacji referencyjnej. Własność zawsze przywoływana zapobiega obchodzeniu mechanizmu przez przeciwników i naruszaniu polityki bezpieczeństwa. Właściwość ta pomaga zapewnić kompletność analizy i testowania mechanizmu w celu wykrycia wszelkich słabych punktów lub braków (tj. ukrytych wad), które uniemożliwiałyby egzekwowanie polityki bezpieczeństwa.

Zabezpieczenia powiązane: AC-3, AC-16, SA-8, SA-17, SC-3, SC-11, SC-39, SI-13.

Zabezpieczenia rozszerzone: Brak.

KATEGORIA AT - UŚWIADAMIANIE I SZKOLENIA

AT-1 POLITYKA I PROCEDURY

Zabezpieczenie podstawowe:

a. Opracowywanie, dokumentowanie i rozpowszechnianie wśród [*Realizacja: personel lub role określone przez organizację*]*:*

   1. [*Wybór (jeden lub więcej): poziom organizacji; poziom misji/procesu biznesowego; poziom systemu*] polityki podnoszenia świadomości bezpieczeństwa i szkolenia, która:

      (a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami; oraz

      (b) Jest zgodna z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi; oraz

   2. Procedur ułatwiających realizację polityki podnoszenia świadomości bezpieczeństwa i szkolenia oraz powiązanych środków bezpieczeństwa w zakresie świadomości i szkolenia;

b. Wyznaczanie [*Realizacja: osoba wyznaczona przez organizację*] do zarządzania rozwojem, dokumentacją i rozpowszechnianiem polityki i procedur w zakresie świadomości bezpieczeństwa i szkoleń; oraz

c. Przeglądanie i aktualizowanie bieżącej:

   1. Polityki świadomości bezpieczeństwa i szkoleń z [Realizacja: *częstotliwość określona przez organizację*] i następujących [*Realizacja: zdarzenia określone przez organizację*]; oraz

   2. Procedur dotyczących świadomości bezpieczeństwa i szkoleń z [Realizacja: *częstotliwość określona przez organizację*] i następujących [*Realizacja: zdarzenia określone przez organizację*].

Omówienie: Polityka i procedury w zakresie świadomości bezpieczeństwa i szkoleń dotyczą zabezpieczeń w kategorii *Uświadamianie i szkolenia* (AT), które są wdrażane w ramach systemów i organizacji. Strategia zarządzania ryzykiem jest ważnym czynnikiem przy tworzeniu takich polityk i procedur. Polityki i procedury przyczyniają się do zapewnienia bezpieczeństwa i ochrony prywatności. Dlatego ważne jest, aby programy bezpieczeństwa i ochrony prywatności były opracowywane wspólnie przy kształtowaniu polityki i procedur uświadamiania i szkolenia. Polityki i procedury dotyczące programów bezpieczeństwa i ochrony prywatności na poziomie organizacji są ogólnie rzecz biorąc preferowane i mogą eliminować potrzeby tworzenia polityk i procedur specyficznych dla danej misji lub systemu. Polityka może być włączona, jako część ogólnej polityki bezpieczeństwa i ochrony prywatności lub reprezentowana przez wiele polityk odzwierciedlających złożony charakter organizacji. Procedury mogą być ustanowione dla programów bezpieczeństwa i ochrony prywatności, dla misji lub procesów biznesowych oraz dla systemów, jeśli to konieczne. Procedury opisują sposób wdrażania zasad lub zabezpieczeń i mogą być skierowane do osoby lub roli, która jest przedmiotem procedury. Procedury mogą być udokumentowane w planach bezpieczeństwa i ochrony prywatności systemu w jednym lub kilku oddzielnych dokumentach.

Zdarzenia, które mogą spowodować konieczność aktualizacji polityki i procedur uświadamiania i szkolenia, obejmują wyniki oceny lub audytu, incydenty lub naruszenia bezpieczeństwa, lub zmiany w przepisach prawa, zarządzeniach, dyrektywach, rozporządzeniach, zasadach, standardach i wytycznych.

Oświadczenie o wprowadzeniu zabezpieczeń nie jest równoznaczne z ustanowieniem polityki lub procedury organizacyjnej.

Zabezpieczenia powiązane: PM-9, PS-8, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [NIST SP 800-12], [NIST SP 800-30], [NIST SP 800-39], [NIST SP 800-50], [NIST SP 800-100].

AT-2 SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA

Zabezpieczenie podstawowe:

a. Zapewnienie użytkownikom systemu (w tym menedżerom, wyższej kadrze kierowniczej i wykonawcom) szkoleń w zakresie bezpieczeństwa i ochrony prywatności:

   1. W ramach szkolenia wstępnego dla nowych użytkowników, a następnie [*Realizacja: częstotliwość określona przez organizację*]; oraz

   2. Gdy jest to wymagane przez zmiany w systemie lub po [*Realizacja: zdarzenia zdefiniowane przez organizację*];

b. Stosowanie następujących technik w celu zwiększenia świadomości bezpieczeństwa i ochrony prywatności użytkowników systemu [*Realizacja: techniki świadomości zdefiniowane przez organizację*];

c. Aktualizacja szkoleń w zakresie uświadamiania bezpieczeństwa [Realizacja: *częstotliwość określona przez organizację*] i wystąpieniu [*Realizacja: zdarzenia określone przez organizację*]; oraz

d. Włączanie wniosków wyciągniętych z wewnętrznych lub zewnętrznych incydentów lub naruszeń bezpieczeństwa do szkoleń w zakresie uświadamiania bezpieczeństwa.

Omówienie: Organizacje zapewniają podstawowy i zaawansowany poziom szkoleń w zakresie uświadamiania bezpieczeństwa użytkownikom systemu, w tym środki umożliwiające sprawdzenie poziomu wiedzy użytkowników. Organizacje określają treść szkolenia w zakresie uświadamiania bezpieczeństwa w oparciu o konkretne wymagania organizacyjne, systemy, do których dostęp ma upoważniony personel, oraz środowiska pracy (np. telepraca, praca zdalna). Treści te obejmują zrozumienie potrzeby zachowania bezpieczeństwa i ochrony prywatności, a także działań podejmowanych przez użytkowników w celu zachowania bezpieczeństwa i ochrony prywatności oraz reagowania na podejrzane incydenty. Treść jest odpowiedzią na

potrzebę bezpieczeństwa operacji i postępowania z danymi osobowymi, które można zidentyfikować.

Techniki uświadamiające obejmują wyświetlanie plakatów, oferowanie materiałów z przypomnieniami o bezpieczeństwie i ochronie prywatności, wyświetlanie komunikatów na ekranie monitora podczas logowania, generowanie porad lub powiadomień e-mailowych od organizacji oraz prowadzenie spotkań uświadamiających. Szkolenie w zakresie uświadamiania bezpieczeństwa prowadzone po szkoleniu wstępnym opisanym w zabezpieczeniu rozszerzonym AT-2a.1 odbywa się z minimalną częstotliwością zgodną z obowiązującym prawem, dyrektywami, przepisami i zasadami. Kolejne szkolenie w zakresie uświadamiania bezpieczeństwa może zostać zakończone jedną lub kilkoma krótkimi sesjami ad hoc i może obejmować aktualne informacje na temat ostatnich schematów ataku, zmian w polityce bezpieczeństwa i ochrony prywatności organizacji, zmienionych oczekiwań w zakresie bezpieczeństwa i ochrony prywatności lub podzbiór tematów ze szkolenia wstępnego. Regularne aktualizowanie treści szkolenia w zakresie uświadamiania bezpieczeństwa pomaga zapewnić, że treści pozostają aktualne. Zdarzenia, które mogą spowodować konieczność aktualizacji treści szkolenia i świadomości, obejmują między innymi ocenę lub wyniki audytu, zdarzenia związane z incydentami lub naruszeniami bezpieczeństwa lub zmiany w obowiązujących przepisach prawa, rozporządzeniach, dyrektywach, zasadach, standardach i wytycznych.

Zabezpieczenia powiązane: AC-3, AC-17, AC-22, AT-3, AT-4, CP-3, IA-4, IR-2, IR-7, IR-9, PL-4, PM-13, PM-21, PS-7, PT-2, SA-8, SA-16.

Zabezpieczenia rozszerzone:

(1) SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | ĆWICZENIA PRAKTYCZNE

Zapewnienie ćwiczeń praktycznych z zakresu uświadamiania bezpieczeństwa, które symulują zdarzenia i incydenty.

Omówienie: Ćwiczenia praktyczne obejmują niezauważalne próby zbierania informacji, uzyskiwania nieautoryzowanego dostępu lub symulowania niekorzystnego wpływu otwarcia złośliwych załączników do wiadomości e-mail lub wywoływania, za pomocą ataków spersonalizowanego wyłudzania informacji (*ang. spear phishing attacks*), złośliwych linków internetowych.

Zabezpieczenia powiązane: CA-2, CA-7, CP-4, IR-3.

(2) SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA |ZAGROŻENIE WEWNĘTRZNE

Zapewnienie szkolenie w zakresie uświadamiania bezpieczeństwa dotyczące rozpoznawania i zgłaszania potencjalnych wskaźników zagrożeń wewnętrznych.

Omówienie: Potencjalne wskaźniki i możliwe prekursory zagrożeń wewnętrznych mogą obejmować zachowania takie jak nadmierne, długotrwałe niezadowolenie z pracy; próby uzyskania dostępu do informacji, które nie są wymagane do wykonywania pracy; niewyjaśniony dostęp do zasobów finansowych; nękanie lub prześladowanie współpracowników; przemoc w miejscu pracy; oraz inne poważne naruszenia polityki, procedur, dyrektyw, przepisów, zasad lub praktyk. Szkolenie w zakresie uświadamiania bezpieczeństwa obejmuje sposoby komunikowania obaw pracowników i kierownictwa dotyczących potencjalnych wskaźników zagrożeń związanych z wykorzystaniem informacji wrażliwych za pośrednictwem kanałów ustalonych przez organizację oraz zgodnie z ustalonymi zasadami i procedurami. Organizacje mogą rozważyć dostosowanie tematów związanych ze świadomością zagrożeń związanych z wykorzystaniem informacji wrażliwych do danej roli. Na przykład, szkolenia dla menedżerów mogą

koncentrować się na zmianach w zachowaniu członków zespołu, natomiast szkolenia dla pracowników mogą skupiać się na bardziej ogólnych obserwacjach.

Zabezpieczenia powiązane: PM-12.

(3) SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | INŻYNIERIA SPOŁECZNA I POZYSKIWANIE DANYCH

Zapewnić szkolenie w zakresie rozpoznawania i raportowania potencjału i rzeczywistych przypadków inżynierii społecznej i pozyskiwania danych z mediów społecznościowych.

Omówienie: Inżynieria społeczna to próba oszukania jednostki w celu ujawnienia informacji lub podjęcia działań, które mogą zostać wykorzystane do naruszenia, ujawnienia lub innego negatywnego wpływu na system. Inżynieria społeczna obejmuje phishing, wymyślone scenariusze pretekstu (*ang. pretexting*), podszywanie się (*ang. impersonation*), wabienie (*ang. baiting*), „coś-za-coś" (*ang. quid pro quo*), podszywanie się pod wątki (*ang. thread-jacking*), przeszukiwanie mediów społecznościowych i próby wejścia „na doczepkę" (*ang. tailgating*). Pozyskiwanie danych z mediów społecznościowych to próba zebrania informacji o organizacji, które mogą zostać wykorzystane do wsparcia przyszłych ataków. Szkolenie w zakresie uświadamiania bezpieczeństwa obejmuje informacje na temat tego, jak komunikować obawy pracowników i kierownictwa dotyczące potencjalnych i rzeczywistych przypadków inżynierii społecznej i eksploracji danych za pośrednictwem kanałów organizacyjnych opartych na ustalonych zasadach i procedurach.

Zabezpieczenia powiązane: Brak.

(4) SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | PODEJRZANA TRANSMISJA I ANOMALIE ZACHOWANIA SYSTEMU

Zapewnienie szkolenia w zakresie rozpoznawania podejrzanych komunikatów i anomalii w systemach organizacyjnych przy użyciu [***Realizacja: wskaźniki złośliwego kodu zdefiniowane przez organizację***]**.**

Omówienie: Dobrze wyszkoleni pracownicy stanowią kolejne zabezpieczenie organizacyjne, które może być wykorzystane, jako część strategii obrony przed złośliwym kodem przychodzącym do organizacji za pośrednictwem poczty elektronicznej lub aplikacji internetowych. Personel jest przeszkolony w zakresie poszukiwania oznak potencjalnie podejrzanych wiadomości e-mail (np. otrzymanie nieoczekiwanej wiadomości e-mail, otrzymanie wiadomości zawierającej dziwną lub złą gramatykę, lub otrzymanie wiadomości e-mail od nieznanego nadawcy, który wydaje się być nadany przez znanego sponsora lub wykonawcę). Personel jest również szkolony w zakresie reagowania na podejrzane wiadomości e-mail lub komunikaty internetowe. Aby proces ten działał skutecznie, pracownicy są szkoleni i uświadamiani o tym, co stanowi podejrzaną korespondencję. Szkolenie personelu w zakresie rozpoznawania anomalnych zachowań w systemach może zapewnić organizacjom wczesne ostrzeganie o obecności złośliwego kodu. Rozpoznawanie anomalnych zachowań przez personel organizacji może stanowić uzupełnienie narzędzi i systemów wykorzystywanych przez organizacje do wykrywania i ochrony przed złośliwym kodem.

Zabezpieczenia powiązane: Brak.

(5) SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | ZAAWANSOWANE TRWAŁE ZAGROŻENIE

Zapewnienie szkolenia w zakresie uświadamiania bezpieczeństwa na temat zaawansowanych trwałych zagrożeń (*ang. advanced persistent threats – APT*).

Omówienie: Skutecznym sposobem wykrywania zaawansowanych trwałych zagrożeń (APT) i zapobiegania udanym atakom jest zapewnienie specjalnego szkolenia w zakresie uświadamiania bezpieczeństwa dla poszczególnych osób. Szkolenie w zakresie rozpoznawania i zwalczania zagrożeń obejmuje edukowanie osób na temat różnych sposobów, w jaki zagrożenia APT mogą przeniknąć do organizacji (np. poprzez strony internetowe, e-maile, wyskakujące okienka reklamowe, artykuły i inżynierię społeczną). Skuteczne szkolenie obejmuje techniki rozpoznawania podejrzanych e-maili, stosowanie systemów wymiennych (usuwalnych) z niezabezpieczonymi ustawieniami oraz potencjalne oddziaływanie na osoby pracujące zdalnie.

Zabezpieczenia powiązane: Brak.

(6) SZKOLENIA W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | ŚRODOWISKA CYBERZAGROŻEŃ

(a) Zapewnienie szkoleń w zakresie uświadamiania bezpieczeństwa dotyczących środowiska cyberzagrożeń; oraz

(b) Odzwierciedlanie aktualnych informacji o cyberzagrożeniach w operacjach systemu.

Omówienie: Ponieważ zagrożenia zmieniają się wraz z upływem czasu, szkolenie w zakresie znajomości zagrożeń przez organizację jest dynamiczne. Co więcej, szkolenia z zakresu znajomości zagrożeń nie są prowadzone w oderwaniu od działań systemowych, które wspierają misję organizacji i funkcje biznesowe.

Zabezpieczenia powiązane: RA-3.

Referencje: [OMB A-130], [NIST SP 800-50], [NIST SP 800-160-2], [NIST SP 800-181], [ODNI CTF].

AT-3 SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH

Zabezpieczenie podstawowe:

a. Zapewnienie personelowi szkolenia w zakresie bezpieczeństwa i ochrony prywatności w oparciu o role i obowiązki wymienione poniżej: [*Realizacja: role i obowiązki określone przez organizację*]*:*

   1. Przed zezwoleniem na dostęp do systemu, informacji lub wykonaniem przydzielonych obowiązków, a następnie [*Przyznanie: częstotliwość określona przez organizację*]; oraz

   2. Gdy wymagają tego zmiany w systemie;

b. Aktualizacja treści szkolenia w oparciu o role [Realizacja: *częstotliwość określona przez organizację*] i następujące po nim [*Realizacja: zdarzenia określone przez organizację*]; oraz

c. Włączenie wniosków wyciągniętych z wewnętrznych lub zewnętrznych incydentów lub naruszeń bezpieczeństwa do szkoleń opartych na rolach.

Omówienie: Organizacje określają treść szkoleń w oparciu o przypisane im role i obowiązki, a także wymagania organizacji w zakresie bezpieczeństwa i ochrony prywatności oraz systemów, do których dostęp ma upoważniony personel, w tym szkoleń technicznych specjalnie dostosowanych do przydzielonych obowiązków. Role, które mogą wymagać szkolenia w oparciu o role, obejmują wyższych rangą liderów lub personel zarządzających (np. szef organizacji/członek zarządu, dyrektor ds. bezpieczeństwa informacji, personel odpowiedzialny za zarządzanie ryzykiem, specjalista ds. bezpieczeństwa informacji, inspektor ochrony danych), właściciele systemów; personel autoryzujący; personel ds. bezpieczeństwa systemów; personel ds. ochrony danych osobowych; personel ds. zakupów i zaopatrzenia; architekci przedsiębiorstw; inżynierowie systemów; twórcy oprogramowania; inżynierowie ds. bezpieczeństwa systemów; inżynierowie ds. ochrony danych osobowych; administratorzy systemów, sieci i baz danych; audytorzy; personel zarządzający

konfiguracją; personel wykonujący czynności weryfikacyjne i zatwierdzające; personel mający dostęp do oprogramowania na poziomie systemu; personel oceniający zabezpieczenia; personel odpowiedzialny za planowanie awaryjne / ciągłość działania i reagowanie na incydenty; personel odpowiedzialny za zarządzanie prywatnością (ochronę danych osobowych); personel mający dostęp do danych osobowych.

Kompleksowe szkolenie w oparciu o podział ról dotyczy zarządzania, ról oraz obowiązków operacyjnych i technicznych obejmujących bezpieczeństwo fizyczne, osobowe i techniczne. Szkolenie w zakresie bezpieczeństwa opartego na rolach obejmuje również politykę, procedury, narzędzia, metody i artefakty dotyczące określonych ról w zakresie bezpieczeństwa i ochrony prywatności. Organizacje zapewniają szkolenia niezbędne do wypełniania przez osoby obowiązków związanych z działalnością i zarządzaniem ryzykiem w łańcuchu dostaw w kontekście programów bezpieczeństwa i ochrony prywatności organizacji. Szkolenie w zakresie ról ma również zastosowanie do wykonawców, którzy świadczą usługi na rzecz organizacji. Rodzaje szkoleń obejmują szkolenia zdalne / sieciowe, szkolenia komputerowe, szkolenia stacjonarne oraz szkolenia praktyczne (w tym szkolenie krok-po-kroku). Regularne aktualizowanie szkoleń prowadzonych w oparciu o role pomaga zapewnić, że ich treść pozostanie aktualna i skuteczna. Do zdarzeń, które mogą spowodować konieczność aktualizacji treści szkolenia dotyczącego ról, należą między innymi: ocena lub wyniki audytu, incydenty lub naruszenia bezpieczeństwa, zmiany w obowiązujących przepisach prawa, rozporządzeniach, dyrektywach, regulacjach, polityce, standardach i wytycznych.

Zabezpieczenia powiązane: AC-3, AC-17, AC-22, AT-2, AT-4, CP-3, IR-2, IR-4, IR-7, IR-9, PL-4, PM-13, PM- 23, PS-7, PS-9, SA-3, SA-8, SA-11, SA-16, SR-5, SR-6, SR-11.

Zabezpieczenia rozszerzone:

(1) SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH | ZABEZPIECZENIA ŚRODOWISKOWE

Zapewnienie [***Realizacja: personel lub role określone przez organizację***] **wstępnego i** [***Realizacja: częstotliwość określona przez organizację***] **szkolenia w zakresie zatrudniania i działania zabezpieczeń środowiskowych.**

Omówienie: Zabezpieczenia środowiskowe obejmują urządzenia lub systemy gaśnicze i wykrywające pożar, systemy tryskaczowe, podręczne gaśnice, stałe węże pożarnicze, czujki dymu, czujki temperatury lub wilgotność, ogrzewanie, wentylację, klimatyzację i zasilanie w obrębie obiektu.

Zabezpieczenia powiązane: PE-1, PE-11, PE-13, PE-14, PE-15.

(2) SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH | ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO

Zapewnienie [***Realizacja: personel lub role określone przez organizację***] **wstępnego i [Realizacja:** ***częstotliwość określona przez organizację***] **szkolenia w zakresie ustanawiania i eksploatacji środków bezpieczeństwa fizycznego.**

Omówienie: Środki bezpieczeństwa fizycznego obejmują fizyczne urządzenia kontroli dostępu, fizyczne alarmy przeciwwłamaniowe i wykrywające, procedury operacyjne dla pracowników ochrony obiektu oraz sprzęt do monitorowania lub nadzoru.

Zabezpieczenia powiązane: PE-2, PE-3, PE-4.

(3) SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH | ĆWICZENIA PRAKTYCZNE

Zapewnienie praktycznych ćwiczeń z zakresu bezpieczeństwa i ochrony prywatności, które wzmacniają cele szkoleniowe.

Omówienie: Praktyczne ćwiczenia z zakresu bezpieczeństwa obejmują szkolenia dla programistów, które dotyczą symulowanych ataków wykorzystujących typowe luki w oprogramowaniu lub ataków typu „spear phishing" lub „whale phishing" i są skierowane do liderów zespołów lub kadry kierowniczej. Praktyczne ćwiczenia z zakresu ochrony prywatności obejmują moduły z quizami dotyczącymi identyfikacji i przetwarzania danych osobowych w różnych scenariuszach lub scenariuszami dotyczącymi przeprowadzania ocen wpływu na prywatność.

Zabezpieczenia powiązane: Brak.

(4) SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH | PODEJRZANA TRANSMISJA I ANOMALIE ZACHOWANIA SYSTEMU

[Wycofane: Włączone do AT-2(4)].

(5) SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH | PRZETWARZANIE DANYCH OSOBOWYCH

Zapewnienie [***Realizacja: personel lub role określone przez organizację***] **wstępnego szkolenia z [Realizacja: *częstotliwość określona przez organizację*] w zakresie wykorzystywania i przetwarzania danych osobowych oraz transparentności zabezpieczeń.**

Omówienie: Przetwarzanie danych osobowych i transparentność zabezpieczeń obejmują upoważnienie organizacji do przetwarzania danych osobowych i celów przetwarzania danych osobowych. Szkolenie w zakresie przetwarzania danych w oparciu o role dotyczy rodzajów informacji, które mogą stanowić informacje możliwe do zidentyfikowania, oraz ryzyka, względów i obowiązków związanych z ich przetwarzaniem. Takie szkolenie uwzględnia również uprawnienia do przetwarzania informacji możliwych do zidentyfikowania, udokumentowanych w polityce prywatności i zawiadomieniach, systemie zawiadomień o rejestrach, ocenach wpływu na prywatność, kontraktach, umowach o wymianie informacji, protokołach ustaleń i/lub innej dokumentacji.

Zabezpieczenia powiązane: PKT-2, PKT-3, PT-5, PT-6.

Referencje: [OMB A-130], [NIST SP 800-50], [NIST SP 800-181].

AT-4 DOKUMENTACJA SZKOLENIOWA

Zabezpieczenie podstawowe:

a. Dokumentowanie i monitorowanie działań szkoleniowych w zakresie bezpieczeństwa informacji i ochrony prywatności, w tym szkolenia w zakresie bezpieczeństwa i świadomości prywatności oraz szkolenia w zakresie bezpieczeństwa i ochrony prywatności w oparciu o konkretne role; oraz

b. Zachowywanie indywidualnych zapisów szkoleń w [*Realizacja: okres czasu określony przez organizację*].

Omówienie: Dokumentacja dotycząca szkoleń specjalistycznych może być przechowywana przez poszczególnych przełożonych według uznania organizacji.

Zabezpieczenia powiązane: AT-2, AT-3, CP-3, IR-2, PM-14, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130].

AT-5 UTRZYMYWANIE KONTAKTÓW Z ZESPOŁAMI I STOWARZYSZENIAMI SPECJALIZUJĄCYMI SIĘ W CYBERBEZPIECZEŃSTWIE

[Wycofane: Włączone do PM-15].

AT-6 INFORMACJE ZWROTNE O SZKOLENIACH

Zabezpieczenie podstawowe: Przekazywanie informacji zwrotnych o wynikach szkoleń organizacyjnych następującym pracownikom [*Realizacja: częstotliwość określona przez organizację*]*:* [*Realizacja: personel określony przez organizację*]*:* [*Realizacja: personel określony przez organizację*].

Omówienie: Informacje zwrotne o szkoleniach obejmują wyniki szkoleń uświadamiających i wyniki szkoleń opartych na roli. Wyniki szkoleń, w szczególności niepowodzenia personelu w pełnieniu kluczowych ról, mogą wskazywać na potencjalnie poważny problem. Dlatego ważne jest, aby kierownictwo wyższego szczebla było świadome takich sytuacji, tak, aby mogło podjąć odpowiednie działania zaradcze. Informacje zwrotne ze szkoleń wspomagają ocenę i aktualizację szkoleń organizacyjnych opisanych w zabezpieczeniach rozszerzonych AT-2b i AT-3b.

Zabezpieczenia powiązane: Brak.

Zabezpieczenia rozszerzone: Brak.

KATEGORIA AU - AUDYT I ROZLICZALNOŚĆ

AU-1 POLITYKA I PROCEDURY

Zabezpieczenie podstawowe:

a. Opracowywanie, dokumentowanie i rozpowszechnianie wśród [*Realizacja: personel lub role określone przez organizację*]*:*

   1. [*Wybór (jeden lub więcej): poziom organizacji; poziom misji/procesu biznesowego; poziom systemu*] polityki audytu i rozliczalności, która:

      (a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami; oraz

      (b) Jest zgodna z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi; oraz

   2. Procedur ułatwiających realizacje polityki audytu i rozliczalności oraz powiązanych zabezpieczeń w zakresie audytu i rozliczalności;

b. Wyznaczanie [*Realizacja: osoba wyznaczona przez organizację*] do zarządzania rozwojem, dokumentacją i rozpowszechnianiem polityki i procedur audytu oraz rozliczalności; oraz

c. Przeglądanie i aktualizowanie bieżącej:

   1. Polityki audytu i rozliczalności z [Realizacja: *częstotliwość określona przez organizację*] i następujących [*Realizacja: zdarzenia określone przez organizację*]; oraz

   2. Procedur dotyczących audytu i rozliczalności z [Realizacja: *częstotliwość określona przez organizację*] i następujących [*Realizacja: zdarzenia określone przez organizację*].

Omówienie: Polityka i procedury w zakresie audytu i rozliczalności dotyczą zabezpieczeń w kategorii *Audyt i rozliczalność* (AU) (które są wdrażane w ramach

systemów i organizacji. Strategia zarządzania ryzykiem jest ważnym czynnikiem przy tworzeniu takich polityk i procedur. Polityki i procedury przyczyniają się do zapewnienia bezpieczeństwa i ochrony prywatności. Dlatego ważne jest, aby programy bezpieczeństwa i ochrony prywatności były opracowywane wspólnie przy kształtowaniu polityki i procedur audytu i rozliczalności. Polityki i procedury dotyczące programów bezpieczeństwa i ochrony prywatności na poziomie organizacji są ogólnie rzecz biorąc preferowane i mogą wyeliminować potrzebę tworzenia polityk i procedur specyficznych dla danej misji lub systemu. Polityka ta może stanowić część ogólnej polityki bezpieczeństwa i ochrony prywatności lub być reprezentowana przez wiele polityk, które odzwierciedlają złożoną naturę organizacji. Procedury mogą być ustanowione dla programów bezpieczeństwa i ochrony prywatności, dla misji lub procesów biznesowych oraz dla systemów, jeśli to konieczne. Procedury opisują sposób wdrażania zasad lub zabezpieczeń i mogą być skierowane do osoby lub roli, która jest przedmiotem procedury. Procedury mogą być udokumentowane w planach bezpieczeństwa i ochrony prywatności systemu lub w jednym lub kilku oddzielnych dokumentach.

Zdarzenia, które mogą spowodować konieczność aktualizacji polityki i procedur audytu i rozliczalności, obejmują ocenę lub wyniki audytu, incydenty lub naruszenia bezpieczeństwa, lub zmiany w obowiązujących przepisach prawa, rozporządzeniach, dyrektywach, regulacjach, zasadach, standardach i wytycznych.

Oświadczenie o wprowadzeniu zabezpieczeń nie jest równoznaczne z ustanowieniem polityki lub procedury organizacyjnej.

Zabezpieczenia powiązane: PM-9, PS-8, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [NSC 800-12], [NIST SP 800-30], [NIST SP 800-39], [NIST SP 800-100].

AU-2 AUDYT ZDARZEŃ

Zabezpieczenie podstawowe:

a. Określenie rodzajów zdarzeń, które system jest w stanie kontrolować na potrzeby funkcji audytu: [*Realizacja: zdefiniowane przez organizację typy zdarzeń, które system jest w stanie rejestrować*];

b. Koordynowanie funkcji rejestrowania zdarzeń z innymi jednostkami organizacyjnymi wymagającymi informacji związanych z audytem w celu prowadzenia i informowania o kryteriach wyboru zdarzeń, które mają być rejestrowane;

c. Określanie następujących typów zdarzeń do logowania w systemie: [*Realizacja: zdefiniowane przez organizację typy zdarzeń (podzbiór typów zdarzeń zdefiniowanych w zabezpieczeniu rozszerzonym AU-2a.) wraz z częstotliwością (lub sytuacją wymagającą) logowania dla każdego zidentyfikowanego typu zdarzenia*];

d. Przedstawianie uzasadnień, dlaczego rodzaje zdarzeń wybrane do logowania uznaje się za odpowiednie do celów badania zdarzeń po fakcie; oraz

e. Przeglądanie i aktualizacja typów zdarzeń wybranych do logowania z [*Realizacja: częstotliwość zdefiniowana przez organizację*].

Omówienie: Zdarzenie jest obserwowalnym zajściem zaistniałym w systemie. Rodzaje zdarzeń, które wymagają rejestrowania, to zdarzenia istotne i znaczące dla bezpieczeństwa systemów i prywatności osób. Rejestrowanie zdarzeń wspiera również konkretne potrzeby w zakresie monitorowania i audytu. Typy zdarzeń obejmują zmiany haseł, nieudane logowanie lub nieudany dostęp związany z systemami, zmiany atrybutów bezpieczeństwa lub prywatności, korzystanie z uprawnień administracyjnych, korzystanie z poświadczeń weryfikacji tożsamości osobistej, zmiany w zakresie danych, parametry zapytań lub korzystanie z poświadczenia zewnętrznego. Określając zestaw typów zdarzeń, które wymagają

logowania, organizacje biorą pod uwagę monitorowanie i audyty odpowiednie dla każdego z zabezpieczeń, które mają być wdrożone. Dla kompletności, rejestracja zdarzeń obejmuje wszystkie protokoły, które są operacyjne i obsługiwane przez system.

Aby zrównoważyć wymagania dotyczące monitorowania i audytu z innymi potrzebami systemu, rejestracja zdarzeń wymaga określenia podzbioru typów zdarzeń, które są rejestrowane w danym momencie. Na przykład, organizacje mogą określić, że systemy potrzebują możliwości rejestrowania każdego dostępu do pliku, który zakończył się sukcesem lub niepowodzeniem, ale nie aktywują tej możliwości, z wyjątkiem szczególnych okoliczności wynikających z potencjalnego obciążenia dla wydajności systemu. Rodzaje zdarzeń, które organizacje chcą rejestrować, mogą się zmienić. Przeglądanie i aktualizacja zbioru rejestrowanych zdarzeń jest konieczna, aby zapewnić, że zdarzenia te pozostają istotne i nadal wspierają potrzeby organizacji. Organizacje rozważają, w jaki sposób rodzaje rejestrowanych zdarzeń mogą ujawniać informacje o osobach, które mogą stwarzać zagrożenie dla prywatności, oraz w jaki sposób najlepiej ograniczyć takie ryzyko. Na przykład, istnieje możliwość ujawnienia informacji umożliwiających identyfikację osób w ścieżce audytu, w szczególności jeżeli zdarzenie związane z rejestrowaniem jest oparte na wzorcach lub czasie użytkowania.

Wymagania dotyczące rejestrowania zdarzeń, w tym konieczność rejestrowania określonych typów zdarzeń, mogą być przywoływane w innych zabezpieczeniach i zabezpieczeniach rozszerzonych. Obejmują one zabezpieczenia AC-2(4), AC-3(10), AC-6(9), AC-17(1), CM-3f, CM-5(1), IA-3(3.b), MA-4(1), MP-4(2), PE-3, PM-21, PT-7, RA-8, SC-7(9), SC-7(15), SI-3(8), SI-4(22), SI-7(8) oraz SI-10(1). Organizacje obejmują rodzaje zdarzeń, które są wymagane przez obowiązujące prawo, zarządzenia, dyrektywy, zasady, regulacje, standardy i wytyczne. Zapisy audytowe mogą być generowane na różnych poziomach, w tym na poziomie pakietów, gdy informacje przechodzą przez sieć. Wybór odpowiedniego poziomu rejestrowania zdarzeń jest ważną częścią możliwości monitorowania i audytu i może zidentyfikować pierwotne

przyczyny problemów. Definiując typy zdarzeń, organizacje biorą pod uwagę rejestrację niezbędną do uwzględnienia powiązanych typów zdarzeń, takich jak kroki w procesach rozproszonych, opartych na transakcjach i działaniach, które występują w architekturach zorientowanych na usługi.

Zabezpieczenia powiązane: AC-2, AC-3, AC-6, AC-7, AC-8, AC-16, AC-17, AU-3, AU-4, AU-5, AU-6, AU-7, AU- 11, AU-12, CM-3, CM-5, CM-6, CM-13, IA-3, MA-4, MP-4, PE-3, PM-21, PT-2, PT-7, RA-8, SA-8, SC- 7, SC-18, SI-3, SI-4, SI-7, SI-10, SI-11.

Zabezpieczenia rozszerzone:

(1) AUDYT ZDARZEŃ | KOMPILACJA ZAPISÓW AUDYTU Z WIELU ŹRÓDEŁ

[Wycofane: Włączone do AU-12].

(2) AUDYT ZDARZEŃ | WYBÓR ZDARZEŃ AUDYTOWYCH WEDŁUG KOMPONENTÓW

[Wycofane: Włączone do AU-12].

(3) AUDYT ZDARZEŃ | OPINIE I AKTUALIZACJE

[Wycofane: Włączone do AU-2].

(4) AUDYT ZDARZEŃ | UPRZYWILEJOWANE FUNKCJE

[Wycofane: Włączone do AC-6(9)]

Referencje: [OMB A-130], [NIST SP 800-92].

AU-3 ZAWARTOŚĆ REJESTRÓW AUDYTU

Zabezpieczenie podstawowe: Zapewnienie, że zapisy z audytu zawierają informacje, które ustalają:

a. Jakiego rodzaju zdarzenie miało miejsce;

b. Kiedy zdarzenie miało miejsce;

c. Gdzie to zdarzenie miało miejsce;

d. Źródło zdarzenia;

e. Rezultaty zdarzenia; oraz

f. Tożsamość wszelkich osób, podmiotów lub przedmiotów/podmiotów związanych ze zdarzeniem.

Omówienie: Zawartość zapisów audytowych, które mogą być niezbędne do obsługi funkcji audytowej, obejmuje opisy zdarzeń (pozycja a), znaczniki czasu (pozycja b), adresy źródłowe i docelowe (pozycja c), identyfikatory użytkownika lub procesu (pozycje d oraz f), wskazania powodzenia lub niepowodzenia (pozycja e) oraz odpowiednie nazwy plików (pozycje a, c, e oraz f). Wyniki zdarzenia obejmują wskaźniki powodzenia lub porażki zdarzenia oraz wyniki specyficzne dla danego zdarzenia, takie jak bezpieczeństwo systemu i zachowanie prywatności po wystąpieniu zdarzenia. Organizacje biorą pod uwagę, w jaki sposób zapisy z audytu mogą ujawnić informacje o osobach, które mogą stwarzać zagrożenie dla prywatności i jak najlepiej ograniczyć takie ryzyko. Na przykład, istnieje możliwość ujawnienia informacji umożliwiających identyfikację osób w ścieżce audytu, w szczególności jeśli ścieżka audytu wprowadza dane lub jest oparta na wzorcach lub czasie użytkowania.

Zabezpieczenia powiązane: AU-2, AU-8, AU-12, AU-14, MA-4, PL-9, SA-8, SI-7, SI-11.

Zabezpieczenia rozszerzone:

(1) ZAWARTOŚĆ REJESTRÓW AUDYTU | DODATKOWE INFORMACJE KONTROLNE

Tworzenie zapisów audytu zawierających następujące dodatkowe informacje: [***Realizacja: informacje dodatkowe określone przez organizację***]**.**

Omówienie: Możliwość dodawania informacji generowanych w rekordach audytowych jest uzależniona od funkcjonalności systemu w zakresie konfiguracji zawartości rekordów audytowych. Organizacje mogą uwzględniać dodatkowe informacje w rekordach audytowych, w tym m.in. przywołane reguły kontroli dostępu lub kontroli przepływu oraz indywidualne tożsamości użytkowników kont grupowych. Organizacje mogą również rozważyć ograniczenie dodatkowych informacji w rekordach audytowych tylko do tych informacji, które są wyraźnie potrzebne do spełnienia wymagań audytu. Ułatwia to korzystanie ze ścieżek audytu i dzienników audytów poprzez nieuwzględnianie w dokumentacji audytowej informacji, które mogą potencjalnie wprowadzać w błąd, utrudniać zlokalizowanie interesujących nas informacji lub zwiększać zagrożenie dla danych osobowych.

Zabezpieczenia powiązane: Brak.

(2) ZAWARTOŚĆ REJESTRÓW AUDYTU | CENTRALNE ZARZĄDZANIE TREŚCIĄ PLANOWANEGO REJESTRU AUDYTU

[Wycofane: Włączone do PL-9].

(3) ZAWARTOŚĆ REJESTRÓW AUDYTU | OGRANICZENIE INFORMACJI UMOŻLIWIAJĄCYCH IDENTYFIKACJĘ OSÓB

Ograniczenie informacji umożliwiających identyfikację osób zawartych w dokumentacji z audytu do następujących elementów określonych w ocenie ryzyka naruszenia prywatności: [***Realizacja: elementy określone przez organizację***]**.**

Omówienie: Ograniczenie informacji umożliwiających identyfikację osób w dokumentacji audytowej, gdy informacje takie nie są potrzebne do celów operacyjnych, pomaga zmniejszyć poziom zagrożenia prywatności stwarzanego przez system.

Zabezpieczenia powiązane: RA-3.

Referencje: [OMB A-130], [IR 8062].

AU-4 POJEMNOŚĆ PAMIĘCI ZAPISÓW AUDYTU

Zabezpieczenie podstawowe: Przydzielenie miejsca na przechowywanie dziennika audytów, aby pomieścić [*Realizacja: wymagania dotyczące przechowywania dziennika audytów określone przez organizację*].

Omówienie: Organizacje biorą pod uwagę rodzaje rejestrów audytowych, które mają być wykonywane, oraz wymogi dotyczące przetwarzania rejestrów audytowych przy przydzielaniu pojemności magazynowej rejestrów audytowych. Przydzielenie wystarczającej pojemności do przechowywania dzienników audytowych zmniejsza prawdopodobieństwo przekroczenia tej zdolności i potencjalnej utraty lub zmniejszenia zdolności w zakresie pozyskiwania danych z audytów.

Zabezpieczenia powiązane: AU-2, AU-5, AU-6, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4.

Zabezpieczenia rozszerzone:

(1) POJEMNOŚĆ PAMIĘCI ZAPISÓW AUDYTU | TRANSFER REKORDÓW DO ALTERNATYWNYCH URZĄDZEŃ MAGAZYNUJĄCYCH

Przenoszenie dzienników audytowych z częstotliwością [***Realizacja: częstotliwość zdefiniowana przez organizację***] **do innego systemu, komponentu systemu lub nośnika innego niż system lub komponent systemu przeprowadzającego logowanie.**

Omówienie: Transfer dzienników audytowych, znany również jako "off-loading", jest powszechnym procesem w systemach o ograniczonych możliwościach przechowywania dzienników audytowych i tym samym wspiera ich dostępność. Początkowy zapis dziennika audytu jest wykorzystywany jedynie przejściowo do czasu, gdy system będzie mógł komunikować się z systemem wtórnym lub alternatywnym przydzielonym do zapisu dziennika audytu, w którym to momencie dzienniki audytu są przenoszone. Przenoszenie dzienników audytów do miejsca alternatywnego jest podobne do zabezpieczenia rozszerzonego AU-9(2), ponieważ dzienniki audytów są przenoszone do innej jednostki. Celem

wyboru AU-9(2) jest jednak ochrona poufności i integralności rejestrów audytu. Organizacje mogą wybrać zarówno zabezpieczenie rozszerzone w celu uzyskania korzyści w postaci zwiększonej pojemności pamięci dzienników audytu jak i zabezpieczenie pozwalające na zachowanie poufności, integralności i dostępności dokumentacji i dzienników zapisów audytu.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

AU-5 REAKCJA NA BŁĘDY PROCESÓW AUDYTU

Zabezpieczenie podstawowe:

a. Alarmowanie [*Realizacja: określonego przez organizację personelu lub ról*] w ramach [*Realizacja: określony przez organizację okres czasu*] w przypadku niewykonania procesów audytu; oraz

b. Podejmowanie następujących dodatkowych działań: [*Realizacja: dodatkowe działania zdefiniowane przez organizację*].

Omówienie: Niewykonanie procesów audytu obejmuje błędy programowe i sprzętowe, awarie mechanizmów przechwytywania dzienników audytów oraz osiągnięcie lub przekroczenie pojemności pamięci masowej dzienników audytów. Organizacje mogą zdefiniować dodatkowe działania dla dziennika audytu w zależności od rodzaju i lokalizacji niepowodzenia, oraz powagi lub kombinacji tych czynników. Gdy niepowodzenie procesu zapisu dziennika audytu jest związane z przechowywaniem, odpowiedź jest wykonywana dla repozytorium zapisu dziennika audytu (tj. odrębnego komponentu systemu, w którym przechowywane są dzienniki audytu), systemu, w którym przechowywane są dzienniki audytu, całkowitej pojemności pamięci dziennika audytu organizacji (tj. wszystkich repozytoriów zapisu dziennika audytu łącznie) lub wszystkich trzech powyższych obiektów. Organizacje mogą podjąć decyzję o niepodejmowaniu żadnych dodatkowych działań po dokonaniu powiadomienia wyznaczonych ról lub personelu.

Zabezpieczenia powiązane: AU-2, AU-4, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4, SI-12.

Zabezpieczenia rozszerzone:

(1) REAKCJA NA BŁĘDY PROCESÓW AUDYTU | OSTRZEŻENIA DOTYCZĄCE LIMITU PAMIĘCI PRZECHOWYWANIA REKORDÓW AUDYTU

Ostrzeganie [***Realizacja: określonego przez organizację personelu, ról i/lub lokalizacji***] **w ciągu** [***Realizacja: określony przez organizację okres czasu***]**, kiedy przydzielona pojemność pamięci masowej dziennika audytu osiągnie**

[***Realizacja: określony przez organizację procent***] **maksymalnej pojemności pamięci masowej dziennika audytu.**

Omówienie: Organizacje mogą posiadać wiele repozytoriów dzienników audytów rozmieszczonych na wielu komponentach systemu, przy czym każde z nich może mieć inną pojemność pamięci masowej.

Zabezpieczenia powiązane: Brak.

(2) REAKCJA NA BŁĘDY PROCESÓW AUDYTU | ALERTY CZASU RZECZYWISTEGO

W ciągu [***Realizacja: zdefiniowany przez organizację okres czasu rzeczywistego***] **do** [***Realizacja: zdefiniowany przez organizację personel, role i/lub lokalizacje***] **powiadomienie o wystąpieniu następujących zdarzeń niepowodzeń audytu: [Realizacja: *zdefiniowany przez organizację rejestr zdarzeń związanych z rejestrowaniem audytów wymagających alertów w czasie rzeczywistym*].**

Omówienie: Alerty dostarczają organizacjom pilnych wiadomości. Alerty w czasie rzeczywistym dostarczają tych wiadomości z największą możliwą szybkością (tj. czas od wykrycia zdarzenia do otrzymania alertu wynosi kilka sekund lub mniej).

Zabezpieczenia powiązane: Brak.

(3) REAKCJA NA BŁĘDY PROCESÓW AUDYTU | KONFIGUROWALNE PROGI NATĘŻENIA RUCHU

Egzekwowanie konfigurowalnych progów natężenia ruchu sieciowego odzwierciedlających limity pojemności pamięci masowej dziennika audytu oraz [***Wybór: odrzucenie; opóźnienie***] **ruchu sieciowego powyżej tych progów.**

Omówienie: Organizacje mają możliwość odrzucenia lub opóźnienia przetwarzania ruchu sieciowego, jeżeli informacje z dziennika zabezpieczeń tego ruchu zostaną uznane za przekraczające pojemność pamięci masowej funkcji dziennika zabezpieczeń systemu. Odpowiedź na odrzucenie lub opóźnienie jest wyzwalana przez ustalone organizacyjne progi natężenia ruchu, które mogą być

dostosowywane na podstawie zmian w pojemności pamięci masowej dziennika audytowego.

Zabezpieczenia powiązane: Brak.

(4) REAKCJA NA BŁĘDY PROCESÓW AUDYTU | WYŁĄCZENIE W PRZYPADKU AWARII

Wywołanie [*Wybór: pełne wyłączenie systemu; częściowe wyłączenie systemu; awaryjny tryb pracy z ograniczoną dostępnością funkcji misji lub działalności biznesowych*] w przypadku [*Realizacja: niepowodzenie audytu zdefiniowane przez organizację*], chyba, że istnieje alternatywna możliwość prowadzenia audytów.

Omówienie: Organizacje określają rodzaje niepowodzeń rejestru audytowego, które mogą powodować automatyczne wyłączenia systemu lub awarie. Ze względu na znaczenie zapewnienia misji i ciągłości biznesowej, organizacje mogą określić, że charakter awarii rejestru audytowego nie jest na tyle poważny, aby uzasadniał całkowite wyłączenie systemu wspierającego podstawową misję i funkcje biznesowe organizacji. W takich przypadkach, częściowe wyłączenie systemu lub praca w trybie awaryjnym z ograniczonymi możliwościami może być realną alternatywą.

Zabezpieczenia powiązane: AU-15.

(5) REAKCJA NA BŁĘDY PROCESÓW AUDYTU | ZDOLNOŚĆ ALTERNATYWNEGO PROWADZENIA REJESTRU AUDYTÓW

Zapewnienie możliwości alternatywnego rejestrowania audytów w przypadku awarii podstawowej funkcji rejestrowania audytów, która implementuje [*Realizacja: zdefiniowana przez organizację funkcja alternatywnego rejestrowania audytów*].

Omówienie: Ponieważ funkcja alternatywnego rejestrowania audytów może być krótkoterminowym rozwiązaniem zabezpieczającym stosowanym do czasu usunięcia usterki w podstawowej funkcji rejestrowania audytów, organizacje

mogą określić, że funkcja alternatywnego rejestrowania audytów musi zapewniać tylko podzbiór podstawowej funkcji rejestrowania audytów, na który wpływ ma usterka.

Zabezpieczenia powiązane: AU-9.

Referencje: Brak.

AU-6 PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE

Zabezpieczenie podstawowe:

a. Przegląd i analiza zapisów z audytu systemu [*Realizacja: częstotliwość określona przez organizację*] pod kątem wskazań [*Realizacja: działalność określona przez organizację, jako nieodpowiednia lub nietypowa*] oraz potencjalnego wpływu działalności nieodpowiedniej lub nietypowej;

b. Zgłoszenie ustaleń do [*Realizacja: personel lub role określone przez organizację*]*;* oraz

c. Dostosowanie poziomu przeglądu dokumentacji audytowej, analizy i sprawozdawczości w ramach systemu w przypadku zmiany ryzyka w oparciu o informacje dotyczące egzekwowania prawa, informacje wywiadowcze lub inne wiarygodne źródła informacji.

Omówienie: Przegląd dokumentacji audytowej, analiza i raportowanie obejmuje rejestrowanie informacji związanych z bezpieczeństwem i ochroną prywatności, prowadzone przez organizacje, w tym rejestrowanie wynikające z monitorowania korzystania z konta, dostępu zdalnego, łączności bezprzewodowej, połączeń z urządzeniami mobilnymi, ustawień konfiguracyjnych, inwentaryzacji komponentów systemu, korzystania z narzędzi utrzymaniowych i obsługi zdalnej, dostępu fizycznego, pomiaru temperatury i wilgotności, dostarczania i usuwania sprzętu, komunikacji na interfejsach systemowych oraz korzystania z kodu mobilnego lub protokołu VoIP (*ang. Voice over Internet Protocol*). Ustalenia można zgłaszać jednostkom organizacyjnym, w tym zespołowi reagowania na incydenty, działowi pomocy technicznej oraz biurom bezpieczeństwa i ochrony danych osobowych. Jeżeli organizacjom nie wolno przeglądać i analizować zapisów z audytu lub nie są one w stanie prowadzić takich działań, przegląd lub analizę mogą przeprowadzić inne organizacje, które uzyskały takie uprawnienia. Częstotliwość, zakres i/lub szczegółowość przeglądu, analizy i raportowania zapisów z audytów mogą być dostosowane do potrzeb organizacji w oparciu o otrzymane informacje.

Zabezpieczenia powiązane: AC-2, AC-3, AC-5, AC-6, AC-7, AC-17, AU-7, AU-16, CA-2, CA-7, CM-2, CM-5, CM-6, CM-10, CM-11, IA-2, IA-3, IA-8, IR-5, MA-4, MP-4, PE-3, PE-6, RA-5, SA-8, SC-7, SI-3, SI-4, SI-7.

Zabezpieczenia rozszerzone:

(1) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | ZAUTOMATYZOWANA INTEGRACJA PROCESÓW

Integracja procesów przeglądu, analizy i raportowania zapisów audytowych za pomocą [***Realizacja: automatyczne mechanizmy zdefiniowane przez organizację***]**.**

Omówienie: Procesy organizacyjne, które korzystają ze zintegrowanego przeglądu, analizy i raportowania zapisów audytów, obejmują reagowanie na incydenty, stałe monitorowanie, planowanie awaryjne / ciągłość działania, dochodzenie i reagowanie na podejrzane działania oraz audyty.

Zabezpieczenia powiązane: PM-7.

(2) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | AUTOMATYCZNE ALARMY BEZPIECZEŃSTWA

[Wycofane: Włączone do SI-4].

(3) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | KORELACJA ZBIORÓW AUDYTU

Analizowanie i korelowanie zapisów z audytów w różnych repozytoriach w celu zwiększenia świadomości sytuacyjnej w całej organizacji.

Omówienie: Świadomość sytuacyjna w całej organizacji obejmuje świadomość we wszystkich trzech poziomach zarządzania ryzykiem (tzn. na poziomie organizacji, misji/procesów biznesowych i systemu informatycznego) i wspiera świadomość międzybranżową.

Zabezpieczenia powiązane: AU-12, IR-4.

(4) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | CENTRALNE PRZEGLĄDANIE I ANALIZY

Zapewnienie i wdrożenie możliwości centralnego przeglądania i analizowania zapisów audytowych z wielu komponentów systemu.

Omówienie: Zautomatyzowane mechanizmy do scentralizowanych przeglądów i analiz obejmują produkty z zakresu bezpieczeństwa informacji i zarządzania zdarzeniami.

Zabezpieczenia powiązane: AU-2, AU-12.

(5) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | ZINTEGROWANA ANALIZA ZAPISÓW Z AUDYTU

Integracja analizy zapisów z audytu z analizą [***Wybór (jeden lub więcej): informacje o skanowaniu podatności; dane o wydajności; informacje o monitorowaniu systemu;*** [***Realizacja: dane/informacje określone przez organizację zebrane z innych źródeł***]] **w celu dalszego zwiększenia możliwości identyfikacji niewłaściwych lub nietypowych działań.**

Omówienie: Zintegrowana analiza zapisów audytowych nie wymaga skanowania luk, generowania danych o wydajności ani monitorowania systemu. Zintegrowana analiza wymaga, aby analiza informacji generowanych podczas skanowania, monitorowania lub innych działań związanych z gromadzeniem danych była zintegrowana z analizą informacji z zapisów audytowych. Narzędzia dotyczące bezpieczeństwa informacji i zarządzania zdarzeniami mogą ułatwić agregację lub konsolidację zapisów audytowych z wielu komponentów systemu, a także korelację i analizę zapisów audytowych. Wykorzystanie standardowych skryptów analizy zapisów audytowych opracowanych przez organizacje (w razie potrzeby z korektą lokalnego skryptu) zapewnia bardziej ekonomiczne podejście do analizy zebranych informacji o zapisach audytowych. Korelacja informacji o rekordach audytowych z informacjami o skanowaniu podatności jest istotna dla określenia prawdziwości skanów podatności systemu oraz dla skorelowania

zdarzeń wykrycia ataku z wynikami skanowania. Korelacja z danymi o wydajności może ujawnić ataki typu Odmowa świadczenia usług (*ang. denial of service – DoS*) lub inne rodzaje ataków, które skutkują nieautoryzowanym wykorzystaniem zasobów. Korelacja z informacjami z monitoringu systemu może pomóc w wykryciu ataków i lepszym powiązaniu informacji z audytu z sytuacjami operacyjnymi.

Zabezpieczenia powiązane: AU-12, IR-4.

(6) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | KORELACJA AUDYTU Z MONITOROWANIEM FIZYCZNYM

Korelacja informacji z rejestrów audytowych z informacjami uzyskanymi z monitorowania dostępu fizycznego w celu dalszego zwiększenia zdolności do identyfikacji podejrzanych, niewłaściwych, nietypowych lub złośliwych działań.

Omówienie: Korelacja informacji o zapisach z monitorowania fizycznego z zapisami audytów z systemów może pomóc organizacjom w identyfikacji podejrzanych zachowań lub stanowić dowód takiego zachowania. Na przykład, korelacja tożsamości osoby fizycznej uzyskującej logiczny dostęp do niektórych systemów z dodatkowymi informacjami dotyczącymi bezpieczeństwa fizycznego, które osoba ta posiadała w obiekcie w momencie uzyskania logicznego dostępu, może być przydatna w dochodzeniu.

Zabezpieczenia powiązane: Brak.

(7) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | DOPUSZCZALNE DZIAŁANIA

Określić dozwolone działania dla każdego z [***Wybór (jeden lub więcej): proces systemowy; rola; użytkownik***] **związane z przeglądem, analizą i raportowaniem informacji z zapisów audytu.**

Omówienie: Organizacje określają dozwolone działania dla procesów systemowych, ról i użytkowników związane z przeglądem, analizą i raportowaniem zapisów audytowych poprzez działania związane z zarządzaniem

kontami systemowymi. Określenie dopuszczalnych działań odnoszących się do informacji uzyskanych z rejestrów audytowych jest sposobem na egzekwowanie zasady wiedzy koniecznej. Dozwolone działania są egzekwowane przez system i obejmują odczyt, zapis, wykonanie, dołączenie i usunięcie.

Zabezpieczenia powiązane: Brak.

(8) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | PEŁNA ANALIZA TEKSTU UPRZYWILEJOWANYCH POLECEŃ

Przeprowadzenie pełnej analizy tekstowej zarejestrowanych uprzywilejowanych poleceń w fizycznie odrębnym komponencie lub podsystemie systemu, lub w innym systemie, który jest dedykowany do tej analizy.

Omówienie: Pełna analiza tekstowa uprzywilejowanych poleceń wymaga odrębnego środowiska do analizy informacji uzyskanych z zapisów audytowych dotyczących uprzywilejowanych użytkowników (bez naruszania tych informacji) w systemie, w którym użytkownicy mają podwyższone uprawnienia, w tym możliwość wykonywania uprzywilejowanych poleceń. Analiza pełnotekstowa odnosi się do analizy, która uwzględnia pełny tekst uprzywilejowanych poleceń (tj. poleceń i parametrów), w przeciwieństwie do analizy, która uwzględnia tylko nazwę polecenia. Analiza pełnotekstowa obejmuje wykorzystanie dopasowania wzorców i heurystyki.

Zabezpieczenia powiązane: AU-3, AU-9, AU-11, AU-12.

(9) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | KORELACJA Z INFORMACJAMI UZYSKANYMI ZE ŹRÓDEŁ NIETECHNICZNYCH

Korelacja informacji ze źródeł nietechnicznych z informacjami z zapisów audytów w celu zwiększenia świadomości sytuacyjnej w całej organizacji.

Omówienie: Źródła nietechniczne obejmują np. dokumentację dotyczącą zasobów ludzkich, dokumentującą naruszenia zasad organizacyjnych (np.

przypadki molestowania seksualnego, niewłaściwe wykorzystanie zasobów informacji organizacyjnych). Takie informacje mogą prowadzić do ukierunkowanych wysiłków analitycznych mających na celu wykrycie potencjalnie złośliwych działań osób mających dostęp do informacji wrażliwych. Organizacje ograniczają dostęp do informacji, które są dostępne ze źródeł nietechnicznych ze względu na ich wrażliwy charakter. Ograniczony dostęp minimalizuje możliwość nieumyślnego ujawnienia informacji związanych z ochroną prywatności osobom, które nie mają potrzeby ich posiadania. Korelacja informacji ze źródeł nietechnicznych z informacjami z rejestrów audytowych ma miejsce zazwyczaj tylko wtedy, gdy osoby są podejrzane o udział w incydencie. Organizacje uzyskują poradę prawną przed rozpoczęciem takich działań.

Zabezpieczenia powiązane: PM-12.

(10) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | KORYGOWANIE POZIOMU AUDYTU

[Wycofane: Włączone do AU-6].

Referencje: [NIST SP 800-86], [NIST SP 800-101].

AU-7 REDUKCJA TREŚCI ZAPISÓW Z AUDYTU I GENEROWANIE RAPORTÓW

Zabezpieczenie podstawowe: Zapewnienie i wdrożenie redukcji treści zapisów audytowych i zdolności generowania raportów, które:

a. Wspierają przegląd treści zapisów z audytu na żądanie, analizę i wymogi w zakresie sprawozdawczości oraz badania powykonawcze po wystąpieniu incydentów; oraz

b. Nie zmieniają pierwotnej treści ani kolejności czasowej zapisów z audytu.

Omówienie: Redukcja treści zapisów audytowych jest procesem, który przetwarza zebrane informacje z dzienników audytowych i organizuje je w formacie podsumowującym, bardziej zrozumiałym dla analityków. Możliwości redukcji treści zapisów audytów i generowania raportów nie zawsze pochodzą z tego samego systemu lub z tych samych jednostek organizacyjnych, które prowadzą czynności związane z rejestrowaniem audytów. Możliwości redukcji treści zapisów audytowych obejmują nowoczesne techniki eksploracji danych z zaawansowanymi filtrami danych, w celu identyfikacji anomalii w zapisach audytowych. Możliwości generowania raportów przez system mogą być dostosowywane do indywidualnych potrzeb. Uporządkowanie rekordów audytowych w czasie może stanowić problem, jeśli ziarnistość znacznika czasowego w rekordzie jest niewystarczająca.

Zabezpieczenia powiązane: AC-2, AU-2, AU-3, AU-4, AU-5, AU-6, AU-12, AU-16, CM-5, IA-5, IR-4, PM-12, SI- 4.

Zabezpieczenia rozszerzone:

(1) REDUKCJA TREŚCI ZAPISÓW Z AUDYTU I GENEROWANIE RAPORTÓW | AUTOMATYZACJA PROCESU

Zapewnienie i wdrożenie możliwości przetwarzania, sortowania i wyszukiwania zapisów audytów interesujących nas zdarzeń w oparciu o następującą treść: [***Realizacja: pola zdefiniowane przez organizację w dokumentacji audytowej***]**.**

Omówienie: Interesujące zdarzenia można zidentyfikować na podstawie zawartości rejestrów audytowych, w tym zaangażowanych zasobów systemowych, udostępnionych obiektów informatycznych, tożsamości osób, rodzajów zdarzeń, lokalizacji zdarzeń, dat i godzin, adresów protokołu internetowego oraz powodzenia lub porażki zdarzenia. Organizacje mogą definiować kryteria zdarzeń w dowolnym wymaganym stopniu szczegółowości, np. lokalizacje wybierane przez ogólną lokalizację w sieci lub przez określony komponent systemu.

Zabezpieczenia powiązane: Brak.

(2) REDUKCJA TREŚCI ZAPISÓW Z AUDYTU I GENEROWANIE RAPORTÓW | AUTOMATYCZNE SORTOWANIE I WYSZUKIWANIE

[Wycofane: Włączone do AU-7(1)].

Referencje: Brak.

AU-8 ZNACZNIKI CZASU

Zabezpieczenie podstawowe:

a. Wykorzystanie wewnętrznych zegarów systemowych do generowania znaczników czasu dla rekordów audytów; oraz

b. Zapisywanie znaczników czasu dla rekordów audytowych, które spełniają [*Realizacja: zdefiniowana przez organizację granulacja pomiaru czasu*] i które wykorzystują uniwersalny czas koordynowany (UTC), mają stałe przesunięcie czasu lokalnego w stosunku do uniwersalnego czasu koordynowanego lub które zawierają przesunięcie czasu lokalnego, jako część znacznika czasu.

Omówienie: Znaczniki czasowe generowane przez system zawierają datę i czas. Czas jest powszechnie wyrażany, jako uniwersalny czas koordynowany (UTC), współczesna kontynuacja czasu uniwersalnego Greenwich (GMT), lub czas lokalny z przesunięciem względem UTC. Ziarnistość pomiarów czasu odnosi się do stopnia synchronizacji pomiędzy zegarami systemowymi, a zegarami referencyjnymi (np. zegary synchronizujące w ciągu setek milisekund lub dziesiątek milisekund). Organizacje mogą definiować różne granulacje czasu dla różnych elementów systemu. Obsługa czasu może być krytyczna dla innych funkcji bezpieczeństwa, takich jak zabezpieczenie dostępu oraz identyfikacja i uwierzytelnianie, w zależności od charakteru mechanizmów wykorzystywanych do obsługi tych funkcji.

Zabezpieczenia powiązane: AU-3, AU-12, AU-14, SC-45.

Zabezpieczenia rozszerzone:

(1) ZNACZNIKI CZASU | SYNCHRONIZACJA Z AUTORYZOWANYM ŹRÓDŁEM CZASU ODNIESIENIA

[Wycofane: Włączone do SC-45(1)]

(2) ZNACZNIKI CZASU | WTÓRNE ŹRÓDŁO CZASU ODNIESIENIA

[Wycofane: Włączone do SC-45(2)]

Referencje: Brak.

AU-9 OCHRONA INFORMACJI AUDYTOWYCH

Zabezpieczenie podstawowe:

a. Ochrona informacji audytowych i narzędzi rejestrujących audyt przed nieautoryzowanym dostępem, modyfikacją i usuwaniem; oraz

b. Alarmowanie [*Realizacja: zdefiniowany przez organizację personel lub role*] w przypadku wykrycia nieautoryzowanego dostępu, modyfikacji lub usunięcia informacji o audycie.

Omówienie: Informacje o audycie obejmują wszystkie informacje potrzebne do pomyślnego przeprowadzenia audytu działalności systemu, takie jak zapisy audytów, ustawienia dzienników audytów, raporty z audytów oraz informacje umożliwiające identyfikację osób. Narzędzia do rejestrowania audytów to programy i urządzenia służące do przeprowadzania audytu systemu i rejestrowania działań. Ochrona informacji audytowych skupia się na ochronie technicznej i ogranicza możliwość dostępu i przydzielania narzędzi rejestrujących audyt do uprawnionych osób. Fizyczna ochrona informacji audytowych jest realizowana zarówno w ramach zabezpieczeń ochrony mediów, jak i zabezpieczeń ochrony fizycznej i środowiskowej.

Zabezpieczenia powiązane: AC-3, AC-6, AU-6, AU-11, AU-14, AU-15, MP-2, MP-4, PE-2, PE-3, PE-6, SA-8, SC-8, SI-4.

Zabezpieczenia rozszerzone:

(1) OCHRONA INFORMACJI AUDYTOWYCH | NOŚNIKI JEDNOKROTNEGO ZAPISU

Zapisywanie ścieżek audytu na wymuszonych sprzętowo nośnikach jednorazowego zapisu.

Omówienie: Zapisywanie ścieżek audytu na wymuszanych sprzętowo nośnikach jednorazowego zapisu dotyczy wstępnego generowania ścieżek audytu (tj. gromadzenia dokumentacji audytowej, która przedstawia informacje wykorzystywane do celów wykrywania, analizy i sprawozdawczości) oraz tworzenia kopii zapasowych tych ścieżek audytu. Zapisywanie ścieżek audytu na

wymuszanych sprzętowo nośnikach jednokrotnego zapisu nie ma zastosowania do wstępnej generacji zapisów z audytu przed ich zapisaniem do ścieżki audytu. Technologia zapisywania jednokrotnego i wielokrotnego odczytywana (*ang. Write-once, read-many - WORM*) obejmuje płyty kompaktowe (*CD-R*), płyty Blu-Ray (*BD-R*) oraz płyty DVD-R (*ang. Digital Versatile Disc-Recordable*).

Zabezpieczenia powiązane: AU-4, AU-5.

(2) OCHRONA INFORMACJI AUDYTOWYCH | BACKUP AUDYTU W ODSEPAROWANYM FIZYCZNIE SYSTEMIE / KOMPONENCIE

Przechowywanie zapisów z audytu [***Realizacja: częstotliwość określona przez organizację***] **w repozytorium, które jest fizycznie częścią innego systemu lub komponentu systemu niż system lub komponent będący przedmiotem audytu.**

Omówienie: Przechowywanie zapisów z audytu w repozytorium odrębnym od audytowanego systemu lub komponentu systemu pomaga zapewnić, że naruszenie audytowanego systemu nie spowoduje również ujawnienia zapisów z audytu. Przechowywanie zapisów z audytów w oddzielnych systemach fizycznych lub komponentach pozwala również na zachowanie poufności i integralności zapisów z audytów oraz ułatwia zarządzanie zapisami z audytów, jako działalnością całej organizacji. Przechowywanie zapisów z audytów w oddzielnych systemach lub komponentach dotyczy zarówno początkowego generowania, jak i tworzenia kopii zapasowych oraz długoterminowego przechowywania zapisów z audytów.

Zabezpieczenia powiązane: AU-4, AU-5.

(3) OCHRONA INFORMACJI AUDYTOWYCH | OCHRONA KRYPTOGRAFICZNA

Wdrożenie mechanizmów kryptograficznych w celu ochrony integralności informacji dotyczących audytu i narzędzi audytu.

Omówienie: Mechanizmy kryptograficzne stosowane do ochrony integralności informacji o audycie obejmują podpisane funkcje skrótu (*ang. hash*)

z wykorzystaniem kryptografii asymetrycznej. Umożliwia to dystrybucję klucza publicznego w celu weryfikacji informacji skrótu przy jednoczesnym zachowaniu poufności tajnego klucza używanego do generowania skrótu.

Zabezpieczenia powiązane: AU-10, SC-12, SC-13.

(4) OCHRONA INFORMACJI AUDYTOWYCH | DOSTĘP DO PODZBIORU UPRZYWILEJOWANYCH UŻYTKOWNIKÓW

Zezwolenie na dostęp do zarządzania funkcjami audytu tylko do [***Realizacja: zdefiniowany przez organizację podzbiór uprzywilejowanych użytkowników lub ról***]**.**

Omówienie: Osoby lub role mające uprzywilejowany dostęp do systemu, które są również przedmiotem audytu prowadzonego przez ten system, mogą wpływać na wiarygodność informacji z audytu poprzez blokowanie działań audytowych lub modyfikowanie zapisów z audytu. Wymóg, aby uprzywilejowany dostęp został dokładniej określony pomiędzy uprawnieniami związanymi z audytem, a innymi uprawnieniami, ogranicza liczbę użytkowników lub ról z uprawnieniami związanymi z audytem.

Zabezpieczenia powiązane: AC-5.

(5) OCHRONA INFORMACJI AUDYTOWYCH | PODWÓJNA AUTORYZACJA

Egzekwowanie podwójnej autoryzacji dla [***Wybór (jeden lub więcej): przemieszczenie; usunięcie***] **[Realizacja:** ***informacja o audycie zdefiniowana przez organizację*****].**

Omówienie: Organizacje mogą wybrać różne opcje wyboru dla różnych typów informacji o audycie. Podwójne mechanizmy autoryzacji (znane również, jako autoryzacja dwuosobowa) wymagają zgody dwóch upoważnionych osób do wykonywania funkcji audytowych. Aby zmniejszyć ryzyko zmowy, organizacje rozważają rotację obowiązków związanych z podwójną autoryzacją pomiędzy różnymi osobami. Organizacje nie wymagają mechanizmów podwójnej

autoryzacji, gdy do zapewnienia bezpieczeństwa publicznego i środowiskowego konieczne są natychmiastowe reakcje.

Zabezpieczenia powiązane: AC-3.

(6) OCHRONA INFORMACJI AUDYTOWYCH | DOSTĘP TYLKO DO ODCZYTU

Zezwolenie na dostęp tylko do odczytu do informacji o audycie [***Realizacja: zdefiniowany przez organizację podzbiór uprzywilejowanych użytkowników lub ról***]**.**

Omówienie: Ograniczenie do *tylko do odczytu* uprawnień uprzywilejowanych użytkowników lub ról pomaga ograniczyć potencjalne szkody dla organizacji, które mogą być inicjowane przez tych użytkowników lub role, takie jak usuwanie zapisów audytowych w celu ukrycia złośliwej działalności.

Zabezpieczenia powiązane: Brak.

(7) OCHRONA INFORMACJI AUDYTOWYCH | PRZECHOWYWANIE INFORMACJI NA KOMPONENTACH Z RÓŻNYMI SYSTEMAMI OPERACYJNYMI

Przechowywanie informacji o audycie na komponencie wykonującym inny system operacyjny niż system lub komponent będący przedmiotem audytu.

Omówienie: Przechowywanie informacji audytowych w komponencie systemu działającym w innym systemie operacyjnym zmniejsza ryzyko wystąpienia specyficznej dla tego systemu podatności, skutkującej naruszeniem zapisów audytu.

Zabezpieczenia powiązane: AU-4, AU-5, AU-11, SC-29.

Referencje: [FIPS 140-3], [FIPS 180-4], [FIPS 202].

AU-10 NIEZAPRZECZALNOŚĆ

Zabezpieczenie podstawowe: Dostarczenie niezbitych dowodów na to, że osoba (lub proces działający w imieniu osoby) wykonała [*Realizacja: działania zdefiniowane przez organizację, które mają być objęte zakazem odrzucania*].

Omówienie: Rodzaje indywidualnych działań objętych zasadą niezaprzeczalności obejmują tworzenie informacji, wysyłanie i odbieranie wiadomości oraz zatwierdzanie informacji. Niezaprzeczalność chroni przed roszczeniami autorów, którzy nie są twórcami określonych dokumentów, nadawców, którzy nie nadali wiadomości, odbiorców, którzy nie otrzymali wiadomości, oraz strony podpisujące, którzy nie podpisali dokumentów. Usługi niezaprzeczalności mogą być wykorzystane do ustalenia, czy informacje pochodzą od osoby, czy też osoba podjęła określone działania (np. wysłanie wiadomości e-mail, podpisanie umowy, zatwierdzenie wniosku o udzielenie zamówienia lub otrzymanie określonych informacji). Organizacje uzyskują usługi niezaprzeczalności poprzez zastosowanie różnych technik lub mechanizmów, w tym podpisów cyfrowych i cyfrowych potwierdzeń odbioru wiadomości.

Zabezpieczenia powiązane: AU-9, PM-12, SA-8, SC-8, SC-12, SC-13, SC-16, SC-17, SC-23.

Zabezpieczenia rozszerzone:

(1) NIEZAPRZECZALNOŚĆ | POŁĄCZENIE TOŻSAMOŚCI

(a) Połączenie tożsamości twórcy informacji z informacją z [***Realizacja: siła wiążąca określona przez organizację***]***;*** **oraz**

(b) Zapewnienie upoważnionym osobom środków umożliwiających ustalenie tożsamości twórcy informacji.

Omówienie: Połączenie tożsamości z informacjami wspiera wymagania audytu, które zapewniają personelowi organizacyjnemu środki do identyfikacji, kto opracował konkretne przekazane informacje. Organizacje określają i zatwierdzają

siłę przypisania wiążącej cechy między twórcą informacji, a informacjami w oparciu o kategorię bezpieczeństwa informacji i inne istotne czynniki ryzyka.

Zabezpieczenia powiązane: AC-4, AC-16.

(2) NIEZAPRZECZALNOŚĆ | POWIĄZANIE INFORMACJI Z TOŻSAMOŚCIĄ TWÓRCY

(a) Zatwierdzanie powiązania tożsamości twórcy informacji z informacjami z [***Realizacja: częstotliwość określona przez organizację***]**; oraz**

(b) Wykonywanie [***Realizacja: czynności zdefiniowane przez organizację***] ***w* przypadku błędu sprawdzania poprawności powiązania.**

Omówienie: Zatwierdzenie powiązania tożsamości twórcy informacji z informacjami uniemożliwia zmianę informacji pomiędzy procesem tworzenia, a recenzją. Poprawność wiązań można uzyskać na przykład poprzez zastosowanie kryptograficznych sum kontrolnych. Organizacje określają, czy oceny poprawności powiązań są odpowiedzią na żądania użytkowników, czy też są generowane automatycznie.

Zabezpieczenia powiązane: AC-3, AC-4, AC-16.

(3) NIEZAPRZECZALNOŚĆ |ŁAŃCUCH NADZORU

Utrzymywanie tożsamości recenzenta / wydawcy informacji w ramach ustalonego łańcucha dowodowego odnoszącego się do informacji poddanych przeglądowi lub opublikowaniu.

Omówienie: Łańcuch nadzoru jest procesem, który śledzi przepływ materiału dowodowego poprzez jego gromadzenie, zabezpieczanie i analizę cyklu życia, dokumentując każdą osobę, która zapoznawała się z materiałem dowodowym, datę i czas zebrania lub przekazania materiału dowodowego oraz cel przekazania. Jeżeli recenzent jest osobą lub jeżeli funkcja przeglądu jest zautomatyzowana, ale oddzielona od funkcji udostępniania lub przekazywania, system łączy tożsamość recenzenta informacji, które mają zostać udostępnione, z informacjami i etykietą informacyjną.

W przypadku recenzji prowadzonych przez człowieka, zachowanie referencji recenzentów lub wydawców zapewnia organizacji środki do identyfikacji, kto recenzował i publikował informacje. W przypadku przeglądów automatycznych recenzja zapewnia, że wykorzystywane są tylko zatwierdzone funkcje przeglądowe.

Zabezpieczenia powiązane: AC-4, AC-16.

(4) NIEZAPRZECZALNOŚĆ | POTWIERDZANIE TOŻSAMOŚCI PRZEGLĄDAJĄCEGO INFORMACJE

(a) Zatwierdzanie powiązania tożsamości recenzenta wiadomości z informacjami w punktach transferu lub udostępniania, przed ich udostępnieniem lub transferem pomiędzy [***Realizacja: zdefiniowane przez organizację domeny bezpieczeństwa***]***;*** **oraz**

(b) Wykonywanie [***Realizacja: czynności zdefiniowane przez organizację***] ***w*** **przypadku błędu potwierdzania (walidacji).**

Omówienie: Zatwierdzenie powiązania tożsamości recenzenta informacji z informacjami w punktach transferu lub udostępniania uniemożliwia nieuprawnioną modyfikację informacji pomiędzy udostępnieniem, a transferem lub publikacją. Potwierdzanie wiązań może być przeprowadzone przy użyciu kryptograficznych sum kontrolnych. Organizacje określają, czy potwierdzenia są odpowiedzią na żądania użytkowników, czy też są generowane automatycznie.

Zabezpieczenia powiązane: AC-4, AC-16.

(5) NIEZAPRZECZALNOŚĆ | PODPISY CYFROWE

[Wycofane: Włączone do SI-7].

Referencje: [FIPS 140-3], [FIPS 180-4], [FIPS 186-4], [FIPS 202], [NIST SP 800-177].

AU-11 RETENCJA ZAPISÓW AUDYTU

Zabezpieczenie podstawowe: Przechowywanie zapisów z audytu przez okres [*Realizacja: okres zdefiniowany przez organizację zgodnie z polityką przechowywania rejestru*] w celu zapewnienia wsparcia procesów dochodzeniowych dotyczących incydentów bezpieczeństwa oraz w celu spełnienia wymagań prawnych i organizacyjnych dotyczących przechowywania informacji.

Omówienie: Organizacje zachowują zapisy z audytów do czasu ustalenia, że zapisy te nie są już potrzebne do celów administracyjnych, prawnych, audytowych lub innych celów operacyjnych. Obejmuje to przechowywanie i dostępność dokumentacji audytowej związanej z wnioskami o dostęp do informacji publicznej, wezwaniami sądu i działaniami organów ścigania oraz uprawnionych podmiotów. Organizacje opracowują standardowe kategorie dokumentacji audytowej w odniesieniu do takich rodzajów działań oraz standardowe procesy reagowania dla każdego rodzaju działań.
Zabezpieczenia powiązane: AU-2, AU-4, AU-5, AU-6, AU-9, AU-14, MP-6, RA-5, SI-12.

Zabezpieczenia rozszerzone:

(1) RETENCJA ZAPISÓW Z AUDYTU | DŁUGOTERMINOWA ZDOLNOŚĆ DO ODZYSKU

Stosowanie przez organizację [***Realizacja: środki określone przez organizację***] ***w*** **celu zapewnienia możliwości odzyskania zapisów z audytu generowanych przez system.**

Omówienie: Organizacje muszą mieć dostęp i odczytywać zapisy z audytów wymagających długoterminowego przechowywania (w kolejności lat). Środki zastosowane w celu ułatwienia pobierania zapisów z audytów obejmują konwersję zapisów do nowszych formatów, przechowywanie sprzętu umożliwiającego odczytywanie zapisów oraz przechowywanie niezbędnej dokumentacji, aby pomóc personelowi w zrozumieniu sposobu interpretacji zapisów.

Zabezpieczenia powiązane: Brak.

Referencje: [OMB A-130].

AU-12 TWORZENIE ZAPISÓW AUDYTU

Zabezpieczenie podstawowe:

a. Udostępnianie możliwość generowania zapisów audytowych dla typów zdarzeń, które system jest w stanie audytować zgodnie z definicją zawartą w AU-2a w obszarze [*Realizacja: komponenty systemu zdefiniowane przez organizację*]*;*

b. Zezwolenie [*Realizacja: personel lub role zdefiniowane przez organizację*] na wybór typów zdarzeń, które mają być rejestrowane przez określone elementy systemu; oraz

c. Generowanie zapisów audytowych dla typów zdarzeń zdefiniowanych w AU-2c, które zawierają zawartość zapisów audytowych określonych w zabezpieczeniach AU-3.

Omówienie: Zapisy audytowe mogą być generowane z wielu różnych komponentów systemu. Typy zdarzeń określone w AU-2d są typami zdarzeń, dla których mają być generowane logi audytowe i stanowią podzbiór wszystkich typów zdarzeń, dla których system może generować zapisy audytowe.

Zabezpieczenia powiązane: AC-6, AC-17, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-14, CM-5, MA-4, MP-4, PM-12, SA-8, SC-18, SI-3, SI-4, SI-7, SI-10.

Zabezpieczenia rozszerzone:

(1) TWORZENIE ZAPISÓW AUDYTU | OGÓLNOSYSTEMOWE / SKORELOWANE W CZASIE ŚCIEŻKI AUDYTU

Kompilacja zapisów audytu z [***Realizacja: zdefiniowane przez organizację składniki systemu***] **do ogólnosystemowej (logicznej lub fizycznej) ścieżki audytu, która jest związana z czasem w ramach** [***Realizacja: zdefiniowany przez organizację poziom tolerancji dla relacji pomiędzy znacznikami czasu poszczególnych zapisów w ścieżce audytu***]**.**

Omówienie: Ścieżki audytu są powiązane z czasem, jeżeli znaczniki czasu w poszczególnych zapisach z audytów mogą być wiarygodnie powiązane ze

znacznikami czasu w innych zapisach z audytów, aby osiągnąć porządek czasowy zapisów w ramach tolerancji organizacyjnych.

Zabezpieczenia powiązane: AU-8, SC-45.

(2) TWORZENIE ZAPISÓW AUDYTU | UJEDNOLICONE FORMATY

Stworzenie ogólnosystemowej (logicznej lub fizycznej) ścieżki audytu składającej się z zapisów audytowych w znormalizowanym (ujednoliconym) formacie.

Omówienie: Dokumentacja audytowa zgodna ze wspólnymi standardami promuje interoperacyjność i wymianę informacji pomiędzy urządzeniami i systemami. Promowanie interoperacyjności i wymiany informacji ułatwia tworzenie informacji o zdarzeniach, które mogą być łatwo analizowane i skorelowane. Jeśli mechanizmy rejestracji nie są zgodne ze znormalizowanymi formatami, systemy mogą przekształcać pojedyncze zapisy z audytów na znormalizowane formaty podczas opracowywania ogólnosystemowych ścieżek audytu.

Zabezpieczenia powiązane: Brak.

(3) TWORZENIE ZAPISÓW AUDYTU | ZMIANY DOKONYWANE PRZEZ UPRAWNIONE OSOBY

Zapewnienie i wdrożenie zdolności [***Realizacja: osoby lub role określone przez organizację***] **do zmiany logowania, które ma być wykonywane na [Realizacja: *komponenty systemu określone przez organizację*] w oparciu o [Realizacja: *kryteria zdarzeń do wyboru określone przez organizację*] w ramach [Realizacja: *progi czasowe określone przez organizację*].**

Omówienie: Zezwolenie upoważnionym osobom na dokonywanie zmian w sposobie logowania do systemu pozwala organizacjom na rozszerzenie lub ograniczenie logowania w zależności od wymagań organizacyjnych. Logowanie, które jest ograniczone do ochrony zasobów systemu, może być rozszerzone

(tymczasowo lub na stałe) w celu uwzględnienia pewnych sytuacji zagrożenia. Ponadto, logowanie może być ograniczone do określonego zestawu typów zdarzeń, aby umożliwić redukcję audytu, oraz ułatwić analizę i raportowanie. Organizacje mogą ustalić progi czasowe, w których działania związane z rejestrowaniem są zmieniane (np. w czasie zbliżonym do rzeczywistego, w ciągu kilku minut lub godzin).

Zabezpieczenia powiązane: AC-3.

(4) TWORZENIE ZAPISÓW AUDYTU | AUDYT PARAMETRÓW ZAPYTAŃ O DANE OSOBOWE

Zapewnienie i wdrożenie możliwości audytowania parametrów zapytań użytkowników o zbiory danych zawierające dane osobowe.

Omówienie: Parametry zapytań to wyraźne kryteria, które pojedynczy lub zautomatyzowany system przesyła do systemu w celu pobrania danych. Zabezpieczenie parametrów zapytań do zbiorów danych, które zawierają dane osobowe, zwiększa zdolność organizacji do śledzenia i zrozumienia dostępu, wykorzystania lub udostępniania danych osobowych przez upoważniony personel.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

AU-13 MONITOROWANIE UJAWNIANIA INFORMACJI

Zabezpieczenie podstawowe:

a. Monitorowanie [*Realizacja: zdefiniowanych przez organizację informacji o otwartym kodzie źródłowym i/lub witryn informatycznych*] *z* częstotliwością [*Realizacja: zdefiniowana przez organizację częstotliwość*] pod kątem dowodów nieautoryzowanego ujawnienia informacji organizacyjnych; oraz

b. W przypadku ujawnienia informacji:

   1. Powiadomienie [*Realizacja: personel lub role określone przez organizację*]*;*

   2. Podejmowanie następujących dodatkowych działań: [*Realizacja: dodatkowe działania zdefiniowane przez organizację*].

Omówienie: Nieautoryzowane ujawnienie informacji jest formą wycieku danych. Informacje typu open-source (otwarty kod źródłowy) obejmują portale społecznościowe oraz platformy współdzielenia kodu i repozytoria. Przykłady informacji organizacyjnych obejmują informacje umożliwiające identyfikację danych osobowych lub informacje wrażliwe wygenerowane przez organizację.

Zabezpieczenia powiązane: AC-22, PE-3, PM-12, RA-5, SC-7, SI-20.

Zabezpieczenia rozszerzone:

(1) MONITOROWANIE UJAWNIANIA INFORMACJI | WYKORZYSTYWANIE ZAUTOMATYZOWANYCH NARZĘDZI

Monitorowanie informacji i witryn informatycznych o otwartym kodzie źródłowym za pomocą [***Realizacja: organizacyjnie zdefiniowane mechanizmy automatyczne***]**.**

Omówienie: Zautomatyzowane mechanizmy obejmują usługi komercyjne, które dostarczają organizacjom powiadomienia i alerty oraz zautomatyzowane skrypty do monitorowania nowych wpisów na stronach internetowych.

Zabezpieczenia powiązane: Brak.

(2) MONITOROWANIE UJAWNIANIA INFORMACJI | PRZEGLĄD MONITOROWANYCH STRON

Przegląd listy monitorowanych stron internetowych z otwartym kodem źródłowym z częstotliwością [***Realizacja: częstotliwość określona przez organizację***]**.**

Omówienie: Regularny przegląd aktualnej listy stron internetowych z otwartym kodem źródłowym, które są regularnie monitorowane, pomaga zapewnić, że wybrane strony pozostają aktualne. Przegląd daje również możliwość dodania nowych stron z informacjami o otwartym kodzie źródłowym, które mogą dostarczyć dowodów na nieautoryzowane ujawnienie informacji organizacyjnych. Lista monitorowanych miejsc może być prowadzona i wspierana przez informacje o zagrożeniach pochodzące z innych wiarygodnych źródeł informacji.

Zabezpieczenia powiązane: Brak.

(3) MONITOROWANIE UJAWNIANIA INFORMACJI | NIEAUTORYZOWANE POWIELANIE INFORMACJI

Stosowanie technik wykrywania, procesów i narzędzi do w celu ustalenia, czy podmioty zewnętrzne powielają informacje organizacyjne w sposób nieautoryzowany.

Omówienie: Nieautoryzowane wykorzystanie lub powielanie informacji organizacyjnych przez podmioty zewnętrzne może mieć negatywny wpływ na działalność i aktywa organizacji, w tym na reputację. Takie działanie może obejmować replikację strony internetowej organizacji przez przeciwnika lub wrogiego aktora zagrażającego, który próbuje podszyć się pod organizację hostingową. Do narzędzi, technik i procesów służących do wykrywania, czy podmioty zewnętrzne odtwarzają informacje organizacyjne w sposób nieuprawniony, należą: skanowanie zewnętrznych stron internetowych, monitorowanie mediów społecznościowych oraz szkolenie pracowników

w zakresie rozpoznawania nieuprawnionego wykorzystania informacji organizacyjnych.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

AU-14 AUDYT SESJI

Zabezpieczenie podstawowe:

a. Zapewnienie i wdrożenie możliwości [*Realizacja: zdefiniowani przez organizację użytkownicy lub role*] do [*Wybór (jeden lub więcej): nagrywanie; przeglądanie; słuchanie; dziennik*] zawartości sesji użytkownika w ramach [*Realizacja: okoliczności zdefiniowane przez organizację*]; oraz

b. Opracowywanie, integrowanie i wykorzystywanie audytów sesji w porozumieniu z działem prawnym oraz zgodnie z obowiązującymi przepisami prawa, rozporządzeniami, dyrektywami, polityką, standardami i wytycznymi.

Omówienie: Audyty sesji mogą obejmować monitorowanie naciśnięć klawiszy, śledzenie odwiedzanych stron internetowych oraz rejestrowanie informacji i/lub transferów plików. Funkcja audytu sesji jest wdrażana oprócz rejestrowania zdarzeń i może obejmować wdrożenie specjalistycznej technologii rejestrowania sesji. Organizacje powinny rozważyć, w jaki sposób audyt sesji może ujawnić informacje o osobach, które mogą stwarzać zagrożenie dla prywatności, a także, w jaki sposób ograniczyć to ryzyko. Ponieważ audyt sesji może mieć wpływ na wydajność systemu i sieci, organizacje aktywują zdolność w ściśle określonych sytuacjach (np. organizacja jest podejrzliwa wobec konkretnej osoby). Organizacje konsultują się z działem prawnym, osobą odpowiedzialną za ochronę danych osobowych i bezpieczeństwo informacji w celu zapewnienia, że wszelkie kwestie prawne, dotyczące prywatności, praw obywatelskich lub swobód obywatelskich, w tym wykorzystanie informacji umożliwiających identyfikację osoby, są odpowiednio uwzględnione.

Zabezpieczenia powiązane: AC-3, AC-8, AU-2, AU-3, AU-4, AU-5, AU-8, AU-9, AU-11, AU-12.

Zabezpieczenia rozszerzone:

(1) AUDYT SESJI | URURUCHAMIANIE SYSTEMU

Automatyczne inicjowanie audytów sesji przy uruchamianiu systemu.

Omówienie: Automatyczne inicjowanie audytów sesji podczas uruchamiania systemu pomaga zapewnić, że informacje pozyskiwane na temat wybranych osób są kompletne i nie są narażone na ujawnienie poprzez manipulację przez podmioty dokonujące złośliwych zagrożeń.

Zabezpieczenia powiązane: Brak.

(2) AUDYT SESJI | PRZECHWYTY / NAGRYWANIE I ZAWARTOŚĆ DZIENNIKÓW LOGOWANIA

[Wycofane: Włączone do AU-14].

(3) AUDYT SESJI | ZDALNE WYŚWIETLANIE / ODSŁUCHIWANIE

Zapewnienie i wdrożenie możliwości zdalnego przeglądania i odsłuchiwania w czasie rzeczywistym przez uprawnionych użytkowników treści związanych z ustaloną sesją użytkownika.

Omówienie: Brak.

Zabezpieczenia powiązane: AC-17.

Referencje: Brak.

AU-15 ZDOLNOŚĆ DO ALTERNATYWNEGO AUDYTU

[Wycofane: Włączone do AU-5(5)]

AU-16 AUDYT MIĘDZYORGANIZACYJNY

Zabezpieczenie podstawowe: Stosowanie [*Realizacja: metody zdefiniowane przez organizację*] do koordynacji [*Realizacja: informacje o audycie zdefiniowane przez organizację*] pomiędzy zewnętrznymi organizacjami, w przypadku przekazywania informacje o audycie poza granice organizacji.

Omówienie: W przypadku, gdy organizacje korzystają z systemów lub usług organizacji zewnętrznych, zdolność do prowadzenia rejestrów audytowych wymaga skoordynowanego, międzyorganizacyjnego podejścia. Na przykład, utrzymanie tożsamości osób, które zwracają się o określone usługi poza granicami organizacyjnymi, może być często trudne i może się okazać, że ma to istotne konsekwencje dla wydajności i prywatności. Dlatego też często zdarza się, że międzyorganizacyjne rejestry audytowe po prostu przechwytują tożsamość osób, które składają wnioski w systemie macierzystym, a kolejne systemy rejestrują, że wnioski pochodziły od upoważnionych osób. Organizacje rozważają włączenie procesów koordynacji wymagań dotyczących informacji o audycie i ochrony informacji o audycie do umów o wymianie informacji.

Zabezpieczenia powiązane: AU-3, AU-6, AU-7, CA-3, PT-7.

Zabezpieczenia rozszerzone:

(1) AUDYT MIĘDZYORGANIZACYJNY | OCHONA TOŻSAMOŚCI

Zachowanie tożsamości osób w ścieżkach audytu między organizacjami.

Omówienie: Zachowanie tożsamości jest stosowane, gdy istnieje potrzeba śledzenia działań konkretnej osoby, które są wykonywane poza granicami organizacyjnymi.

Zabezpieczenia powiązane: IA-2, IA-4, IA-5, IA-8.

(2) AUDYT MIĘDZYORGANIZACYJNY | UDOSTĘPNIANIE INFORMACJI AUDYTOWYCH

Dostarczenie informacji o audycie międzyorganizacyjnym do [***Realizacja: organizacyjnie zdefiniowane organizacje udostępniające informacje***

audytowe] ***w*** **oparciu o** [***Realizacja: umowy międzyorganizacyjne dotyczące udostępniania informacji audytowych***]**.**

Omówienie: Ze względu na rozproszony charakter informacji o audycie, wymiana informacji o audycie pomiędzy organizacjami może być istotna dla skutecznej analizy przeprowadzanego audytu. Na przykład, dokumentacja audytowa jednej organizacji może nie dostarczać wystarczających informacji do określenia właściwego lub niewłaściwego wykorzystania zasobów informacji organizacyjnej przez osoby w innych organizacjach. W niektórych przypadkach tylko macierzyste organizacje użytkowników posiadają odpowiednią wiedzę do dokonania takich ustaleń, wymagając tym samym dzielenia się informacjami z audytu między organizacjami.

Zabezpieczenia powiązane: IR-4, SI-4.

(3) AUDYT MIĘDZYORGANIZACYJNY | ODDZIELANIE DANYCH OSOBOWYCH

Wdrożenie [***Realizacja: środki określone przez organizację***] ***w*** **celu oddzielenia osób od informacji audytowych przekazywanych poza granice organizacji.**

Omówienie: Zachowanie tożsamości w ścieżkach audytu może mieć konsekwencje dla prywatności, takie jak umożliwienie śledzenia i profilowania osób, ale może nie być konieczne z operacyjnego punktu widzenia. Wdrożenie technik kryptograficznych zwiększających ochronę prywatności może oddzielić osoby fizyczne od informacji o audycie i zmniejszyć ryzyko związane z ochroną prywatności przy jednoczesnym zachowaniu rozliczalności.

Zabezpieczenia powiązane: Brak.

KATEGORIA CA - OCENA, AUTORYZACJA I MONITOROWANIE

CA-1 POLITYKA I PROCEDURY

Zabezpieczenie podstawowe:

a. Opracowywanie, dokumentowanie i rozpowszechnianie wśród [*Realizacja: personel lub role określone przez organizację*]*:*

   1. [*Wybór (jeden lub więcej): poziom organizacji; poziom misji/procesu biznesowego; poziom systemu*] polityki oceny, autoryzacji i monitorowania, która:

      (a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami; oraz

      (b) Jest zgodna z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi; oraz

   2. Procedur ułatwiających realizację polityki oceny, autoryzacji i monitorowania oraz powiązanych ocen, autoryzacji i monitorowania zabezpieczeń;

b. Wyznaczanie [*Realizacja: osoba wyznaczona przez organizację*] do zarządzania rozwojem, dokumentacją i rozpowszechnianiem polityki i procedur oceny, autoryzacji i monitorowania; oraz

c. Przeglądanie i aktualizacja bieżącej:

   1. Polityki oceny, autoryzacji i monitorowania z [Realizacja: *częstotliwość określona przez organizację*] i następujących [*Realizacja: zdarzenia określone przez organizację*]; oraz

   2. Procedur dotyczących oceny, autoryzacji i monitorowania z [Realizacja: *częstotliwość określona przez organizację*] i następujących [*Realizacja: zdarzenia określone przez organizację*].

Omówienie: Polityka i procedury w zakresie oceny, autoryzacji i monitorowania dotyczą zabezpieczeń w kategorii *Ocena, autoryzacja i monitorowanie* (CA), które są wdrażane w ramach systemów i organizacji. Strategia zarządzania ryzykiem jest ważnym czynnikiem przy tworzeniu takich polityk i procedur. Polityki i procedury przyczyniają się do zapewnienia bezpieczeństwa i ochrony prywatności. Dlatego ważne jest, aby programy bezpieczeństwa i ochrony prywatności były opracowywane wspólnie przy kształtowaniu polityki i procedur oceny, autoryzacji i monitorowania. Polityki i procedury dotyczące programów bezpieczeństwa i ochrony prywatności na poziomie organizacji są ogólnie rzecz biorąc preferowane i mogą eliminować potrzeby tworzenia polityk i procedur specyficznych dla danej misji lub systemu. Polityka może być włączona, jako część ogólnej polityki bezpieczeństwa i ochrony prywatności lub reprezentowana przez wiele polityk odzwierciedlających złożony charakter organizacji. Procedury mogą być ustanowione dla programów bezpieczeństwa i ochrony prywatności, dla misji lub procesów biznesowych oraz dla systemów, jeśli to konieczne. Procedury opisują sposób wdrażania zasad lub zabezpieczeń i mogą być skierowane do osoby lub roli, która jest przedmiotem procedury. Procedury mogą być udokumentowane w planach bezpieczeństwa i ochrony prywatności systemu w jednym lub kilku oddzielnych dokumentach.

Zdarzenia, które mogą spowodować konieczność aktualizacji polityki i procedur oceny, autoryzacji i monitorowania, obejmują wyniki oceny lub audytu, incydenty lub naruszenia bezpieczeństwa, lub zmiany w przepisach prawa, zarządzeniach, dyrektywach, rozporządzeniach, zasadach, standardach i wytycznych.

Oświadczenie o wprowadzeniu zabezpieczeń nie jest równoznaczne z ustanowieniem polityki lub procedury organizacyjnej.

Zabezpieczenia powiązane: PM-9, PS-8, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [NSC 800-12], [NIST SP 800-30], [NIST SP 800-37], [NIST SP 800-39], [NIST SP 800-53A], [NIST SP 800-100], [NIST SP 800-137], [NIST SP 800-137A], [IR 8062].

CA-2 OCENA ZABEZPIECZEŃ

Zabezpieczenie podstawowe:

a. Wybór odpowiedniego asesora lub zespołu oceniającego przeprowadzającego dany typ oceny, która ma być przeprowadzona;

b. Opracowanie planu oceny zabezpieczeń, który opisuje zakres oceny, w tym:

   1. Zabezpieczenia podstawowe i zabezpieczenia rozszerzone poddawane ocenie;

   2. Procedury oceny stosowane w celu określenia skuteczności zabezpieczeń; oraz

   3. Środowisko oceny, zespół oceniający oraz role i obowiązki związane z oceną;

c. Upewnienie się, że plan oceny zabezpieczeń został przejrzany i zatwierdzony przez osobę autoryzującą lub wyznaczonego pełnomocnika przed przeprowadzeniem oceny;

d. Ocena zabezpieczeń w systemie i jego środowisku działania [*Realizacja: częstotliwość określona przez organizację*] *w* celu określenia zakresu, w jakim zabezpieczenia są realizowane prawidłowo, działają zgodnie z założeniami i dają pożądany rezultat w odniesieniu do spełnienia ustalonych wymogów bezpieczeństwa i ochrony prywatności;

e. Sporządzanie sprawozdań z oceny zabezpieczeń, które dokumentują wyniki oceny; oraz

f. Przekazanie wyników oceny zabezpieczeń do [*Realizacja: osoby lub role określone przez organizację*].

Omówienie: Organizacje dbają o to, aby osoby oceniające zabezpieczenia posiadały wymagane umiejętności i wiedzę techniczną do opracowywania skutecznych planów

oceny oraz do przeprowadzenia oceny zarządzania zabezpieczeniami specyficznymi dla danego systemu, hybrydowego, wspólnego i programowego, w zależności od potrzeb. Wymagane umiejętności obejmują ogólną znajomość koncepcji i podejść w zakresie zarządzania ryzykiem, a także wszechstronną wiedzę i doświadczenie w zakresie wdrażanych komponentów sprzętu, oprogramowania aplikacyjnego i oprogramowania układowego.

Organizacje oceniają zabezpieczenia w systemach i środowiskach, w których systemy te działają w ramach wstępnych i bieżących autoryzacji, ciągłego monitorowania, corocznych ocen, projektowania i rozwoju systemu, inżynierii bezpieczeństwa systemów, inżynierii prywatności oraz cyklu życia systemu. Oceny pomagają zapewnić, że organizacje spełniają wymagania w zakresie bezpieczeństwa informacji i ochrony prywatności, identyfikują słabe punkty i niedociągnięcia w procesie projektowania i rozwoju systemu, dostarczają istotnych informacji potrzebnych do podejmowania decyzji opartych na ryzyku w ramach procesów autoryzacji oraz przestrzegają procedur ograniczania podatności na zagrożenia. Organizacje przeprowadzają oceny wdrożonych zabezpieczeń, udokumentowanych w planach bezpieczeństwa i ochrony prywatności. Oceny mogą być również przeprowadzane w całym cyklu życia systemu w ramach procesów inżynierii systemów i inżynierii bezpieczeństwa systemów. Projekt zabezpieczeń może być oceniany w miarę opracowywania planów zapytań ofertowych (*ang. Request For Proposal – RFP*), oceny reakcji i przeprowadzania przeglądów projektu. Jeżeli projekt wdrożenia zabezpieczeń i późniejsze wdrożenie zgodne z projektem są oceniane podczas opracowywania, końcowe testy zabezpieczeń mogą być zwykłym poświadczeniem, wykorzystującym wcześniej zakończoną ocenę zabezpieczeń i agregującym wyniki.

Organizacje mogą opracować jednolity, skonsolidowany plan oceny bezpieczeństwa i ochrony prywatności dla systemu lub utrzymywać oddzielne plany. Skonsolidowany plan oceny jasno określa role i obowiązki w zakresie oceny zabezpieczeń. Jeżeli w ocenie systemu bierze udział wiele organizacji, skoordynowane podejście może zmniejszyć ilość redundancji i związanych z nią kosztów.

Organizacje mogą korzystać z innych rodzajów działań oceniających, takich jak skanowanie podatności na zagrożenia i monitorowanie systemu, w celu zachowania bezpieczeństwa i ochrony prywatności systemów w trakcie cyklu życia systemu. Sprawozdania z oceny dokumentują wyniki oceny w sposób wystarczająco szczegółowy, jeśli organizacje uznają to za konieczne, w celu określenia dokładności i kompletności sprawozdań oraz tego, czy zabezpieczenia są realizowane prawidłowo, działają zgodnie z założeniami i dają pożądany rezultat w odniesieniu do spełnienia wymagań. Wyniki oceny są dostarczane osobom lub rolom właściwym dla rodzajów przeprowadzanych ocen. Na przykład, oceny przeprowadzone na poparcie decyzji autoryzacyjnych są dostarczane osobom autoryzującym oraz ich pełnomocnikom, personelowi ds. ochrony prywatności i ds. bezpieczeństwa informacji.

Aby spełnić wymagania oceny rocznej, organizacje mogą wykorzystać wyniki oceny z następujących źródeł: wstępna lub bieżąca autoryzacja systemu, ciągłe monitorowanie, procesy inżynierii systemowej lub działania w ramach cyklu życia systemu. Organizacje zapewniają, że wyniki oceny są aktualne, istotne dla określenia skuteczności zabezpieczeń i uzyskiwane przy zachowaniu odpowiedniego poziomu niezależności asesora. Istniejące wyniki oceny zabezpieczeń mogą być ponownie wykorzystane w zakresie, w jakim wyniki te są nadal aktualne, a w razie potrzeby mogą być uzupełnione o dodatkowe oceny. Po uzyskaniu wstępnych autoryzacji, organizacje oceniają zabezpieczenia podczas ciągłego monitorowania. Organizacje ustalają również częstotliwość ocen bieżących zgodnie ze strategiami ciągłego monitorowania organizacji. Audyt zewnętrzny, w tym audyt przeprowadzany przez podmioty zewnętrzne, takie jak podmioty regulacyjne, nie wchodzą w zakres kompetencji CA-2.

Zabezpieczenia powiązane: AC-20, CA-5, CA-6, CA-7, PM-9, RA-5, RA-10, SA-11, SC-38, SI-3, SI-12, SR-2, SR-3.

Zabezpieczenia rozszerzone:

(1) OCENA ZABEZPIECZEŃ | NIEZALEŻNI AUDYTORZY

Zatrudnienie niezależnej osoby oceniającej lub zespołu oceniającego do przeprowadzania oceny zabezpieczeń.

Omówienie: Niezależni oceniający lub zespoły oceniające to osoby lub grupy, które przeprowadzają bezstronne oceny systemów. Bezstronność oznacza, że osoby oceniające są wolne od wszelkich postrzeganych lub faktycznych konfliktów interesów dotyczących rozwoju, funkcjonowania, utrzymania lub zarządzania ocenianymi systemami lub określania skuteczności zabezpieczeń. W celu osiągnięcia bezstronności, osoby oceniające nie tworzą wzajemnych lub sprzecznych interesów z organizacjami, w których przeprowadzane są oceny, nie oceniają własnej pracy, nie działają, jako kierownictwo lub pracownicy organizacji, którym służą, ani nie są wyznaczani na stanowiska rzeczników organizacji nabywających ich usługi.

Niezależne oceny można uzyskać z elementów wewnątrz organizacji lub zleconych podmiotom sektora publicznego lub prywatnego spoza organizacji. Osoby autoryzujące określają wymagany poziom niezależności w oparciu o kategorie bezpieczeństwa systemów i/lub ryzyko dla operacji organizacyjnych, aktywów organizacyjnych lub osób. Osoby autoryzujące określają również, czy poziom niezależności osoby oceniającej daje wystarczającą pewność, że wyniki są rzetelne i mogą być wykorzystane do podejmowania wiarygodnych, opartych na ryzyku decyzji. Określenie niezależności oceniającej (asesora) obejmuje sprawdzenie, czy zakontraktowane usługi oceny mają wystarczającą niezależność, np. czy właściciele systemów nie są bezpośrednio zaangażowani w procesy zawierania umów lub nie mogą wpływać na bezstronność asesorów przeprowadzających oceny. W fazie projektowania i rozwoju systemu, posiadanie niezależnych asesorów jest analogiczne do angażowania niezależnych ekspertów merytorycznych (*ang. Subject Matter Expert – SME*) w przeglądy projektów.

W przypadku, gdy organizacje będące właścicielami systemów są małe lub ich struktury wymagają, aby oceny były przeprowadzane przez osoby znajdujące się w łańcuchu rozwojowym, operacyjnym lub zarządczym właścicieli systemów, niezależność w procesach oceny może być osiągnięta poprzez zapewnienie, że wyniki oceny są dokładnie przeglądane i analizowane przez niezależne zespoły ekspertów w celu potwierdzenia kompletności, dokładności, integralności i wiarygodności wyników. Oceny przeprowadzane w celach innych niż wspomaganie decyzji autoryzacyjnych są bardziej prawdopodobne do wykorzystania przy takich decyzjach, gdy są wykonywane przez osoby oceniające o wystarczającej niezależności, co zmniejsza potrzebę powtarzania ocen.
Zabezpieczenia powiązane: Brak.

(2) OCENA ZABEZPIECZEŃ | OCENY SPECJALISTYCZNE

Uwzględnianie, jako części oceny zabezpieczeń [Realizacja: *częstotliwość określona przez organizację*], [*Wybór: zapowiedziany; niezapowiedziany*], [*Wybór (jeden lub więcej): szczegółowe monitorowanie; narzędzia bezpieczeństwa; zautomatyzowane testy bezpieczeństwa; skanowanie podatności; testowanie złośliwych użytkowników; ocena zagrożeń wewnętrznych; test wydajności i obciążenia; ocena wycieku lub utraty danych;* [*Realizacja: inne formy oceny określone przez organizację*]].

Omówienie: Organizacje mogą przeprowadzać specjalistyczne oceny, w tym weryfikację i uwierzytelnianie, monitorowanie systemu, ocenę zagrożeń wewnętrznych, testowanie złośliwych użytkowników i inne formy testowania. Oceny te mogą poprawić gotowość poprzez wykorzystanie zdolności organizacyjnych i wskazanie aktualnego poziomu wydajności, jako sposobu na skoncentrowanie działań na poprawie bezpieczeństwa i ochrony prywatności. Organizacje przeprowadzają specjalistyczne oceny zgodnie z obowiązującymi przepisami prawa, rozporządzeniami, dyrektywami, regulacjami, politykami, standardami i wytycznymi. Osoby autoryzujące zatwierdzają metody oceny

w koordynacji z funkcją wykonawczą ds. ryzyka organizacyjnego (*ang. Risk executive function)*[41]. Organizacje mogą włączać podatności, które zostały wykryte podczas oceny, do procesów usuwania słabych punktów. Oceny specjalistyczne mogą być również przeprowadzane na początku cyklu życia systemu (np. podczas wstępnego projektowania, rozwoju i testów jednostkowych).

Zabezpieczenia powiązane: PE-3, SI-2.

(3) OCENA ZABEZPIECZEŃ | KORZYSTANIE Z WYNIKÓW UZYSKANYCH OD ORGANIZACJI ZEWNĘTRZNYCH

Akceptacja wyników oceny zabezpieczeń przeprowadzonych przez [Realizacja: *zdefiniowane przez organizację zewnętrzne organizacje*] na [*Realizacja: system zdefiniowany przez organizację*], gdy ocena spełnia [*Realizacja: wymagania zdefiniowane przez organizację*].

Omówienie: Organizacje mogą polegać na ocenach zabezpieczeń systemów organizacyjnych przeprowadzanych przez inne (zewnętrzne) organizacje. Wykorzystanie takich ocen i ponowne wykorzystanie istniejących dowodów oceny może skrócić czas i zmniejszyć zasoby wymagane do przeprowadzenia oceny poprzez ograniczenie niezależnych działań związanych z oceną, które organizacje muszą wykonać. Czynniki, które organizacje biorą pod uwagę przy ustalaniu, czy przyjąć wyniki oceny od organizacji zewnętrznych, mogą się różnić. Czynniki te obejmują wcześniejsze doświadczenia organizacji, która przeprowadziła ocenę, reputację organizacji oceniającej, poziom szczegółowości dostarczanych dowodów oceny oraz nakazy nałożone przez obowiązujące prawo, rozporządzenia, dyrektywy, regulacje, polityki, standardy i wytyczne. Akredytowane laboratoria badawcze, które obsługują Program wspólnych

[41] Osoba (lub grupa osób, kierowana przez wyższego rangą urzędnika w jednostce organizacyjnej) odpowiedzialna za zarządzanie ryzykiem.

kryteriów (*ang. Common Criteria Program*) [ISO 15408-1], Program walidacji modułów kryptograficznych NIST (CMVP) lub Program walidacji algorytmów kryptograficznych NIST (CAVP), mogą dostarczać niezależnych wyników oceny, które organizacje mogą wykorzystać.

Zabezpieczenia powiązane: SA-4.

Referencje: [OMB A-130], [FIPS 199], [NSC 800-18], [NIST SP 800-37], [NIST SP 800-39], [NIST SP 800-53A], [NIST SP 800-115], [NIST SP 800-137], [IR 8011-1], [IR 8062].

CA-3 WYMIANA INFORMACJI

Zabezpieczenie podstawowe:

a. Zatwierdzanie i zarządzanie wymianą informacji pomiędzy systemami przy użyciu [*Wybór (jeden lub więcej): umowy o bezpieczeństwie połączeń wzajemnych; umowy o bezpieczeństwie wymiany informacji; protokoły ustaleń lub umowy; umowy o poziomie usług; umowy z użytkownikami; umowy o zachowaniu poufności;* [*Realizacja: określony przez organizację rodzaj umowy*]];

b. Dokumentowanie, jako część każdej umowy o wymianie, charakterystyki interfejsu, wymogów w zakresie bezpieczeństwa i ochrony prywatności, zabezpieczeń i odpowiedzialności za każdy system i poziomu wpływu przekazywanych informacji; oraz

c. Przegląd i aktualizacja umów [*Realizacja: częstotliwość określona przez organizację*].

Omówienie: Wymogi dotyczące wymiany informacji systemowych mają zastosowanie do wymiany informacji pomiędzy dwoma lub więcej systemami. Wymiana informacji międzysystemowych obejmuje połączenia za pośrednictwem łączy dzierżawionych lub wirtualnych sieci prywatnych, połączenia z dostawcami usług internetowych, współdzielenie baz danych lub wymianę informacji transakcyjnych z bazami danych, połączenia i wymianę z usługami w chmurze, wymianę za pośrednictwem usług internetowych lub wymianę plików za pośrednictwem protokołów przesyłania plików, protokołów sieciowych (np. IPv4, IPv6), poczty elektronicznej lub innej komunikacji między organizacjami. Organizacje rozważają ryzyko związane z nowymi lub zwiększonymi zagrożeniami, które mogą zostać wprowadzone podczas wymiany informacji między systemami mogącymi posiadać różne wymagania i zabezpieczenia w zakresie bezpieczeństwa i ochrony prywatności. Dotyczy to zarówno systemów działających w ramach tej samej organizacji, jak i systemów zewnętrznych wobec organizacji. Autoryzacja wspólna systemów wymieniających informacje, opisana

w zabezpieczeniach CA-6(1) lub CA-6(2), może pomóc w komunikacji i zmniejszeniu ryzyka.

Osoby autoryzujące określają ryzyko związane z wymianą informacji międzysystemowych oraz zabezpieczenia niezbędne do odpowiedniego ograniczenia ryzyka. Wybrane rodzaje umów opierają się na takich czynnikach, jak poziom wpływu wymienianych informacji, relacje pomiędzy organizacjami wymieniającymi informacje (np. rząd z rządem, rząd z biznesem, biznes z dostawcą usług, rząd lub biznes z usługodawcą, rząd lub biznes z osobą fizyczną) lub poziom dostępu do systemu organizacyjnego przez użytkowników drugiego systemu. Jeżeli systemy, które wymieniają informacje, mają tą samą osobę autoryzującą, organizacje nie muszą zawierać umów. Zamiast tego, charakterystyka interfejsu między systemami (np. sposób wymiany informacji, sposób ochrony informacji) jest opisana w odpowiednich planach bezpieczeństwa i ochrony prywatności. Jeśli systemy, które wymieniają informacje, mają różne osoby autoryzujące w ramach tej samej organizacji, organizacje mogą opracować umowy lub dostarczyć te same informacje, które byłyby zawarte w odpowiednim rodzaju umowy przykładowo podanym w zabezpieczeniu CA-3a w stosownych planach bezpieczeństwa i ochrony prywatności systemów. Organizacje mogą włączać informacje o porozumieniach do formalnych umów, w szczególności dotyczących wymiany informacji ustanowionych między organizacjami państwowymi, a organizacjami komercyjnymi (w tym dostawcami usług, wykonawcami, twórcami systemów i integratorami systemów). Rozważania dotyczące ryzyka obejmują systemy, które korzystają z tych samych sieci.

Zabezpieczenia powiązane: AC-4, AC-20, AU-16, CA-6, IA-3, IR-4, PL-2, PT-7, RA-3, SA-9, SC-7, SI-12.

Zabezpieczenia rozszerzone:

(1) WYMIANA INFORMACJI | POŁĄCZENIA JAWNYCH BEZPIECZNYCH SYSTEMÓW KRAJOWYCH

[Wycofane: Włączone do SC-7(25)].

(2) WYMIANA INFORMACJI | POŁĄCZENIA NIEJAWNYCH SYSTEMÓW KRAJOWYCH

[Wycofane: Włączone do SC-7(26)].

(3) WYMIANA INFORMACJI | POŁĄCZENIA JAWNYCH BEZPIECZNYCH SYSTEMÓW TRANSGRANICZNYCH

[Wycofane: Włączone do SC-7(27)].

(4) WYMIANA INFORMACJI | POŁĄCZENIA Z SIECIAMI PUBLICZNYMI

[Wycofane: Włączone do SC-7(28)]

(5) WYMIANA INFORMACJI | OGRANICZENIA DOTYCZĄCE POŁĄCZEŃ SYSTEMÓW ZEWNĘTRZNYCH

[Wycofane: Włączone do SC-7(5)]

(6) WYMIANA INFORMACJI | AUTORYZACJE PRZESYŁU

Należy sprawdzić, przed zaakceptowaniem wymiany danych, czy osoby lub systemy przekazujące dane pomiędzy łączącymi się systemami posiadają wymagane autoryzacje (tj. pozwolenie na piśmie lub uprawnienia).

Omówienie: W celu zapobiegania przekazywaniu informacji do chronionych systemów przez nieupoważnione osoby i systemy, chroniony system weryfikuje - za pomocą niezależnych środków - czy osoba lub system próbujący przekazać informacje jest do tego autoryzowany. Weryfikacja autoryzacji do przekazywania

informacji dotyczy również zabezpieczeń kierowania ruchem (np. routingu i DNS) oraz usług (np. uwierzytelnionych przekaźników SMTP).

Zabezpieczenia powiązane: AC-2, AC-3, AC-4.

(7) WYMIANA INFORMACJI | POBIERANIE INFORMACJI

(a) Określenie wymiany informacji „pobieranych" (*downstream*) z innymi systemami za pośrednictwem systemów określonych w CA-3a; oraz

(b) Podjęcie środków w celu zapewnienia, że wymiana informacji „pobieranych" (*downstream*) zostanie przerwana w przypadku, gdy zabezpieczenia zidentyfikowanych systemów „pobierających" dane (typu *downstream*) nie mogą zostać zweryfikowane lub zatwierdzone.

Omówienie: Pobieranie lub "downstream" informacji to wymiana informacji pomiędzy systemem lub systemami, z którymi system organizacyjny wymienia informacje, a innymi systemami. W przypadku systemów, usług i aplikacji istotnych z punktu widzenia misji, w tym aktywów o dużej wartości, konieczne jest określenie takiej wymiany informacji. Transparentność środków bezpieczeństwa lub ochrony stosowanych w systemach typu „downstream", podłączonych bezpośrednio lub pośrednio do systemów organizacyjnych, jest niezbędna do zrozumienia zagrożeń dla bezpieczeństwa i ochrony prywatności wynikających z tej wymiany informacji. Systemy organizacyjne mogą odziedziczyć ryzyko po systemach typu „downstream" poprzez połączenia i wymianę informacji, co może uczynić systemy organizacyjne bardziej podatnymi na zagrożenia, niebezpieczeństwo i niekorzystne skutki.

Zabezpieczenia powiązane: SC-7.

Referencje: [OMB A-130], [FIPS 199], [NIST SP 800-47].

CA-4 CERTYFIKACJA BEZPIECZEŃSTWA

[Wycofane: Włączone do CA-2].

CA-5 PLAN I ETAPY DZIAŁANIA

Zabezpieczenie podstawowe:

a. Opracowanie planu i etapów działania systemu dokumentującego planowane działania naprawcze organizacji w celu skorygowania słabych punktów lub braków odnotowanych podczas oceny zabezpieczeń oraz w celu zmniejszenia lub wyeliminowania znanych słabych punktów w systemie; oraz

b. Aktualizacja istniejącego planu i etapów działania z częstotliwością [*Realizacja: częstotliwość określona przez organizację*] *na podstawie* ustaleń z oceny zabezpieczeń, niezależnych audytów lub przeglądów oraz działań w zakresie ciągłego monitorowania.

Omówienie: Plany i etapy działania są przydatne dla każdego rodzaju organizacji, aby śledzić planowane działania naprawcze. Plany i etapy działania są wymagane w pakietach autoryzacyjnych i podlegają wymogom sprawozdawczości ustanowionym przez przepisy prawa.

Zabezpieczenia powiązane: CA-2, CA-7, PM-4, PM-9, RA-7, SI-2, SI-12.

Zabezpieczenia rozszerzone:

(1) PLAN I ETAPY DZIAŁANIA | AUTOMATYZACJA WSPIERAJĄCA AKTUALNOŚĆ / SZCZEGÓŁOWOŚĆ PLANÓW

Zapewnienie dokładności, aktualności i dostępność planu i etapów działania systemu za pomocą [***Realizacja: automatyczne mechanizmy zdefiniowane przez organizację***]**.**

Omówienie: Korzystanie ze zautomatyzowanych narzędzi pomaga utrzymać dokładność, aktualność i dostępność planu i etapów działania oraz ułatwia koordynację i wymianę informacji dotyczących bezpieczeństwa i ochrony prywatności w całej organizacji. Taka koordynacja i dzielenie się informacjami pomaga zidentyfikować systemowe słabości lub braki w systemach

organizacyjnych i zapewnić, że odpowiednie zasoby są kierowane na najbardziej krytyczne słabości systemu w odpowiednim czasie.

Zabezpieczenia powiązane: Brak.

Referencje: [OMB A-130], [NSC 800-37].

CA-6 AUTORYZACJA

Zabezpieczenie podstawowe:

a. Przydzielenie osoby z jednostki organizacyjnej, jako osoby autoryzującej system;

b. Wyznaczenie osoby z jednostki organizacyjnej, jako osoby autoryzującej zabezpieczenia wspólne dostępne do dziedziczenia przez systemy organizacyjne;

c. Upewnienie się, że osoba autoryzująca system, przed rozpoczęciem operacji:

   1. Akceptuje użycie zabezpieczeń wspólnych odziedziczonych przez system; oraz

   2. Upoważnia system do działania;

d. Upewnienie się, że osoba autoryzująca zabezpieczenia wspólne zezwala na użytkowanie zabezpieczeń do dziedziczenia przez systemy organizacyjne;

e. Aktualizacje autoryzacji z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Omówienie: Upoważnienia są oficjalnymi decyzjami kierownictwa wyższego szczebla, które zezwalają na działanie systemów, upoważniają do korzystania ze wspólnych zabezpieczeń dziedziczenia przez systemy organizacyjne i wyraźnie akceptują ryzyko dla operacji organizacyjnych i majątku, osób, innych organizacji i Narodu w oparciu o realizację uzgodnionych zabezpieczeń. Osoby autoryzujące zapewniają nadzór budżetowy nad systemami organizacyjnymi i wspólnymi zabezpieczeniami lub przyjmują odpowiedzialność za misję i funkcje biznesowe wspierane przez te systemy lub wspólne zabezpieczenia. Proces autoryzacji należy do obowiązków federalnych, dlatego też urzędnicy autoryzujący muszą być pracownikami federalnymi. Urzędnicy autoryzujący są zarówno odpowiedzialni, jak i odpowiedzialni za zagrożenia bezpieczeństwa i ochrony prywatności związane z funkcjonowaniem i korzystaniem z systemów organizacyjnych. Organizacje niefederalne mogą mieć podobne procesy autoryzacji systemów i wyższych urzędników, którzy przyjmują na siebie rolę autoryzacji i związaną z tym odpowiedzialność.

Urzędnicy autoryzujący wydają bieżące autoryzacje systemów w oparciu o dowody uzyskane z wdrożonych programów ciągłego monitoringu. Solidne programy stałego monitorowania zmniejszają potrzebę stosowania odrębnych procesów autoryzacji. Dzięki zastosowaniu kompleksowych procesów ciągłego monitoringu, informacje zawarte w pakietach autoryzacyjnych (tj. plany bezpieczeństwa i ochrony prywatności, raporty oceniające oraz plany i etapy działania) są na bieżąco aktualizowane. Dzięki temu urzędnicy autoryzacyjni, dostawcy usług wspólnych zabezpieczeń i właściciele systemów otrzymują aktualny status bezpieczeństwa i ochrony prywatności swoich systemów, zabezpieczeń i środowisk operacyjnych. W celu zmniejszenia kosztów autoryzacji, urzędnicy autoryzujący mogą wykorzystać wyniki ciągłych procesów monitorowania w maksymalnym możliwym stopniu, jako podstawę do podejmowania decyzji o autoryzacji.

Zabezpieczenia powiązane: CA-2, CA-3, CA-7, PM-9, PM-10, RA-3, SA-10, SI-12.

Zabezpieczenia rozszerzone:

(1) AUTORYZACJA | AUTORYZACJA WSPÓLNA – WEWNĄTRZORGANIZACYJNA

Zastosowanie wspólnego procesu autoryzacji dla systemu, który obejmuje wielu autoryzujących urzędników z tej samej organizacji przeprowadzających autoryzację.

Omówienie: Wyznaczenie wielu osoby autoryzujące z tej samej organizacji do pełnienia funkcji współtworzących system zwiększa poziom niezależności w procesie podejmowania decyzji w oparciu o ryzyko. Wdraża również koncepcje rozdzielenia obowiązków i podwójnego upoważnienia, stosowane w procesie autoryzacji systemu. Wewnątrzorganizacyjny proces wspólnej autoryzacji jest najbardziej istotny dla systemów połączonych, systemów współdzielonych i systemów z wieloma właścicielami informacji.

Zabezpieczenia powiązane: AC-6.

(2) AUTORYZACJA | AUTORYZACJA WSPÓLNA – MIĘDZYORGANIZACYJNA

Zastosowanie wspólnego procesu autoryzacji dla systemu, który obejmuje wielu autoryzujących urzędników, z co najmniej jednym autoryzującym urzędnikiem z organizacji zewnętrznej w stosunku do organizacji prowadzącej autoryzację.

Omówienie: Wyznaczenie wielu osób autoryzujących, z których co najmniej jedna pochodzi z organizacji zewnętrznej, do pełnienia funkcji współupoważniających dla systemu, zwiększa poziom niezależności w procesie podejmowania decyzji w oparciu o ryzyko, wprowadza w życie koncepcje rozdziału obowiązków i podwójnej autoryzacji, stosowane w procesie autoryzacji systemu. Zatrudnienie urzędników upoważnionych przez organizacje zewnętrzne, jako uzupełnienie urzędnika upoważnionego przez organizację, która jest właścicielem lub gospodarzem systemu, może być konieczne, gdy organizacje zewnętrzne mają interes prawny lub kapitałowy w wyniku decyzji upoważniającej. Wspólny proces autoryzacji między organizacjami jest istotny i właściwy dla połączonych systemów, systemów współdzielonych lub usług oraz systemów posiadających wielu właścicieli informacji. Urzędnicy autoryzujący organizacji zewnętrznych są kluczowymi interesariuszami systemu podlegającego autoryzacji.

Zabezpieczenia powiązane: AC-6.

Referencje: [OMB A-130], [NIST SP 800-37], [NIST SP 800-137].

CA-7 CIĄGŁE MONITOROWANIE

Zabezpieczenie podstawowe: Opracowanie strategii stałego monitorowania na poziomie systemu i wdrożenie stałego monitorowania zgodnie ze strategią stałego monitorowania na poziomie organizacji, która obejmuje:

a. Ustalenie następujących metryk na poziomie systemu, które mają być monitorowane: [*Realizacja: metryka na poziomie organizacji zdefiniowana na poziomie systemowym*];

b. Ustanowienie [*Realizacja: częstotliwość określona przez organizację*] do monitorowania oraz [*Realizacja: częstotliwość określona przez organizację*] do oceny skuteczności zabezpieczeń;

c. Przeprowadzanie bieżących ocen zabezpieczeń zgodnie ze strategią ciągłego monitorowania;

d. Bieżący monitoring metryk systemowych i organizacyjnych, zgodnie ze strategią ciągłego monitorowania;

e. Korelację i analizę informacji generowanych podczas oceny zabezpieczeń i monitorowania;

f. Działania w zakresie reagowania na wyniki analizy informacji dotyczących oceny zabezpieczeń i monitorowania; oraz

g. Zgłaszanie stanu bezpieczeństwa i ochrony prywatności systemu do [*Realizacja: organizacja - określony personel lub role*] [*Realizacja: organizacja - określona częstotliwość*].

Omówienie: Ciągły monitoring na poziomie systemu ułatwia stałą świadomość bezpieczeństwa systemu i postawy prywatnej w celu wsparcia decyzji dotyczących zarządzania ryzykiem organizacyjnym. Terminy "ciągły" i "bieżący" oznaczają, że organizacje oceniają i monitorują swoje zabezpieczenia i ryzyko z częstotliwością wystarczającą do wspierania decyzji opartych na ryzyku. Różne rodzaje zabezpieczeń mogą wymagać różnych częstotliwości monitorowania. Wyniki ciągłego

monitorowania generują działania w odpowiedzi na ryzyko podejmowane przez organizacje. Podczas monitorowania skuteczności wielu zabezpieczeń, które zostały pogrupowane w możliwości, może być konieczna analiza przyczyn źródłowych w celu określenia konkretnego zabezpieczenia, które zawiodło. Programy do ciągłego monitorowania pozwalają organizacjom na utrzymanie uprawnień systemów i wspólnych zabezpieczeń w wysoce dynamicznych środowiskach działania przy zmieniających się potrzebach misyjnych i biznesowych, zagrożeniach, podatnościach i technologiach. Stały dostęp do informacji dotyczących bezpieczeństwa i ochrony prywatności poprzez raporty i pulpity menedżerskie daje pracownikom organizacji możliwość podejmowania skutecznych i terminowych decyzji dotyczących zarządzania ryzykiem, w tym bieżących decyzji autoryzacyjnych.

Automatyka obsługuje częstsze aktualizacje zapasów sprzętu, oprogramowania i firmware'u, pakietów autoryzacyjnych i innych informacji systemowych. Efektywność jest jeszcze większa, gdy wyniki ciągłego monitorowania są formatowane w celu dostarczenia informacji, które są konkretne, mierzalne, możliwe do podjęcia działań, istotne i aktualne. Działania związane z ciągłym monitorowaniem są skalowane zgodnie z kategoriami bezpieczeństwa systemów. Wymogi dotyczące monitorowania, w tym konieczność szczególnego monitorowania, mogą być przywoływane w innych zabezpieczeniach i udoskonaleniach zabezpieczeń, takich jak: AC-2g, AC-2(7), AC-2(12) lit. a), AC-2(7) lit. b), AC-2(7) lit. c), AC-17(1), AT-4a, AU-13, AU-13(1), AU-13(2), CM-3f, CM- 6d, CM-11c, IR-5, MA-2b, MA-3a, MA-4a, PE-3d, PE-6, PE-14b, PE-16, PE-20, PM-6, PM-23, PM- 31, PS-7e, SA-9c, SR-4, SC-5(3)(b), SC-7a, SC-7(24)(b), SC-18b, SC-43b i SI-4.

Zabezpieczenia powiązane: AC-2, AC-6, AC-17, AT-4, AU-6, AU-13, CA-2, CA-5, CA-6, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-16, PE-20, PL-2, PM-4, PM-6, PM-9, PM-10, PM-12, PM-14, PM-23, PM-28, PM-31, PS-7, PT-7, RA-3, RA-5, RA-7, RA-10, SA-8, SA-9, SA-11, SC-5, SC-7, SC-18, SC-38, SC-43, SI-3, SI-4, SI-12, SR-6.

Zabezpieczenia rozszerzone:

(1) CIĄGŁE MONITOROWANIE | NIEZALEŻNA OCENA

Zatrudnianie niezależnych asesorów lub zespołów oceniających w celu bieżącego monitorowania zabezpieczeń w systemie.

Omówienie: Organizacje maksymalizują wartość ocen zabezpieczeń, wymagając, aby oceny były przeprowadzane przez asesorów o odpowiednim poziomie niezależności. Poziom wymaganej samodzielności opiera się na organizacyjnej strategii ciągłego monitorowania. Niezależność asesora zapewnia pewien stopień bezstronności w procesie monitoringu. W celu osiągnięcia takiej bezstronności, asesorzy nie tworzą wzajemnych lub sprzecznych interesów z organizacjami, w których prowadzone są oceny, nie oceniają własnej pracy, nie działają, jako kierownictwo lub pracownicy organizacji, które obsługują, lub zajmują pozycje rzecznika organizacji, które nabywają ich usługi.

Zabezpieczenia powiązane: Brak.

(2) CIĄGŁE MONITOROWANIE | RODZAJE OCEN

[Wycofane: Włączone do CA-2].

(3) CIĄGŁE MONITOROWANIE | ANALIZY TRENDÓW

Analiza trendów zatrudnienia w celu określenia, czy wdrożenia zabezpieczeń, częstotliwość działań w zakresie ciągłego monitorowania oraz rodzaje działań wykorzystywanych w procesie ciągłego monitorowania wymagają modyfikacji na podstawie danych empirycznych.

Omówienie: Analizy trendów obejmują badanie ostatnich informacji o zagrożeniach, które odnoszą się do rodzajów zagrożeń występujących w organizacji lub rządzie federalnym, wskaźników powodzenia niektórych rodzajów ataków, pojawiających się słabych punktów w technologiach, ewoluujących technik inżynierii społecznej, skuteczności

ustawień konfiguracyjnych, wyników wielokrotnych ocen zabezpieczeń oraz ustaleń inspektorów generalnych lub audytorów.

Zabezpieczenia powiązane: Brak.

(4) CIĄGŁE MONITOROWANIE | MONITOROWANIE RYZYKA

Zapewnienie monitorowania ryzyka jest integralną częścią strategii stałego monitorowania, która obejmuje następujące elementy:

(a) Monitorowanie skuteczności;

(b) Monitorowanie zgodności; oraz

(c) Monitorowanie zmian.

Omówienie: Monitorowanie ryzyka odbywa się w oparciu o ustaloną organizacyjną tolerancję ryzyka. Monitorowanie efektywności determinuje bieżącą skuteczność wdrażanych środków reagowania na ryzyko. W ramach monitoringu zgodności weryfikuje się, czy wdrożone zostały wymagane środki reakcji na ryzyko. Weryfikuje również, czy spełnione są wymogi bezpieczeństwa i ochrony prywatności. Monitorowanie zmian identyfikuje zmiany w systemach organizacyjnych i środowiskach działania, które mogą mieć wpływ na ryzyko związane z bezpieczeństwem i prywatnością.

Zabezpieczenia powiązane: Brak.

(5) CIĄGŁE MONITOROWANIE | ANALIZA SPÓJNOŚCI

Podejmowanie następujących działań mających na celu potwierdzenie, że zasady są ustanowione, a wdrożone zabezpieczenia działają w spójny sposób: [***Realizacja: działania zdefiniowane przez organizację***]**.**

Omówienie: Zabezpieczenie bezpieczeństwa i ochrony prywatności jest często dodawana do systemu w sposób stopniowy. W rezultacie polityka w zakresie wyboru i wdrażania zabezpieczeń może być niespójna, a zabezpieczenia mogą nie współpracować ze sobą w spójny lub skoordynowany sposób. Brak spójności

i koordynacji może oznaczać co najmniej, że w systemie istnieją niedopuszczalne luki w zakresie bezpieczeństwa i ochrony prywatności. W najgorszym przypadku mogłoby to oznaczać, że niektóre z mechanizmów zabezpieczeń wdrożonych w jednym miejscu lub przez jeden komponent faktycznie utrudniają funkcjonowanie innych mechanizmów zabezpieczeń (np. szyfrowanie wewnętrznego ruchu sieciowego może utrudniać monitorowanie). W innych sytuacjach brak spójnego monitorowania wszystkich zaimplementowanych protokołów sieciowych (np. podwójny stos IPv4 i IPv6) może stworzyć niezamierzone luki w systemie, które mogłyby zostać wykorzystane przez przeciwników.

Ważne jest, aby walidować poprzez testy, monitorowanie i analizę, że wdrożone zabezpieczenia działają w sposób spójny, skoordynowany i niezakłócający konkurencji.

Zabezpieczenia powiązane: Brak.

(6) CIĄGŁE MONITOROWANIE | AUTOMATYZACJA WSPARCIA MONITOROWANIA

Zapewnienie dokładności, aktualności i dostępności wyników monitoringu systemu za pomocą [***Realizacja: organizacyjnie zdefiniowane automatyczne mechanizmy monitorowania***]**.**

Omówienie: Korzystanie ze zautomatyzowanych narzędzi do monitoringu pomaga utrzymać dokładność, aktualność i dostępność informacji z monitoringu, co z kolei pomaga zwiększyć poziom bieżącej świadomości bezpieczeństwa systemu i postawy prywatności w celu wsparcia decyzji dotyczących zarządzania ryzykiem organizacyjnym.

Zabezpieczenia powiązane: Brak.

Referencje: [OMB A-130], [NIST SP 800-37], [NIST SP 800-39], [NIST SP 800-53A], [NIST SP 800-115], [NIST SP 800-137], [IR 8011-1], [IR 8062].

CA-8 TESTY PENETRACYJNE

Zabezpieczenie podstawowe: Przeprowadzanie testów penetracyjnych [Realizacja: *częstotliwość zdefiniowana przez organizację*] na [*Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację*].

Omówienie: Testy penetracyjne to specjalistyczny rodzaj oceny przeprowadzanej na systemach lub poszczególnych komponentach systemu w celu identyfikacji luk, które mogą być wykorzystane przez przeciwników. Testy penetracyjne wykraczają poza zautomatyzowane skanowanie podatności i są przeprowadzane przez testerów i zespoły posiadające udokumentowane umiejętności i doświadczenie, które obejmują wiedzę techniczną w zakresie bezpieczeństwa sieci, systemu operacyjnego i/lub aplikacji. Testy penetracyjne mogą być wykorzystywane do sprawdzania podatności lub określania stopnia odporności systemów na penetrację przez przeciwników w ramach określonych założeń. Uwarunkowania takie obejmują czas, zasoby i umiejętności. Testy penetracyjne mają na celu zdublowanie działań przeciwników i zapewniają bardziej dogłębną analizę słabości lub braków związanych z bezpieczeństwem i ochroną prywatności. Testy penetracyjne są szczególnie ważne, gdy organizacje przechodzą ze starszych technologii do nowszych (np. przechodzenie od protokołów sieciowych IPv4 do IPv6).

Organizacje mogą wykorzystać wyniki analiz podatności do wsparcia działań związanych z testami penetracyjnymi. Testy penetracyjne mogą być przeprowadzane wewnętrznie lub zewnętrznie na sprzęcie, aplikacjach lub oprogramowaniu układowym komponentów systemu i mogą testować zarówno fizyczne jak i techniczne zabezpieczenia. Standardowa metoda badania penetracyjnego obejmuje analizę przed testem w oparciu o pełną wiedzę o systemie, wstępną identyfikację potencjalnych podatności w oparciu o analizę przed testem oraz badania mające na celu określenie możliwości wykorzystania podatności. Wszystkie strony zgadzają się na zasady zaangażowania przed przystąpieniem do realizacji scenariuszy testów penetracyjnych. Organizacje dokonują korelacji zasad zaangażowania w testy

penetracyjne z narzędziami, technikami i procedurami, które mają być stosowane przez przeciwników. Badania penetracyjne mogą prowadzić do ujawnienia osobom przeprowadzającym badania informacji, które są chronione przepisami prawa. Zasady zaangażowania, umowy lub inne odpowiednie mechanizmy mogą być wykorzystane do ustalenia zasad, co do sposobu ochrony tych informacji. Oceny ryzyka ukierunkowują decyzje dotyczące poziomu niezależności wymaganego od personelu prowadzącego badania penetracyjne.

Zabezpieczenia powiązane: RA-5, RA-10, SA-11, SR-5, SR-6.

Zabezpieczenia rozszerzone:

(1) TESTY PENETRACYJNE | NIEZALEŻNY TESTER LUB ZESPÓŁ PENETRACYJNY

Należy zatrudnić niezależnego testera lub zespół do przeprowadzenia badań penetracyjnych systemu lub jego komponentów.

Omówienie: Niezależni testerzy lub zespoły testujące penetrację to osoby lub grupy, które prowadzą bezstronne testy penetracyjne systemów organizacyjnych. Bezstronność oznacza, że agenci lub zespoły przeprowadzające testy penetracyjne są wolne od postrzeganych lub rzeczywistych konfliktów interesów w odniesieniu do rozwoju, eksploatacji lub zarządzania systemami, które są celem testów penetracyjnych. Zabezpieczenie rozszerzone CA-2(1) dostarcza dodatkowych informacji na temat niezależnych ocen, które mogą być stosowane do badań penetracyjnych.

Zabezpieczenia powiązane: CA-2.

(2) TESTY PENETRACYJNE | ĆWICZENIA ZESPOŁU ATAKUJĄCEGO TYPU „RED TEAM”

Stosowanie przez zespół atakujący typu „Red Team”, następujących ćwiczeń symulujące próby kompromitacji systemów organizacyjnych przez przeciwników, zgodnie z obowiązującymi zasadami działania: [***Realizacja: określone przez organizację ćwiczenia w ramach zespołu „Red Team”***]**.**

Omówienie: Ćwiczenia zespołu typu „Red Team" rozszerzają cele testów penetracyjnych, badając postawę organizacji w zakresie bezpieczeństwa i ochrony prywatności oraz możliwości wdrożenia skutecznej cyberobrony. Ćwiczenia zespołu „Red Team" symulują próby naruszenia przez przeciwników misji i funkcji biznesowych oraz zapewniają kompleksową ocenę postawy bezpieczeństwa i ochrony prywatności systemów i organizacji. Próby takie mogą obejmować ataki oparte na technologii oraz ataki oparte na inżynierii społecznej. Ataki oparte na technologii obejmują interakcję ze sprzętem IT, aplikacjami lub oprogramowaniem układowym i/lub komponentami misji i procesów biznesowych. Ataki oparte na technikach inżynierii społecznej obejmują interakcje za pośrednictwem poczty elektronicznej, telefonu, przeglądania stron internetowych lub osobistych rozmów. Ćwiczenia zespołu „Red Team" są najskuteczniejsze, gdy są przeprowadzane przez testerów i zespoły testujące posiadające wiedzę i doświadczenie w zakresie aktualnych taktyk, technik, procedur i narzędzi stosowanych przez przeciwników. Podczas gdy testy penetracyjne mogą być przede wszystkim testami laboratoryjnymi, organizacje mogą stosować ćwiczenia zespołu „Red Team", aby zapewnić bardziej kompleksowe oceny, które odzwierciedlają rzeczywiste warunki. Wyniki ćwiczeń zespołu „Red Team" mogą być wykorzystane przez organizacje do poprawy świadomości i szkolenia w zakresie bezpieczeństwa i ochrony prywatności oraz do oceny skuteczności zabezpieczeń.

Zabezpieczenia powiązane: Brak.

(3) TESTY PENETRACYJNE | LOKALNE TESTY PENETRACYJNE

Zastosowanie procesu testowania penetracyjnego, który obejmuje [***Realizacja: częstotliwość określona przez organizację***] [***Wybór: zaplanowane; niezapowiedziane***] **próby ominięcia lub obejścia zabezpieczeń związanych z fizycznymi punktami dostępu do obiektu.**

Omówienie: Badania penetracyjne fizycznych punktów dostępu mogą dostarczyć informacji o krytycznych lukach w środowiskach pracy systemów organizacyjnych. Informacje takie mogą być wykorzystane do korygowania słabych punktów lub braków w fizycznych zabezpieczeniach, które są niezbędne do ochrony systemów organizacyjnych.

Zabezpieczenia powiązane: CA-2, PE-3.

Referencje: Brak.

CA-9 POŁĄCZENIA WEWNĘTRZSYSTEMOWE

Zabezpieczenie podstawowe:

a. Autoryzacja wewnętrznych połączeń [*Realizacja: zdefiniowane przez organizację komponenty lub klasy komponentów systemu*] w ramach systemu organizacji;

b. Udokumentowanie, dla każdego połączenia wewnętrznego, charakterystyki interfejsu, wymogów bezpieczeństwa i ochrony prywatności oraz charakteru przekazywanych informacji;

c. Zakończenie wewnętrznych połączeń systemowych po [*Realizacja: warunki określone przez organizację*]; oraz

d. Weryfikacja [*Realizacja: z częstotliwością zdefiniowaną przez organizację*] ciągłego zapotrzebowania na każde połączenie wewnętrzne.

Omówienie: Wewnętrzne połączenia systemowe to połączenia między systemami organizacyjnymi i oddzielnymi składowymi systemu (tj. połączenia między komponentami, które są częścią tego samego systemu), w tym komponentami wykorzystywanymi do rozwoju systemu. Połączenia wewnątrzsystemowe obejmują połączenia z urządzeniami przenośnymi, notebookami i komputerami stacjonarnymi, tabletami, drukarkami, kopiarkami, faksami, skanerami, czujnikami i serwerami. Zamiast autoryzacji każdego wewnętrznego połączenia systemowego z osobna, organizacje mogą autoryzować połączenia wewnętrzne dla klasy komponentów systemowych o wspólnej charakterystyce i/lub konfiguracji, w tym drukarek, skanerów i kopiarek o określonej zdolności przetwarzania, transmisji i przechowywania lub smartfonów i tabletów o określonej konfiguracji podstawowej. Stała konieczność utrzymywania połączenia systemów wewnętrznych jest analizowana z perspektywy tego, czy zapewnia ono wsparcie dla misji organizacji lub funkcji biznesowych.

Zabezpieczenia powiązane: AC-3, AC-4, AC-18, AC-19, CM-2, IA-3, SC-7, SI-12.

Zabezpieczenia rozszerzone:

(1) POŁĄCZENIA WEWNĘTRZSYSTEMOWE | KONTROLE ZGODNOŚCI

Przeprowadzenie kontroli zgodności z zasadami bezpieczeństwa i ochrony prywatności w komponentach systemu przed ustanowieniem połączenia wewnętrznego.

Omówienie: Zabezpieczenia zgodności obejmują weryfikację konfiguracji bazowych.

Zabezpieczenia powiązane: CM-6.

KATEGORIA CM - ZARZĄDZANIE KONFIGURACJĄ

CM-1 POLITYKA I PROCEDURY

Zabezpieczenie podstawowe:

a. Opracowywanie, dokumentowanie i rozpowszechnianie wśród [*Realizacja: personel lub role określone przez organizację*]*:*

1. [*Wybór (jeden lub więcej): poziom organizacji; poziom misji/procesu biznesowego; poziom systemu*] polityki zarządzania konfiguracją, która:

(a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami; oraz

(b) Jest zgodna z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi; oraz

2. Procedur ułatwiających realizację polityki w zakresie zarządzania konfiguracją oraz powiązanych ocen w zakresie zarządzania konfiguracją;

b. Wyznaczanie [*Realizacja: osoba wyznaczona przez organizację*] do zarządzania rozwojem, dokumentacją i rozpowszechnianiem polityki i procedur zarządzania konfiguracją; oraz

c. Przeglądanie i aktualizacja bieżącej:

1. Polityki zarządzania konfiguracją z [Realizacja: *częstotliwość określona przez organizację*] i następujących [*Realizacja: zdarzenia określone przez organizację*]; oraz

2. Procedur zarządzania konfiguracją z [Realizacja: *częstotliwość określona przez organizację*] i następujących [*Realizacja: zdarzenia określone przez organizację*].

Omówienie: Polityka i procedury w zakresie zarządzania konfiguracją dotyczą zabezpieczeń w kategorii *Zarządzanie konfiguracją* (CM), które są wdrażane w ramach systemów i organizacji. Strategia zarządzania ryzykiem jest ważnym czynnikiem przy tworzeniu takich polityk i procedur. Polityki i procedury przyczyniają się do zapewnienia bezpieczeństwa i ochrony prywatności. Dlatego ważne jest, aby programy bezpieczeństwa i ochrony prywatności były opracowywane wspólnie przy kształtowaniu polityki i procedur zarządzania konfiguracją. Polityki i procedury dotyczące programów bezpieczeństwa i ochrony prywatności na poziomie organizacji są ogólnie rzecz biorąc preferowane i mogą eliminować potrzeby tworzenia polityk i procedur specyficznych dla danej misji lub systemu. Polityka może być włączona, jako część ogólnej polityki bezpieczeństwa i ochrony prywatności lub reprezentowana przez wiele polityk odzwierciedlających złożony charakter organizacji. Procedury mogą być ustanowione dla programów bezpieczeństwa i ochrony prywatności, dla misji lub procesów biznesowych oraz dla systemów, jeśli to konieczne. Procedury opisują sposób wdrażania zasad lub zabezpieczeń i mogą być skierowane do osoby lub roli, która jest przedmiotem procedury. Procedury mogą być udokumentowane w planach bezpieczeństwa i ochrony prywatności systemu w jednym lub kilku oddzielnych dokumentach.

Zdarzenia, które mogą spowodować konieczność aktualizacji polityki i procedur zarządzania konfiguracją, obejmują wyniki oceny lub audytu, incydenty lub naruszenia bezpieczeństwa, lub zmiany w przepisach prawa, zarządzeniach, dyrektywach, rozporządzeniach, zasadach, standardach i wytycznych.

Oświadczenie o wprowadzeniu zabezpieczeń nie jest równoznaczne z ustanowieniem polityki lub procedury organizacyjnej.

Zabezpieczenia powiązane: PM-9, PS-8, SA-8, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [NIST SP 800-12], [NIST SP 800-30], [NIST SP 800-39], [NIST SP 800-100].

CM-2 KONFIGURACJA BAZOWA

Zabezpieczenie podstawowe:

a. Opracowanie, udokumentowanie i utrzymanie pod kontrolą bieżącej konfiguracji bazowej systemu; oraz

b. Przeglądanie i aktualizacja konfiguracji bazowej systemu:

   1. Z [*Realizacja: częstotliwość określona przez organizację*]*;*

   2. Jeżeli jest to wymagane ze względu na [*Realizacja: okoliczności określone przez organizację*]*;* oraz

   3. Podczas instalacji lub modernizacji komponentów systemu.

Omówienie: Konfiguracje bazowe systemów i komponentów systemu obejmują aspekty połączeń, działania i komunikacji systemów. Konfiguracje bazowe są udokumentowanymi, formalnie zweryfikowanymi i uzgodnionymi specyfikacjami odnoszącymi się do systemów lub elementów konfiguracyjnych w ramach tych systemów. Konfiguracje bazowe służą, jako podstawa dla przyszłych opracowań, wersji lub zmian systemów i obejmują implementacje środków bezpieczeństwa i ochrony prywatności, procedury operacyjne, informacje o komponentach systemu, topologię sieci oraz logiczne rozmieszczenie komponentów w architekturze systemu. Utrzymanie konfiguracji bazowych wymaga tworzenia nowych konfiguracji bazowych w miarę wprowadzanych zmian systemów organizacyjnych. Konfiguracje bazowe systemów odzwierciedlają obecną architekturę korporacyjną.

Zabezpieczenia powiązane: AC-19, AU-6, CA-9, CM-1, CM-3, CM-5, CM-6, CM-8, CM-9, CP-9, CP-10, CP-12, MA-2, PL-8, PM-5, SA-8, SA-10, SA-15, SC-18.

Zabezpieczenia rozszerzone:

(1) KONFIGURACJA BAZOWA | PRZEGLĄDY I AKTUALIZACJE

[Wycofane: Włączone do CM-2].

(2) KONFIGURACJA BAZOWA | AUTOMATYZACJA WSPIERAJĄCA AKTUALNOŚĆ / SZCZEGÓŁOWOŚĆ

Utrzymanie aktualności, kompletności, dokładności i dostępności konfiguracji bazowej systemu przy użyciu [***Realizacja: organizacyjnie zdefiniowane zautomatyzowane mechanizmy wspomagające***]**.**

Omówienie: Zautomatyzowane mechanizmy, które pomagają organizacjom utrzymać spójne konfiguracje bazowe systemów obejmują narzędzia do zarządzania konfiguracją, sprzęt, oprogramowanie (aplikacje), narzędzia do inwentaryzacji oprogramowania sprzętowego i narzędzia do zarządzania siecią. Narzędzia zautomatyzowane mogą być wykorzystywane na poziomie organizacji, misji i procesów biznesowych lub na poziomie systemu na stacjach roboczych, serwerach, notebookach, komponentach sieciowych lub urządzeniach przenośnych. Narzędzia mogą być wykorzystywane do śledzenia numerów wersji systemów operacyjnych, aplikacji, typów zainstalowanego oprogramowania i aktualnych poziomów poprawek. Wsparcie automatyzacji w zakresie prawidłowości i aktualności może być osiągane poprzez wdrożenie przez organizację zabezpieczenia rozszerzonego CM-8(2), które wykonuje czynności związane z inwentaryzacją komponentów systemu i konfiguracją bazową.

Zabezpieczenia powiązane: CM-7, IA-3, RA-5.

(3) KONFIGURACJA BAZOWA | RETENCJA ZACHOWANYCH KONFIGURACJI

Zachowanie [***Realizacja: liczba zdefiniowany przez organizację***] **poprzednich wersji konfiguracji bazowych systemu w celu obsługi wycofanych wersji konfiguracji bazowych.**

Omówienie: Zachowanie poprzednich wersji konfiguracji bazowych w celu wsparcia wycofywania sprzętu, aplikacji, oprogramowania układowego, plików konfiguracyjnych, rekordów konfiguracyjnych i związanej z nimi dokumentacji.

Zabezpieczenia powiązane: Brak.

(4) KONFIGURACJA BAZOWA | NIEAUTORYZOWANE OPROGRAMOWANIE

[Wycofane: Włączone do CM-7(4)]

(5) KONFIGURACJA BAZOWA | AUTORYZOWANE OPROGRAMOWANIE

[Wycofane: Włączone do CM-7(5)].

(6) KONFIGURACJA BAZOWA | ŚRODOWISKA PROGRAMISTYCZNE I TESTOWE

Utrzymanie konfiguracji bazowej do rozbudowy systemów i środowiska testowego, które są zarządzane niezależnie od operacyjnej konfiguracji bazowej.

Omówienie: Ustanowienie odrębnych konfiguracji dla środowisk rozwojowych, testowych i operacyjnych chroni systemy przed nieplanowanymi lub nieoczekiwanymi zdarzeniami związanymi z działaniami programistycznymi i testowymi. Oddzielne konfiguracje bazowe pozwalają organizacjom na zastosowanie zarządzania konfiguracją, które jest najbardziej odpowiednie dla każdego typu konfiguracji. Na przykład, zarządzanie konfiguracjami operacyjnymi zazwyczaj podkreśla potrzebę stabilności, podczas gdy zarządzanie konfiguracjami rozwojowymi lub testowymi wymaga większej elastyczności. Konfiguracje w środowisku testowym odzwierciedlają konfiguracje w środowisku operacyjnym w takim zakresie, w jakim jest to możliwe, tak, aby wyniki testów były reprezentatywne dla proponowanych zmian w systemach operacyjnych. Oddzielne konfiguracje bazowe nie muszą wymagać oddzielnych środowisk fizycznych.

Zabezpieczenia powiązane: CM-4, SC-3, SC-7.

(7) KONFIGURACJA BAZOWA | KONFIGURACJA SYSTEMÓW I KOMPONENTÓW W OBSZARACH WYSOKIEGO RYZYKA

(a) Przydzielanie [Realizacja: *systemy lub komponenty systemowe zdefiniowane przez organizację*] z [*Realizacja: konfiguracje zdefiniowane przez*

organizację] **osobom podróżującym do lokalizacji, które organizacja uważa za miejsca o istotnym ryzyku; oraz**

(b) Zastosowanie następujących zabezpieczeń w systemach lub komponentach będących w posiadaniu osób powracających z podróży: [Realizacja: zabezpieczenia zdefiniowane przez organizację].

Omówienie: Kiedy wiadomo, że systemy lub elementy systemu będą znajdować się poza organizacją w obszarach wysokiego ryzyka, można wprowadzić dodatkowe zabezpieczenia w celu przeciwdziałania zwiększonemu zagrożeniu w takich lokalizacjach. Na przykład, organizacje mogą podjąć działania w odniesieniu do notebooków używanych przez osoby wyjeżdżające i powracające z podróży. Działania te obejmują określenie miejsc, które stanowią zagrożenie, zdefiniowanie wymaganych konfiguracji komponentów, zapewnienie, że komponenty są skonfigurowane zgodnie z założeniami przed rozpoczęciem podróży oraz zastosowanie środków bezpieczeństwa do komponentów po jej zakończeniu. Specjalnie skonfigurowane notebooki obejmują komputery poddane sanityzacji dysków twardych, ograniczaniu aplikacji i bardziej rygorystycznym ustawieniom konfiguracyjnym. Zabezpieczenia stosowane do urządzeń przenośnych użytkowanych na poza lokalizacją organizacji obejmują badanie urządzenia przenośnego pod kątem śladów ingerencji fizycznej oraz czyszczeniu i odtwarzaniu dysków. Ochrona informacji znajdujących się na urządzeniach przenośnych jest uwzględniona w kategorii *Ochrona nośników danych* (MP).

Zabezpieczenia powiązane: MP-4, MP-5.

Referencje: [NIST SP 800-124], [NIST SP 800-128].

CM-3 ZABEZPIECZANIE ZMIAN KONFIGURACJI

Zabezpieczenie podstawowe:

a. Należy określić i udokumentować rodzaje zmian w systemie, które są zabezpieczane konfiguracyjnie;

b. Dokonanie przeglądu proponowanych zmian konfiguracji zabezpieczeń w systemie i zatwierdzenie lub odrzucenie takich zmian, z wyraźnym uwzględnieniem analizy wpływu na bezpieczeństwo systemu i prywatność;

c. Dokumentowanie decyzji związanych ze zmianą konfiguracji systemu;

d. Wdrożenie zatwierdzonych zmian w zabezpieczeniach konfiguracji systemu;

e. Przechowywanie dokonanych zapisów zmian w zabezpieczeniach systemu przez okres [*Realizacja: okres czasu określony przez organizację*];

f. Monitorowanie i przeglądanie czynności związanych z dokonywanymi zmianami w zabezpieczeniach konfiguracji systemu; oraz

g. Koordynacja i nadzór nad działaniami związanymi z dokonywanymi zmianami w zabezpieczeniach konfiguracji przez [*Realizacja: zdefiniowany przez organizację element zabezpieczeń zmian konfiguracyjnych*], który wywołuje z [*Wybór (jeden lub więcej)*]: [*Realizacja: częstotliwość zdefiniowana przez organizację*]; występowanie [*Realizacja: warunki zmiany konfiguracji zdefiniowanej przez organizację*]].

Omówienie: Zabezpieczenie zmian konfiguracyjnych w systemach organizacyjnych obejmuje systematyczne zgłaszanie, uzasadnianie, wdrażanie, testowanie, przegląd i usuwanie zmian w systemie, w tym aktualizacje i modyfikacje systemu. Zabezpieczenie zmian konfiguracyjnych obejmuje zmiany konfiguracji bazowych, elementów konfiguracyjnych systemów, procedur operacyjnych, ustawień konfiguracyjnych komponentów systemu, usuwanie luk oraz nieplanowanych lub nieautoryzowanych zmian. Procesy zarządzania zmianami konfiguracji systemów są realizowane przez zespoły kontroli konfiguracji (*ang. Configuration Control Boards* -

CCB) lub zespoły doradcze ds. wprowadzania zmian (*ang. Change Advisory Boards - CAB*), które dokonują przeglądu i zatwierdzenia proponowanych zmian. W przypadku zmian, które mają wpływ na ryzyko związane z ochroną prywatności, SAOP[42]/inspektor ochrony danych aktualizuje oceny wpływu na prywatność oraz system powiadomień o zmianach. W przypadku nowych systemów lub kluczowych aktualizacji, organizacje rozważają włączenie przedstawicieli organizacji deweloperskich (programistycznych) do CCB lub CAB. Audyt zmian obejmuje działania przed i po wprowadzeniu modyfikacji w systemach oraz działania audytowe wymagane do wdrożenia tych zmian. Patrz również zabezpieczenie SA-10.

Zabezpieczenia powiązane: CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, CM-11, IA-3, MA-2, PE-16, PT-6, RA-8, SA-8, SA-10, SC-28, SC-34, SC-37, SI-2, SI-3, SI-4, SI-7, SI-10, SR-11.

Zabezpieczenia rozszerzone:

(1) ZABEZPIECZENIE ZMIAN KONFIGURACJI | AUTOMATYCZNA DOKUMENTACJA / POWIADAMIANIE / ZAKAZ WPROWADZANIA ZMIAN

Stosowanie [***Realizacja: mechanizmy automatyczne zdefiniowane przez organizację***] **do:**

(a) Dokumentowania proponowanych zmian w systemie;

(b) Powiadamianie [***Realizacja: określone przez organizację organy zatwierdzające***] **o proponowanych zmianach w systemie i zażądanie zatwierdzenia zmian;**

(c) Wskazanie proponowanych zmian w systemie, które nie zostały zatwierdzone lub odrzucone w ciągu [Realizacja: *okres czasu określony przez organizację*];

[42] Patrz: NSC 800-37; NSC 7298.

(d) Zakazanie wprowadzania zmian w systemie do czasu otrzymania stosownych akceptacji;

(e) Dokumentowanie wszystkich zmian w systemie; oraz

(f) Powiadomienie [***Realizacja: personel zdefiniowany przez organizację***] ***o* zakończeniu wprowadzania zatwierdzonych zmian w systemie.**

Omówienie: Brak.

Zabezpieczenia powiązane: Brak.

(2) ZABEZPIECZENIE ZMIAN KONFIGURACJI | TESTY, WALIDACJA I ZMIANY DOKUMENTÓW

Testowanie, zatwierdzenie i dokumentowanie zmian w systemie przed ich wdrożeniem do systemu.

Omówienie: Zmiany w systemach obejmują modyfikacje sprzętu, aplikacji lub oprogramowania układowego komponentów oraz ustawienia konfiguracyjne zdefiniowane w CM-6. Organizacje zapewniają, że testy nie kolidują z wykonywanymi przez system operacjami wspierającymi misję organizacji i funkcje biznesowe. Osoby lub grupy przeprowadzające testy rozumieją zasady i procedury bezpieczeństwa i ochrony prywatności, politykę i procedury bezpieczeństwa systemu oraz zagrożenia dla zdrowia, bezpieczeństwa i środowiska związane z określonymi obiektami lub procesami. Przed przeprowadzeniem testów może zaistnieć potrzeba wyłączenia systemów operacyjnych z sieci lub ich replikacja w możliwym do przeprowadzenia zakresie. Jeżeli systemy muszą zostać wyłączone z eksploatacji w celu przeprowadzenia testów, testy planuje się przeprowadzić w miarę możliwości podczas planowanych przerw w funkcjonowaniu systemów. Jeżeli testy nie mogą być przeprowadzone na systemach operacyjnych, organizacje stosują zabezpieczenia kompensacyjne.

Zabezpieczenia powiązane: Brak.

(3) ZABEZPIECZENIE ZMIAN KONFIGURACJI | AUTOMATYCZNE WPROWADZANIE ZMIAN

Zaimplementowanie zmian w aktualnej bazie systemu i wdrożenie uaktualnionej konfiguracji bazowej w zainstalowanej bazie za pomocą [***Realizacja: automatyczne mechanizmy zdefiniowane przez organizację***]**.**

Omówienie: Zautomatyzowane narzędzia mogą poprawić dokładność, spójność i dostępność informacji dotyczących konfiguracji bazowych. Automatyzacja może również zapewnić agregację danych i możliwość korelacji danych, mechanizmy ostrzegawcze i pulpity nawigacyjne wspierające podejmowanie decyzji w organizacji w oparciu o ryzyko.

Zabezpieczenia powiązane: Brak.

(4) ZABEZPIECZENIE ZMIAN KONFIGURACJI | FUNKCYJNI DS. BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Wymaganie, aby [***Realizacja: zdefiniowani przez organizację*** **przedstawiciele ds. bezpieczeństwa i ochrony prywatności], byli członkami** [***Realizacja: zdefiniowany przez organizację zespół zabezpieczeń zmiany konfiguracji***]**.**

Omówienie: Przedstawiciele ds. bezpieczeństwa informacji i ochrony prywatności obejmują SSO, SAISO, SAOP, lub SPO.[43] Zaangażowanie personelu posiadającego wiedzę z zakresu bezpieczeństwa informacji i ochrony prywatności jest istotne, ponieważ zmiany konfiguracji systemu mogą mieć niezamierzone skutki uboczne, z których niektóre mogą mieć znaczenie dla bezpieczeństwa lub ochrony prywatności. Wykrycie takich zmian na wczesnym etapie procesu może pomóc uniknąć niezamierzonych, negatywnych konsekwencji, które mogłyby ostatecznie wpłynąć na bezpieczeństwo i stan ochrony prywatność systemów. Element zabezpieczeń zmian w konfiguracji, określony w parametrze

[43] Role i obowiązki przedstawicieli opisane są w NSC -800-37 oraz NSC 7298.

definiowanym przez organizację, odzwierciedla elementy zabezpieczenia zmian zdefiniowane przez organizacje w zabezpieczeniu CM-3g.

Zabezpieczenia powiązane: Brak.

(5) ZABEZPIECZANIE ZMIAN KONFIGURACJI | AUTOMATYCZNA REAKCJA BEZPIECZEŃSTWA

Zaimplementowanie następujących automatycznych reakcji środków bezpieczeństwa na nieautoryzowane zmiany konfiguracji bazowych: [Realizacja: *reakcje środków bezpieczeństwa zdefiniowane przez organizację*].

Omówienie: Zautomatyzowane odpowiedzi mechanizmów bezpieczeństwa w przypadku nieautoryzowanej modyfikacji elementu konfiguracji obejmują zatrzymanie wybranych funkcji systemu, wstrzymanie przetwarzania systemu oraz generowanie ostrzeżeń lub powiadomień personelu organizacji.

Zabezpieczenia powiązane: Brak.

(6) ZABEZPIECZENIE ZMIAN KONFIGURACJI | ZARZĄDZANIE KRYPTOGRAFICZNE

Zapewnienie, że mechanizmy kryptograficzne używane do zapewnienia [*Realizacja: środki bezpieczeństwa zdefiniowane przez organizację*] podlegają zarządzaniu konfiguracji.

Omówienie: Zabezpieczenia te odnoszą się do środków bezpieczeństwa i ochrony prywatności zawartych w katalogu zabezpieczeń. Niezależnie od zastosowanych mechanizmów kryptograficznych, istnieją procesy i procedury służące do zarządzania tymi mechanizmami. Na przykład, jeśli komponenty systemu używają certyfikatów do identyfikacji i uwierzytelniania, wdrażany jest proces mający na celu uwzględnienie wygaśnięcia tych certyfikatów.

Zabezpieczenia powiązane: SC-12.

(7) ZABEZPIECZENIE ZMIAN KONFIGURACJI | PRZEGLĄD ZMIAN W SYSTEMIE

Przeglądanie zmian w systemie z [***Realizacja: częstotliwość zdefiniowana przez organizację***] **lub wystąpienia** [***Realizacja: okoliczności zdefiniowane przez organizację***] **w celu ustalenia, czy wystąpiły nieautoryzowane zmiany.**

Omówienie: Wskazówki, które uzasadniają dokonanie przeglądu zmian w systemie i specyficzne okoliczności wymagające takich przeglądów można uzyskać z działań prowadzonych przez organizacje w trakcie procesu zmiany konfiguracji lub procesu ciągłego monitorowania.

Zabezpieczenia powiązane: AU-6, AU-7, CM-3.

(8) ZABEZPIECZANIE ZMIAN KONFIGURACJI | ZAPOBIEGANIE LUB OGRANICZANIE ZMIAN KONFIGURACJI

Zapobieganie lub ograniczanie zmian w konfiguracji systemu w następujących okolicznościach: [Realizacja: *okoliczności zdefiniowane przez organizację*].

Omówienie: Zmiany w konfiguracji systemu mogą mieć negatywny wpływ na krytyczne funkcje bezpieczeństwa i ochrony prywatności systemu. Ograniczenia zmian mogą być egzekwowane za pomocą automatycznych mechanizmów.

Zabezpieczenia powiązane: Brak.

Referencje: [NIST SP 800-124], [NIST SP 800-128], [IR 8062].

CM-4 ANALIZY WPŁYWU

Zabezpieczenie podstawowe: Analizowanie zmian w systemie w celu określenia potencjalnego wpływu na bezpieczeństwo i prywatność przed wprowadzeniem zmian.

Omówienie: Personel organizacyjny odpowiedzialny za bezpieczeństwo lub prywatność przeprowadza analizy wpływu. Osoby przeprowadzające analizy wpływu posiadają niezbędne umiejętności i wiedzę techniczną, aby analizować zmiany w systemach, a także wpływ tych zmian na bezpieczeństwo lub prywatności. Analizy wpływu obejmują przegląd planów, polityk i procedur w zakresie bezpieczeństwa i ochrony prywatności w celu zrozumienia wymagań dotyczących zabezpieczeń; przegląd dokumentacji projektowej systemu i procedur operacyjnych w celu zrozumienia wdrażania zabezpieczeń i sposobu, w jaki konkretne zmiany w systemie mogą wpływać na zabezpieczenia; przeglądanie z interesariuszami wpływu zmian na partnerów organizacyjnych łańcucha dostaw; oraz określenie, w jaki sposób potencjalne zmiany w systemie stwarzają nowe zagrożenia dla prywatności osób fizycznych oraz możliwości ograniczania tych zagrożeń przez wdrożone zabezpieczenia. Analizy wpływu obejmują również ocenę ryzyka w celu zrozumienia wpływu zmian i określenia, czy konieczne są dodatkowe zabezpieczenia.

Zabezpieczenia powiązane: CA-7, CM-3, CM-8, CM-9, MA-2, RA-3, RA-5, RA-8, SA-5, SA-8, SA-10, SI-2.

Zabezpieczenia rozszerzone:

(1) ANALIZY WPŁYWU | ODDZIELNE ŚRODOWISKA BADAWCZE

Analizowanie zmian w systemie w oddzielnym środowisku testowym przed ich wdrożeniem w środowisku operacyjnym, zwracając uwagę na wpływ na bezpieczeństwo i prywatność z powodu wad, słabości, niekompatybilności lub celowego złośliwego działania.

Omówienie: Odrębne środowisko badawcze wymaga środowiska, które jest fizycznie lub logicznie oddzielone i różni się od środowiska operacyjnego. Odrębność jest wystarczająca, aby zapewnić, że działania w środowisku badawczym nie mają wpływu na działania w środowisku operacyjnym oraz, że informacje w środowisku operacyjnym nie są przypadkowo przekazywane do środowiska badawczego. Oddzielne środowiska można osiągnąć za pomocą środków fizycznych lub logicznych. Jeżeli nie zostaną wdrożone fizycznie oddzielne środowiska testowe, organizacje określają siłę mechanizmu wymaganego przy wdrażaniu rozdziału logicznego.

Zabezpieczenia powiązane: SA-11, SC-7.

(2) ANALIZY WPŁYWU | WERYFIKACJA ZABEZPIECZEŃ

Po dokonaniu zmian w systemie, należy sprawdzić, czy zabezpieczenie jest wdrożone prawidłowo, działa zgodnie z założeniami i przynosi pożądany rezultat w odniesieniu do spełnienia wymogów bezpieczeństwa i ochrony prywatności systemu.

Omówienie: Wdrożenie w tym kontekście odnosi się do instalacji zmienionego kodu w systemie operacyjnym, który może mieć wpływ na bezpieczeństwo lub ochronę prywatności.

Zabezpieczenia powiązane: SA-11, SC-3, SI-6.

Referencje: [NIST SP 800-128].

CM-5 OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN

Zabezpieczenie podstawowe: Definiowanie, dokumentowanie, zatwierdzanie i egzekwowanie fizycznych i logicznych ograniczeń dostępu związanych ze zmianami w systemie.

Omówienie: Zmiany w sprzęcie, aplikacjach lub oprogramowaniu układowym systemów lub w procedurach operacyjnych związanych z systemem mogą potencjalnie mieć znaczący wpływ na bezpieczeństwo systemów lub prywatność osób. W związku z tym organizacje zezwalają na dostęp do systemów tylko osobom wykwalifikowanym i upoważnionym w celu zainicjowania zmian. Ograniczenia dostępu obejmują fizyczne i logiczne zabezpieczenie dostępu (zob. zabezpieczenia AC-3 i PE-3), biblioteki oprogramowania, automatyzację przepływu pracy, biblioteki multimedialne, warstwy abstrakcyjne (tj. zmiany wprowadzane do interfejsów zewnętrznych, a nie bezpośrednio do systemów) oraz okna zmian (tj. zmiany następują tylko w określonym czasie).

Zabezpieczenia powiązane: AC-3, AC-5, AC-6, CM-9, PE-3, SC-28, SC-34, SC-37, SI-2, SI-10.

Zabezpieczenia rozszerzone:

(1) OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | AUTOMATYCZNE EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU I ZAPISY Z AUDYTU

(a) Egzekwowanie ograniczeń dostępu przy użyciu [***Realizacja: automatyczne mechanizmy zdefiniowane przez organizację***]***;*** **oraz**

(b) Automatyczne generowanie zapisów z audytu działań wykonawczych.

Omówienie: Organizacje uzyskują dostęp do logów systemowych związanych z wprowadzaniem zmian konfiguracyjnych w celu zapewnienia, że zabezpieczenie

zmian konfiguracyjnych jest realizowana oraz w celu wsparcia działań po fakcie wykrycia przez organizacje nieautoryzowanych zmian.

Zabezpieczenia powiązane: AU-2, AU-6, AU-7, AU-12, CM-6, CM-11, SI-12.

(2) OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | PRZEGLĄD ZMIAN W SYSTEMIE

[Wycofane: Włączone do CM-3(7)]

(3) OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | PODPISANE KOMPONENTY

[Wycofane: Włączone do CM-14].

(4) OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | PODWÓJNA AUTORYZACJA

Egzekwowanie podwójnej autoryzacji do wprowadzania zmian w [***Realizacja: zdefiniowane przez organizacje komponenty systemu i informacje na poziomie systemu***]**.**

Omówienie: Organizacje stosują podwójną autoryzację, aby zapewnić, że wszelkie zmiany w wybranych komponentach systemu i informacjach nie mogą wystąpić, chyba, że dwie wykwalifikowane osoby zatwierdzą i wdrożą takie zmiany. Te dwie osoby posiadają umiejętności i wiedzę specjalistyczną pozwalające stwierdzić, czy proponowane zmiany są prawidłowym wdrożeniem zatwierdzonych zmian. Osoby te są również odpowiedzialne za zmiany. Podwójna autoryzacja może być również znana, jako zabezpieczenie dwuosobowe. Aby zmniejszyć ryzyko zmowy, organizacje rozważają rotację obowiązków wynikających z podwójnej autoryzacji w stosunku do innych osób. Informacje na poziomie systemu obejmują procedury operacyjne.

Zabezpieczenia powiązane: AC-2, AC-5, CM-3.

(5) OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | OGRANICZANIE PRZYWILEJÓW W ZAKRESIE WYTWARZANIA I EKSPLOATACJI

(a) Ograniczenie uprawnienia do zmiany komponentów systemu i informacji związanych z systemem w ramach środowiska produkcyjnego lub operacyjnego; oraz

(b) Przeglądanie i ponowna ocena uprawnień [***Realizacja: częstotliwość określona przez organizację***]**.**

Omówienie: W wielu organizacjach systemy wspierają wiele misji i funkcji biznesowych. Ograniczenie uprawnień do zmiany komponentów systemu w odniesieniu do systemów operacyjnych jest konieczne, ponieważ zmiany w komponencie systemu mogą mieć daleko idące skutki dla misji i procesów biznesowych wspieranych przez system. Relacje pomiędzy systemami, a procesami misyjnymi/biznesowymi są w niektórych przypadkach nieznane programistom. Informacje związane z systemem obejmują procedury operacyjne.

Zabezpieczenia powiązane: AC-2.

(6) OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | OGRANICZANIE PRZYWILEJÓW W BIBLIOTEKACH OPROGRAMOWANIA

Ograniczenie uprawnień do zmiany oprogramowania rezydenta w bibliotekach oprogramowania.

Omówienie: Biblioteki oprogramowania zawierają aplikacje uprzywilejowane.

Zabezpieczenia powiązane: AC-2.

(7) OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | AUTOMATYCZNE WDRAŻANIE ŚRODKÓW BEZPIECZEŃSTWA

[Wycofane: Włączone do SI-7].

Referencje: [FIPS 140-3]; [FIPS 186-4].

CM-6 USTAWIENIA KONFIGURACJI

Zabezpieczenie podstawowe:

a. Ustalenie i udokumentowanie ustawień konfiguracyjnych komponentów stosowanych w systemie, które odzwierciedlają najbardziej restrykcyjny tryb zgodny z wymogami operacyjnymi, korzystając z [*Realizacja: listy kontrolne konfiguracji zabezpieczeń zdefiniowane przez organizację*];

b. Zaimplementowanie ustawień konfiguracyjnych;

c. Określanie, dokumentowanie i zatwierdzanie wszelkich odstępstw od ustalonych ustawień konfiguracyjnych dla [Realizacja: *zdefiniowane przez organizację komponenty systemu*] w oparciu o [*Realizacja: zdefiniowane przez organizację wymagania operacyjne*]; oraz

d. Monitorowanie i zabezpieczanie zmian w ustawieniach konfiguracyjnych zgodnie z zasadami i procedurami organizacji.

Omówienie: Ustawienia konfiguracyjne to parametry, które mogą być zmieniane w komponentach sprzętowych, aplikacjach lub oprogramowaniu układowym, a które wpływają na bezpieczeństwo i prywatność lub funkcjonalność systemu. Produkty informatyczne, w których można zdefiniować ustawienia konfiguracyjne, obejmują komputery typu mainframe, serwery, stacje robocze, systemy operacyjne, urządzenia przenośne, urządzenia wejścia/wyjścia, protokoły i aplikacje. Parametry, które mają wpływ na bezpieczeństwo systemów, obejmują ustawienia rejestru; ustawienia uprawnień do konta, pliku lub katalogu; oraz ustawienia funkcji, protokołów, portów, usług i połączeń zdalnych. Parametry ochrony prywatności to parametry wpływające na stan ochrony prywatności systemów, w tym parametry wymagane do spełnienia innych zabezpieczeń prywatności. Parametry prywatności obejmują ustawienia kontroli dostępu, preferencje dotyczące przetwarzania danych oraz uprawnienia do przetwarzania i zatrzymywania danych. Organizacje ustanawiają ustawienia konfiguracyjne dla całej organizacji, a następnie wprowadzają specyficzne ustawienia

konfiguracyjne dla systemów. Ustalone ustawienia stają się częścią składową konfiguracji bazowej systemu.

Bezpieczne konfiguracje wspólne (znane również jako listy kontrolne konfiguracji zabezpieczeń, przewodniki blokowania i ograniczania oraz przewodniki referencyjne dotyczące zabezpieczeń) zapewniają uznane, standaryzowane i ustalone wzorce, które określają bezpieczne ustawienia konfiguracyjne dla produktów i platform informatycznych, a także instrukcje dotyczące konfiguracji tych produktów lub platform w celu spełnienia wymagań operacyjnych. Bezpieczne konfiguracje wspólne mogą być opracowywane przez różne organizacje, w tym przez twórców produktów informatycznych, producentów, sprzedawców, agencje państwowe, konsorcja, środowiska akademickie, przemysł i inne organizacje z sektora publicznego i prywatnego.

Wdrożenie bezpiecznej konfiguracji wspólnej może być zlecone na poziomie organizacji, misji i procesów biznesowych, na poziomie systemu lub na wyższym poziomie, w tym przez organ regulacyjny. Bezpieczne konfiguracje wspólne obejmują Podstawową Konfigurację Rządową Stanów Zjednoczonych (*ang. United States Government Configuration Baseline* - [USGCB]) oraz Techniczne Instrukcje Implementacji Bezpieczeństwa (*ang. security technical implementation guides - STIGs*), które mają wpływ na implementację zabezpieczeń CM-6 i innych zabezpieczeń, takich jak AC-19 i CM-7. Protokół SCAP (*ang. Security Content Automation Protocol - SCAP*) oraz zdefiniowane w nim standardy stanowią skuteczną metodę unikalnej identyfikacji, śledzenia i zabezpieczeń ustawień konfiguracyjnych.

Zabezpieczenia powiązane: AC-3, AC-19, AU-2, AU-6, CA-9, CM-2, CM-3, CM-5, CM-7, CM-11, CP-7, CP-9, CP-10, IA-3, IA-5, PL-8, PL-9, RA-5, SA-4, SA-8, SA-9, SC-18, SC-28, SC-43, SI-2, SI-4, SI-6.

Zabezpieczenia rozszerzone:

(1) USTAWIENIA KONFIGURACJI | AUTOMATYCZNE ZARZĄDZANIE, STOSOWANIE I WERYFIKACJA

Zarządzanie, realizacja i weryfikacja ustawień konfiguracyjnych dla [Realizacja: *zdefiniowane przez organizację komponenty systemu*] za pomocą [*Realizacja: zdefiniowane przez organizację automatyczne mechanizmy*].

Omówienie: Zautomatyzowane narzędzia (np. narzędzia do ograniczania, narzędzia do konfiguracji bazowej) mogą poprawić dokładność, spójność i dostępność informacji o ustawieniach konfiguracyjnych. Automatyzacja może również zapewnić możliwość agregacji i korelacji danych, mechanizmy ostrzegania i pulpity menedżerskie wspierające podejmowanie decyzji opartych na analizie ryzyka w organizacji.

Zabezpieczenia powiązane: CA-7.

(2) USTAWIENIA KONFIGURACJI | ODPOWIEDŹ NA NIEAUTORYZOWANE ZMIANY

W odpowiedzi na nieautoryzowane zmiany w [*Realizacja: ustawienia konfiguracyjne zdefiniowane przez organizację*] *należy wykonać* następujące czynności: [*Realizacja: ustawienia konfiguracyjne zdefiniowane przez organizację*]: [*Realizacja: działania zdefiniowane przez organizację*].

Omówienie: Odpowiedzi na nieautoryzowane zmiany w ustawieniach konfiguracyjnych obejmują alarmowanie wyznaczonego personelu organizacyjnego, przywracanie ustalonych ustawień konfiguracyjnych, a w skrajnych przypadkach - wstrzymanie przetwarzania systemu.

Zabezpieczenia powiązane: IR-4, IR-6, SI-7.

(3) USTAWIENIA KONFIGURACJI | WYKRYWANIE NIEAUTORYZOWANYCH ZMIAN

[Wycofane: włączone do SI-7].

(4) USTAWIENIA KONFIGURACJI | PREZENTACJA ZGODNOŚCI

[Wycofane: włączone do CM-4].

Referencje: [NIST SP 800-70], [NIST SP 800-126], [NIST SP 800-128], [USGCB], [NCPR], [DOD STIG].

CM-7 ZASADA MINIMALNEJ FUNKCJONALNOŚCI

Zabezpieczenie podstawowe:

a. Skonfigurowanie systemu tak, aby zapewniał tylko [*Realizacja: niezbędne wymagane funkcje*]; oraz

b. Zakazanie lub ograniczenie korzystania z następujących funkcji, portów, protokołów, oprogramowania i/lub usług: [*Realizacja: zdefiniowane przez organizację zabronione lub ograniczone funkcje, porty systemowe, protokoły, oprogramowanie i/lub usługi*].

Omówienie: Systemy zapewniają szeroki zakres funkcji i usług. Niektóre z rutynowo dostarczanych funkcji i usług mogą nie być konieczne do wspierania istotnych misji organizacyjnych, funkcji lub operacji. Dodatkowo, czasami wygodnie jest dostarczyć wiele usług z jednego komponentu systemu, ale to zwiększa ryzyko ograniczenia usług dostarczanych przez ten pojedynczy komponent. Tam, gdzie jest to możliwe, organizacje ograniczają funkcjonalność komponentu do jednej funkcji na komponent. Organizacje rozważają usunięcie nieużywanego lub nieprzydatnego oprogramowania oraz wyłączenie nieużywanych lub niepotrzebnych fizycznych i logicznych portów i protokołów, aby zapobiec nieautoryzowanemu podłączaniu komponentów, przesyłaniu informacji i tunelowaniu. Organizacje stosują narzędzia do skanowania sieci, systemy wykrywania i zapobiegania włamaniom oraz technologie ochrony punktów końcowych, takie jak zapory ogniowe i systemy wykrywania włamań oparte na hostach, w celu identyfikacji i zapobiegania wykorzystywaniu zabronionych funkcji, protokołów, portów i usług. Najmniejszą funkcjonalność można również osiągnąć w ramach podstawowego projektu i rozwoju systemu (zobacz zabezpieczenia SA- 8, SC-2 i SC-3).

Zabezpieczenia powiązane: AC-3, AC-4, CM-2, CM-5, CM-6, CM-11, RA-5, SA-4, SA-5, SA-8, SA-9, SA-15, SC- 2, SC-3, SC-7, SC-37, SI-4.

Zabezpieczenia rozszerzone:

(1) ZASADA MINIMALNEJ FUNKCJONALNOŚCI | PRZEGLĄDY OKRESOWE

(a) Przegląd systemu [***Realizacja: częstotliwość określona przez organizację***] ***w* celu zidentyfikowania niepożądanych i/lub niezabezpieczonych funkcji, portów, protokołów, oprogramowania i usług; oraz**

(b) Wyłączenie lub usunięcie [***Realizacja: funkcje zdefiniowane przez organizację, porty, protokoły, oprogramowanie i usługi w ramach systemu uznane za* niepożądane *i/lub niezabezpieczone*]**.**

Omówienie: Organizacje dokonują przeglądu funkcji, portów, protokołów i usług dostarczanych przez systemy lub komponenty systemu w celu określenia funkcjonalności i usług, które kwalifikują się do wyeliminowania. Takie przeglądy są szczególnie ważne podczas przechodzenia od starszych technologii do nowszych (np. przejście z IPv4 do IPv6). Takie zmiany technologiczne mogą wymagać jednoczesnego wdrożenia starszych i nowszych technologii w okresie przejściowym i jak najszybszego powrotu do minimalnych niezbędnych funkcji, portów, protokołów i usług. Organizacje mogą albo zdecydować o relatywnym bezpieczeństwie funkcji, portu, protokołu i/lub usługi, albo oprzeć decyzję o bezpieczeństwie na ocenie innych podmiotów. Do niezabezpieczonych protokołów zalicza się Bluetooth, FTP i sieć peer-to-peer.

Zabezpieczenia powiązane: AC-18.

(2) ZASADA MINIMALNEJ FUNKCJONALNOŚCI | ZAPOBIEGANIA WYKONYWANIU PROGRAMU

Zapobieganie wykonywaniu programu zgodnie z [***Wybór (jeden lub więcej):*** [***Realizacja: zasady określone przez organizację, zasady zachowania i/lub umowy dostępu dotyczące użytkowania i ograniczeń w użytkowaniu oprogramowania*]***; zasady autoryzujące warunki użytkowania oprogramowania***]**.**

Omówienie: Zapobieganie realizacji programu dotyczy polityki organizacyjnej, zasad zachowania i/lub umów dostępu, które ograniczają korzystanie z oprogramowania oraz z warunków narzuconych przez twórcę lub producenta, w tym licencji na oprogramowanie i praw autorskich. Ograniczenia obejmują zakaz automatycznego wykonywania funkcji, ograniczanie ról dozwolonych do zatwierdzania wykonania programu, zezwalanie lub blokowanie uruchamiania określonych programów lub ograniczanie liczby jednocześnie wykonywanych instancji programu.

Zabezpieczenia powiązane: CM-8, PL-4, PL-9, PM-5, PS-6.

(3) ZASADA MINIMALNEJ FUNKCJONALNOŚCI | STOSOWANIE REJESTRACJI

Zapewnienie zgodności z [***Realizacja: określone przez organizację wymagania rejestracyjne dla funkcji, portów, protokołów i usług***]**.**

Omówienie: Organizacje wykorzystują proces rejestracji do zarządzania, śledzenia i zapewnienia nadzoru nad systemami i wdrażanymi funkcjami, portami, protokołami i usługami.

Zabezpieczenia powiązane: Brak.

(4) ZASADA MINIMALNEJ FUNKCJONALNOŚCI | NIEAUTORYZOWANE OPROGRAMOWANIE („CZARNA LISTA")

(a) Zidentyfikowanie [***Realizacja: programy zdefiniowane przez organizację, które nie są uprawnione do wykonywania w systemie***]**;**

(b) Stosowanie polityki „zezwalaj na wszystko za wyjątkiem" (***ang. "allow-all, deny-by-exception"***) **w celu zakazania wykonywania nieautoryzowanych programów w systemie; oraz**

(c) Przeglądanie i aktualizacja listy nieautoryzowanych programów [***Realizacja: częstotliwość zdefiniowana przez organizację***]**.**

Omówienie: Nieautoryzowane programy mogą być ograniczone do określonych wersji lub określonego źródła. Koncepcja zakazu wykonywania

nieautoryzowanego oprogramowania może być również zastosowana do działań użytkownika, portów i protokołów systemowych, adresów IP/pul adresów IP, stron internetowych i adresów MAC.

Zabezpieczenia powiązane: CM-6, CM-8, CM-10, PL-9, PM-5.

(5) ZASADA MINIMALNEJ FUNKCJONALNOŚCI | AUTORYZOWANE OPROGRAMOWANIE („BIAŁA LISTA")

(a) Zidentyfikowanie [***Realizacja: programy zdefiniowane przez organizację uprawnione do zainstalowania w systemie***]**;**

(b) Stosowanie zasady „odmawiaj wszystkiego za wyjątkiem" (*ang. "deny-all", "permit-by-exception"*), aby umożliwić wykonanie autoryzowanych programów w systemie; oraz

(c) Przeglądanie i aktualizacja listy autoryzowanych programów [***Realizacja: częstotliwość zdefiniowana przez organizację***]**.**

Omówienie: Autoryzowane programy mogą być ograniczone do określonych wersji lub określonego źródła. W celu ułatwienia kompleksowego procesu autoryzacji oprogramowania i zwiększenia siły ochrony przed atakami, które omijają autoryzowane oprogramowanie na poziomie aplikacji, programy komputerowe mogą być dzielone i monitorowane na różnych poziomach szczegółowości. Poziomy te obejmują aplikacje, interfejsy programowania aplikacji, moduły aplikacji, skrypty, procesy systemowe, usługi systemowe, funkcje jądra (kernel), rejestry, sterowniki i biblioteki linków dynamicznych. Koncepcja pozwalająca na wykonywanie autoryzowanego oprogramowania może być również stosowana w odniesieniu do działań użytkowników, portów i protokołów systemowych, adresów IP/pul adresów IP, stron internetowych i adresów MAC. Organizacje rozważają weryfikację integralności autoryzowanych programów przy użyciu podpisów cyfrowych, kryptograficznych sum kontrolnych czy funkcji „hash". Weryfikacja autoryzowanego oprogramowania może nastąpić przed jego wykonaniem lub podczas uruchamiania systemu. Identyfikacja

ujednoliconych formatów adresowania URL (*ang. Universal Resource Locator*) dla stron internetowych jest uwzględniona w zabezpieczeniach CA-3(5) i SC-7.

Zabezpieczenia powiązane: CM-2, CM-6, CM-8, CM-10, PL-9, PM-5, SA-10, SC-34, SI-7.

(6) ZASADA MINIMALNEJ FUNKCJONALNOŚCI | ZAMKNIĘTE ŚRODOWISKA Z OGRANICZONYMI UPRAWNIENIAMI

Wymaganie, aby poniższe oprogramowanie zainstalowane przez użytkownika było uruchamiane w ograniczonym fizycznym lub wirtualnym środowisku urządzenia z limitowanymi uprawnieniami: [***Realizacja: oprogramowanie zainstalowane przez użytkownika, zdefiniowane przez organizację***]**.**

Omówienie: Organizacje identyfikują oprogramowanie, które może budzić obawy, co do jego pochodzenia lub potencjalnego występowania złośliwego kodu. W przypadku tego typu oprogramowania instalacje użytkowników odbywają się w ograniczonych środowiskach pracy, aby wyeliminować lub ograniczyć uszkodzenia powodowane przez złośliwy kod, który może zostać wykonany.

Zabezpieczenia powiązane: CM-11, SC-44.

(7) ZASADA MINIMALNEJ FUNKCJONALNOŚCI | WYKONYWANIE KODU W CHRONIONYCH ŚRODOWISKACH

Zezwolenie na wykonanie kodu binarnego lub maszynowego tylko w ograniczonym fizycznym lub wirtualnym środowisku urządzenia i za jednoznacznym zatwierdzeniem [***Realizacja: personel lub role określone przez organizację***]**, gdy taki kod jest:**

(a) Uzyskany ze źródeł z ograniczonym zaufaniem lub niezaufanych; i/lub

(b) Bez podania kodu źródłowego.

Omówienie: Wykonywanie kodu w chronionych środowiskach dotyczy wszystkich źródeł kodu binarnego lub maszynowego, w tym oprogramowania komercyjnego i oprogramowania układowego oraz oprogramowania open-source.

Zabezpieczenia powiązane: CM-10, SC-44.

(8) ZASADA MINIMALNEJ FUNKCJONALNOŚCI | KOD BINARNY LUB KOD WYKONYWALNY (MOBILNY)

(a) Zakazanie używania kodu binarnego lub maszynowego ze źródeł z ograniczonym zaufaniem lub niezaufanych lub bez podania kodu źródłowego; oraz

(b) Zezwalanie na wyjątki tylko w przypadku istotnych wymogów dotyczących misji lub operacji oraz za zgodą osoby autoryzującej (*ang. authorizing offcial – AO*).

Omówienie: Binarny lub maszynowo wykonywalny kod dotyczy wszystkich źródeł kodu binarnego lub maszynowego, w tym oprogramowania komercyjnego i oprogramowania układowego oraz oprogramowania open-source. Organizacje oceniają oprogramowanie bez towarzyszącego mu kodu źródłowego lub pochodzące ze źródeł z ograniczonym zaufaniem lub niezaufanych pod względem potencjalnego wpływu na bezpieczeństwo. Oceny dotyczą faktu, że oprogramowanie bez udostępnienia kodu źródłowego może być trudne do przejrzenia, naprawy lub rozszerzenia. Ponadto, może nie być żadnych właścicieli, którzy dokonywaliby takich napraw w imieniu organizacji. Jeśli używane jest oprogramowanie open-source, oceny uwzględniają fakt, że nie jest ono zaufane, może zawierać furtki (*ang. back doors*) lub złośliwe oprogramowanie (*ang. malware*) i może nie być dostępne wsparcie.

Zabezpieczenia powiązane: SA-5, SA-22.

(9) ZASADA MINIMALNEJ FUNKCJONALNOŚCI | ZAKAZ UŻYWANIA NIEAUTORYZOWANEGO SPRZĘTU

(a) Zidentyfikowanie [***Realizacja: zdefiniowane przez organizację komponenty sprzętowe dopuszczone do eksploatacji w systemie***]**;**

(b) Zakazanie używania lub podłączania nieautoryzowanych komponentów sprzętowych;

(c) Przeglądanie i aktualizowanie listy autoryzowanych komponentów sprzętowych [***Realizacja: częstotliwość zdefiniowana przez organizację***]**.**

Omówienie: Komponenty sprzętowe stanowią podstawę dla systemów organizacyjnych oraz platformę do realizacji autoryzowanych programów. Zarządzanie inwentaryzacją komponentów sprzętowych oraz kontrolowanie, które komponenty sprzętowe mogą być instalowane lub podłączane do systemów organizacyjnych jest niezbędne w celu zapewnienia odpowiedniego bezpieczeństwa.

Zabezpieczenia powiązane: Brak.

Referencje: [FIPS 140-3], [FIPS 180-4], [FIPS 186-4], [FIPS 202], [NIST SP 800-167].

CM-8 INWENTARYZACJA KOMPONENTÓW SYSTEMU

Zabezpieczenie podstawowe:

a. Opracowanie i udokumentowanie inwentaryzacji komponentów systemu, która:

   1. Dokładnie odzwierciedla system;

   2. Zawiera wszystkie komponenty systemu;

   3. Nie obejmuje podwójnego księgowania tych samych komponentów lub komponentów przypisanych do jakiegokolwiek innego systemu;

   4. Jest na poziomie szczegółowości uznanym za niezbędny do śledzenia i raportowania; oraz

   5. Zawiera następujące informacje umożliwiające rozliczalność komponentów systemu: [*Realizacja: informacje zdefiniowane przez organizację uznane za niezbędne do osiągnięcia skutecznej rozliczalności komponentów systemu teleinformatycznego*]; oraz

b. Przeglądanie i aktualizacja spisu komponentów systemu [*Realizacja: częstotliwość określona przez organizację*].

Omówienie: Komponenty systemu są dyskretnymi, możliwymi do zidentyfikowania aktywami informatycznymi, które obejmują sprzęt, aplikacje i oprogramowanie układowe. Organizacje mogą zdecydować się na wdrożenie scentralizowanej inwentaryzacji elementów systemu, które zawierają komponenty ze wszystkich systemów organizacyjnych. W takich sytuacjach organizacje dbają o to, aby w spisach tych znajdowały się informacje specyficzne dla danego systemu, wymagane do rozliczania komponentów. Informacje niezbędne do skutecznego rozliczania składników systemu obejmują nazwę systemu, właścicieli oprogramowania, numery wersji oprogramowania, specyfikacje inwentaryzacji sprzętu, informacje o licencjach na oprogramowanie, a w przypadku składników sieciowych - nazwy maszyn i adresy sieci we wszystkich zaimplementowanych protokołach (np. IPv4, IPv6). Specyfikacje

inwentaryzacyjne zawierają datę odbioru, koszt, model, numer seryjny, producenta, informacje o dostawcy, typ komponentu i fizyczną lokalizację.

Zapobieganie podwójnemu księgowaniu tych samych komponentów systemu rozwiązuje problem braku rozliczalności, który pojawia się, gdy własność komponentów i ich skojarzenie nie jest znane, szczególnie w dużych lub złożonych, połączonych systemach. Skuteczne zapobieganie podwójnemu księgowaniu komponentów systemu wymaga użycia unikalnego identyfikatora dla każdego komponentu. W przypadku inwentaryzacji oprogramowania, centralnie zarządzane oprogramowanie, dostępne za pośrednictwem innych systemów, jest traktowane, jako część składowa systemu, na którym jest ono zainstalowane i zarządzane. Oprogramowanie zainstalowane w wielu systemach organizacyjnych i zarządzane na poziomie systemowym jest adresowane do każdego systemu i może pojawić się więcej niż raz w scentralizowanej inwentaryzacji składników, co wymaga skojarzenia systemu dla każdej instancji oprogramowania w scentralizowanej inwentaryzacji, aby uniknąć podwójnego księgowania składników. Skanowanie systemów implementujących wiele protokołów sieciowych (np. IPv4 i IPv6) może spowodować, że zduplikowane komponenty będą identyfikowane w różnych przestrzeniach adresowych. Wdrożenie zabezpieczenia CM-8(7) może pomóc w wyeliminowaniu podwójnego księgowania komponentów.

Zabezpieczenia powiązane: CM-2, CM-7, CM-9, CM-10, CM-11, CM-13, CP-2, CP-9, MA-2, MA-6, PE-20, PL- 9, PM-5, SA-4, SA-5, SI-2, SR-4.

Zabezpieczenia rozszerzone:

(1) INWENTARYZACJA KOMPONENTÓW SYSTEMU | AKTUALIZACJE INSTALACJI I USUWANIA KOMPONENTÓW

Aktualizacja spisu komponentów systemu w ramach instalacji, usuwania i aktualizacji komponentów systemu.

Omówienie: Organizacje mogą poprawić dokładność, kompletność i spójność spisu komponentów systemu, jeżeli inwentaryzacje te są aktualizowane w ramach

instalacji lub usuwania komponentów lub podczas ogólnych aktualizacji systemu. Jeśli zapasy nie są aktualizowane w tych kluczowych momentach, istnieje większe prawdopodobieństwo, że informacje te nie zostaną odpowiednio uchwycone i udokumentowane. Aktualizacje systemu obejmują komponenty sprzętowe, aplikacje i oprogramowanie układowe.

Zabezpieczenia powiązane: PM-16.

(2) INWENTARYZACJA KOMPONENTÓW SYSTEMU | AUTOMATYCZNA KONSERWACJA (UTRZYMYWANIE)

Utrzymanie aktualności, kompletności, dokładności i dostępności zapasów komponentów systemu przy użyciu [***Realizacja: organizacyjnie zdefiniowane mechanizmy automatyczne***]**.**

Omówienie: Organizacje prowadzą inwentaryzację systemów w takim zakresie, w jakim jest to wykonalne. Na przykład, maszyny wirtualne mogą być trudne do monitorowania, ponieważ nie są one widoczne w sieci, gdy nie są używane. W takich przypadkach organizacje utrzymują tak aktualny, kompletny i dokładny spis komponentów, jak uznają to za uzasadnione. Zautomatyzowane utrzymanie może być osiągnięte poprzez wdrożenie przez organizację zabezpieczenia CM-2(2), które łączy inwentaryzację komponentów systemu z działaniami związanymi z konfiguracją bazową.

Zabezpieczenia powiązane: Brak.

(3) INWENTARYZACJA KOMPONENTÓW SYSTEMU | AUTOMATYCZNE WYKRYWANIE KOMPONENTÓW NIEAUTORYZOWANYCH

(a) Wykrywanie obecności nieautoryzowanego sprzętu, aplikacji i oprogramowania układowego w systemie przy użyciu [***Realizacja: mechanizmy automatyczne zdefiniowane przez organizację***] [***Realizacja: częstotliwość zdefiniowana przez organizację***]**; oraz**

(b) W przypadku wykrycia nieautoryzowanych komponentów podjęcie następujących działań: *Wybór (jeden lub więcej): wyłączenie dostępu do sieci przez takie komponenty; odizolowanie komponentów; powiadomienie* [*Realizacja: personel lub role zdefiniowane przez organizację*]].

Omówienie: Oprócz monitorowania nieautoryzowanych połączeń zdalnych i urządzeń przenośnych, stosowane jest automatyczne wykrywanie nieautoryzowanych komponentów. Monitorowanie nieautoryzowanych elementów systemu może być realizowane na bieżąco lub poprzez okresowe skanowanie systemów. Zautomatyzowane mechanizmy mogą być również stosowane do zapobiegania podłączaniu nieautoryzowanych komponentów (patrz zabezpieczenie CM-7(9)). Mechanizmy zautomatyzowane mogą być zaimplementowane w systemach lub w oddzielnych komponentach systemu. Podczas nabywania i wdrażania mechanizmów automatycznego wykrywania organizacje rozważają, czy mechanizmy te są uzależnione od zdolności komponentu systemu do obsługi agenta lub suplikanta, ponieważ niektóre rodzaje komponentów nie mają lub nie mogą obsługiwać agentów (np. urządzenia IoT, czujniki). Izolację można osiągnąć na przykład poprzez umieszczenie nieautoryzowanych komponentów systemu w oddzielnych domenach lub podsieciach lub poddanie takich komponentów kwarantannie. Ten rodzaj izolacji elementów (środowisko izolowane) jest powszechnie określany, jako "piaskownica" (*ang. sandboxing*).

Zabezpieczenia powiązane: AC-19, CA-7, RA-5, SC-3, SC-39, SC-44, SI-3, SI-7.

(4) INWENTARYZACJA KOMPONENTÓW SYSTEMU | INFORMACJE DOTYCZĄCE ODPOWIEDZIALNOŚCI I ROZLICZALNOŚCI

Włączenie do spisu komponentów informacji o sposobie identyfikacji *osób* odpowiedzialnych za administrowanie tymi składnikami [***Wybór (jeden lub więcej): imię i nazwisko; stanowisko; rola***]**.**

Omówienie: Identyfikacja osób odpowiedzialnych za administrowanie komponentami systemu zapewnia, że przydzielone komponenty są właściwie administrowane oraz organizacje mogą skontaktować się z tymi osobami, jeśli wymagane są jakieś działania (np. gdy komponent jest określony, jako źródło naruszenia wymaga wycofania lub wymiany, lub musi zostać przeniesiony).

Zabezpieczenia powiązane: AC-3.

(5) INWENTARYZACJA KOMPONENTÓW SYSTEMU | BRAK DUPLIKACJI KOMPONENTÓW

[Wycofane: Włączone do CM-8].

(6) INWENTARYZACJA KOMPONENTÓW SYSTEMU | OCENA KONFIGURACJI I ZATWIERDZONE ODSTĘPSTWA

Uwzględnienie w spisie komponentów systemu konfiguracji ocenianych komponentów oraz wszelkich zatwierdzonych odstępstw od aktualnie stosowanych konfiguracji.

Omówienie: Ocenione konfiguracje i zatwierdzone odchylenia koncentrują się na ustawieniach konfiguracyjnych ustanowionych przez organizacje dla komponentów systemu, konkretnych komponentach, które zostały ocenione w celu określenia zgodności z wymaganymi ustawieniami konfiguracyjnymi oraz wszelkich zatwierdzonych odchyleniach od ustalonych ustawień konfiguracyjnych.

Zabezpieczenia powiązane: Brak.

(7) INWENTARYZACJA KOMPONENTÓW SYSTEMU | SCENTRALIZOWANE REPOZYTORIUM

Zapewnienie scentralizowanego repozytorium spisu komponentów systemu.

Omówienie: Organizacje mogą stosować scentralizowane spisy komponentów systemu, które zawierają komponenty wszystkich systemów organizacyjnych. Scentralizowane repozytoria inwentaryzacyjne zapewniają możliwość

efektywnego rozliczania zasobów sprzętu, aplikacji i oprogramowania układowego organizacji. Takie repozytoria mogą również pomóc organizacjom w szybkiej identyfikacji lokalizacji komponentów i osób odpowiedzialnych za komponenty, które zostały narażone na szwank, naruszone lub w inny sposób wymagają zastosowania działań łagodzących. Organizacje zapewniają, że powstałe w ten sposób scentralizowane spisy zawierają informacje specyficzne dla danego systemu, niezbędne do właściwego rozliczania komponentów.

Zabezpieczenia powiązane: Brak.

(8) INWENTARYZACJA KOMPONENTÓW SYSTEMU | AUTOMATYCZNE ŚLEDZENIE LOKALIZACJI

Wsparcie śledzenia komponentów systemu według lokalizacji geograficznej za pomocą [***Realizacja: mechanizmy automatyczne zdefiniowane przez organizację***]**.**

Omówienie: Wykorzystanie automatycznych mechanizmów do śledzenia lokalizacji elementów systemu może zwiększyć dokładność inwentaryzacji komponentów. Taka zdolność może pomóc organizacjom w szybkiej identyfikacji lokalizacji komponentów i osób odpowiedzialnych za elementy systemu, które zostały narażone na szwank, naruszone lub w inny sposób wymagają podjęcia działań łagodzących. Korzystanie z mechanizmów śledzenia można skoordynować z SAOP[44], jeśli istnieją implikacje, które mają wpływ na prywatność poszczególnych osób.

Zabezpieczenia powiązane: Brak.

(9) INWENTARYZACJA KOMPONENTÓW SYSTEMU | PRZYPISANIE KOMPONENTÓW DO SYSTEMÓW

[44] Patrz: NSC 800-37; NSC 7298.

(a) Przypisanie posiadanych komponentów do systemu; oraz

(b) Otrzymanie od [***Realizacja: personel lub role określone przez organizację***] **potwierdzeń wykonania tego zadania.**

Omówienie: Komponenty systemu, które nie są przypisane do systemu, mogą być niezarządzane, pozbawione wymaganej ochrony i stać się podatnością organizacji.

Zabezpieczenia powiązane: Brak.

Referencje: [OMB A-130], [NIST SP 800-57-1], [NIST SP 800-57-2], [NIST SP 800-57-3], [NIST SP 800-128], [IR 8011-2], [IR 8011-3].

CM-9 PLAN ZARZĄDZANIA KONFIGURACJĄ

Zabezpieczenie podstawowe: Opracowanie, udokumentowanie i wdrożenie planu zarządzania konfiguracją systemu, który:

a. Adresuje role, obowiązki oraz procesy i procedury zarządzania konfiguracją;

b. Ustanawia proces identyfikacji elementów konfiguracji w całym cyklu życia systemu oraz zarządzania konfiguracją elementów konfiguracji;

c. Określa elementy konfiguracyjne systemu i włącza je do zarządzania konfiguracją;

d. Jest weryfikowany i zatwierdzany przez [*Realizacja: personel lub role określone przez organizację*]*;* oraz

e. Jest chroniony przed nieautoryzowanym ujawnieniem i modyfikacją.

Omówienie: Działania związane z zarządzaniem konfiguracją występują w całym cyklu życia systemu. W związku z tym istnieją działania związane z zarządzaniem konfiguracją rozwojową (np. zabezpieczenie nad bibliotekami kodu i oprogramowania) oraz działania związane z zarządzaniem konfiguracją operacyjną (np. zabezpieczenie zainstalowanych komponentów i sposobu ich konfiguracji). Plany zarządzania konfiguracją spełniają wymagania polityki zarządzania konfiguracją, a jednocześnie są dostosowane do poszczególnych systemów. Plany zarządzania konfiguracją definiują procesy i procedury, w jaki sposób zarządzanie konfiguracją jest wykorzystywane do wspierania działań związanych z cyklem życia systemu. Plany zarządzania konfiguracją są generowane na etapie rozwoju i nabywania w cyklu życia systemu. Plany te opisują sposób wprowadzania zmian w procesach zarządzania zmianami, aktualizowania ustawień konfiguracyjnych i bazowych, utrzymywania zapasów komponentów, kontrolowania środowiska programistycznego, testowego i operacyjnego oraz opracowywania, wydawania i aktualizowania kluczowych dokumentów.

Organizacje mogą korzystać z szablonów, aby zapewnić spójne i terminowe opracowywanie i wdrażanie planów zarządzania konfiguracją. Szablony mogą

przedstawiać plan zarządzania konfiguracją w organizacji z podzbiorami planu wdrożonymi na zasadzie system po systemie. Procesy zatwierdzania zarządzania konfiguracją obejmują wyznaczenie kluczowych interesariuszy odpowiedzialnych za przegląd i zatwierdzenie proponowanych zmian w systemach oraz personel, który przed wdrożeniem zmian w systemach przeprowadza analizy wpływu na bezpieczeństwo i prywatność. Elementy konfiguracyjne to komponenty systemu, takie jak sprzęt, aplikacje, oprogramowanie układowe oraz dokumentacja do zarządzania konfiguracją. W miarę jak systemy przechodzą przez cykl życia systemu, mogą być identyfikowane nowe pozycje konfiguracyjne, a niektóre istniejące pozycje konfiguracyjne mogą już nie wymagać kontroli konfiguracji.

Zabezpieczenia powiązane: CM-2, CM-3, CM-4, CM-5, CM-8, PL-2, RA-8, SA-10, SI-12.

Zabezpieczenia rozszerzone:

(1) PLAN ZARZĄDZANIA KONFIGURACJĄ | PRZYPISANIE ODPOWIEDZIALNOŚCI

Powierzenie odpowiedzialności za rozwój procesu zarządzania konfiguracją personelowi organizacyjnemu, który nie jest bezpośrednio zaangażowany w rozwój systemu.

Omówienie: W przypadku braku dedykowanych zespołów zarządzania konfiguracją utworzonych w ramach organizacji, deweloperzy systemów mogą otrzymać zadanie opracowania procesów zarządzania konfiguracją z wykorzystaniem personelu, który nie jest bezpośrednio zaangażowany w rozwój systemu lub integrację systemu. Taki podział obowiązków zapewnia, że organizacje ustanawiają i utrzymują wystarczający stopień niezależności pomiędzy procesami rozwoju i integracji systemu, a procesami zarządzania konfiguracją w celu ułatwienia kontroli jakości i bardziej efektywnego nadzoru.

Zabezpieczenia powiązane: Brak.

Referencje: [NIST SP 800-128].

CM-10 OGRANICZENIA W UŻYCIU OPROGRAMOWANIA

Zabezpieczenie podstawowe:

a. Korzystanie z oprogramowania i związanej z nim dokumentacji zgodnie z postanowieniami umownymi prawami autorskimi;

b. Śledzenie korzystania z oprogramowania i związanej z nim dokumentacji chronionej licencjami ilościowymi w celu kontroli kopiowania i dystrybucji; oraz

c. Kontrolowanie i dokumentowanie korzystania z technologii wymiany plików w systemie „peer-to-peer" w celu zapewnienia, że funkcja ta nie jest wykorzystywana do nieautoryzowanego rozpowszechniania, wyświetlania, wykonywania lub reprodukcji utworów chronionych prawem autorskim.

Omówienie: Śledzenie licencji oprogramowania może być realizowane metodami ręcznymi lub automatycznymi, w zależności od potrzeb organizacyjnych. Przykładami umów są umowy licencyjne na oprogramowanie (*ang. software license agreements*) oraz umowy o nieujawnianiu informacji (*ang. non-disclosure agreements - NDA*).

Zabezpieczenia powiązane: AC-17, AU-6, CM-7, CM-8, PM-30, SC-7.

Zabezpieczenia rozszerzone:

(1) OGRANICZENIA W UŻYCIU OPROGRAMOWANIA | OPROGRAMOWANIE OTWARTE (OPEN-SOURCE)

Ustanowienie następujących ograniczeń w korzystaniu z oprogramowania otwartego (typu „open-source"): [***Realizacja: ograniczenia zdefiniowane przez organizację***]**.**

Omówienie: Oprogramowanie „open-source" odnosi się do oprogramowania, które jest dostępne w formie kodu źródłowego. Niektóre prawa do oprogramowania, zwykle zastrzeżone dla właścicieli praw autorskich, są rutynowo dostarczane w ramach umów licencyjnych na oprogramowanie, które pozwalają osobom na studiowanie, zmienianie i ulepszanie oprogramowania. Z punktu widzenia bezpieczeństwa, główną zaletą oprogramowania „open-

source" jest to, że daje ono organizacjom możliwość badania kodu źródłowego. W niektórych obszarach istnieje społeczność online związana z oprogramowaniem, która na bieżąco kontroluje, testuje, aktualizuje i zgłasza problemy wykryte w oprogramowaniu. Jednak naprawianie luk w oprogramowaniu „open-source" może być problematyczne.
Z oprogramowaniem „open-source" mogą również wiązać się problemy licencyjne, w tym ograniczenia dotyczące używania takiego oprogramowania w celach pochodnych. Oprogramowanie „open-source", które jest dostępne tylko w formie binarnej, może zwiększać poziom ryzyka związanego z użytkowaniem takiego oprogramowania.

Zabezpieczenia powiązane: SI-7.

Referencje: Brak.

CM-11 OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA

Zabezpieczenie podstawowe:

a. Ustanowienie [*Realizacja: zasady zdefiniowane przez organizację*] regulujących instalację oprogramowania przez użytkowników;

b. Egzekwowanie polityki instalacji oprogramowania za pomocą następujących metod: [*Realizacja: metody zdefiniowane przez organizację*]*;* oraz

c. Monitorowanie zgodności polityki z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Omówienie: Jeżeli użytkownik posiada niezbędne uprawnienia, może zainstalować oprogramowanie w systemach organizacyjnych. W celu zapewnienia kontroli nad zainstalowanym oprogramowaniem, organizacje identyfikują dozwolone i zabronione działania dotyczące instalacji oprogramowania. Dozwolone instalacje oprogramowania obejmują aktualizacje i łatki zabezpieczające istniejącego oprogramowania oraz pobieranie nowych aplikacji z zatwierdzonych przez organizację "sklepów z aplikacjami" (*ang. „app stores”).* Zabronione instalacje oprogramowania obejmują oprogramowanie o nieznanym lub podejrzanym pochodzeniu lub oprogramowanie, które organizacje uznają za potencjalnie szkodliwe. Zasady wybrane do zarządzania oprogramowaniem zainstalowanym przez użytkownika są opracowywane przez organizację lub dostarczane przez podmiot zewnętrzny. Metody egzekwowania zasad mogą obejmować metody proceduralne i metody zautomatyzowane.

Zabezpieczenia powiązane: AC-3, AU-6, CM-2, CM-3, CM-5, CM-6, CM-7, CM-8, PL-4, SI-4, SI-7.

Zabezpieczenia rozszerzone:

(1) OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA | OSTRZEGANIE O NIEAUTORYZOWANYCH INSTALACJACH

[Wycofane: Włączone do CM-8(3)]

(2) OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA | ZABRONIONA INSTALACJA BEZ POSIADANIA STOSOWNYCH UPRAWNIEŃ

Zezwolenie na instalację oprogramowania tylko przez użytkownika z jednoznacznie określonym statusem uprzywilejowania.

Omówienie: Uprzywilejowany status można uzyskać na przykład poprzez pełnienie funkcji administratora systemu.

Zabezpieczenia powiązane: AC-5, AC-6.

(3) OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA | AUTOMATYCZNE EGZEKWOWANIE I MONITOROWANIE

Egzekwowanie i monitorowanie zgodności z zasadami instalacji oprogramowania za pomocą [***Realizacja: mechanizmy automatyczne zdefiniowane przez organizację***]**.**

Omówienie: Organizacje egzekwują i monitorują zgodność z zasadami instalacji oprogramowania za pomocą automatycznych mechanizmów, pozwalających na szybsze wykrywanie i reagowanie na nieautoryzowaną instalację oprogramowania, która może być wskaźnikiem wewnętrznego lub zewnętrznego wrogiego ataku.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

CM-12 POŁOŻENIE (LOKACJA) INFORMACJI

Zabezpieczenie podstawowe:

a. Określenie i udokumentowanie lokalizacji [*Realizacja: informacje określone przez organizację*] oraz określone składniki systemu, na których informacje są przetwarzane i przechowywane;

b. Określenie i udokumentowanie użytkowników, którzy mają dostęp do systemu i komponentów systemu, w których informacje są przetwarzane; oraz

c. Dokumentowanie zmiany lokalizacji (tj. systemu lub komponentów systemu), w których informacje są przetwarzane.

Omówienie: Lokalizacja informacji służy określeniu miejsca przetwarzania informacji. Lokalizacja informacji pozwala określić, gdzie w komponentach systemu znajdują się określone rodzaje informacji oraz w jaki sposób informacje są przetwarzane, tak, aby można było ustalić przepływ informacji oraz zapewnić odpowiednią ochronę i zarządzanie polityką w odniesieniu do tych informacji oraz komponentów systemu. Kategoria bezpieczeństwa informacji jest także czynnikiem decydującym o zabezpieczeniach niezbędnych do ochrony informacji i komponentów systemu, w którym informacje się znajdują (zob. NSC 199). Lokalizacja informacji i komponentów systemu jest również czynnikiem wpływającym na architekturę i projekt systemu (patrz SA-4, SA-8, SA-17).

Zabezpieczenia powiązane: AC-2, AC-3, AC-4, AC-6, AC-23, CM-8, PM-5, RA-2, SA-4, SA-8, SA-17, SC-4, SC- 16, SC-28, SI-4, SI-7.

Zabezpieczenia rozszerzone:

(1) POŁOŻENIE (LOKACJA) INFORMACJI | AUTOMATYCZNE NARZĘDZIA DO OBSŁUGI LOKACJI INFORMACJI

Używanie zautomatyzowanych narzędzi do identyfikacji [Realizacja: *informacje określone przez organizację według typu informacji*] przetwarzanych w [*Realizacja: komponenty systemu określone przez organizację*] *w* celu

upewnienia się, że stosowane są zabezpieczenia informacji organizacyjnych i ochrony prywatności osób.

Omówienie: Wykorzystanie zautomatyzowanych narzędzi pomaga zwiększyć efektywność i skuteczność wdrożonych w systemie możliwości lokalizowania informacji. Automatyzacja pomaga również organizacjom w zarządzaniu danymi powstającymi podczas działań związanych z lokalizacją informacji oraz w dzieleniu się takimi informacjami w całej organizacji. Dane wyjściowe z narzędzi do automatycznej lokalizacji informacji mogą być wykorzystywane do prowadzenia i informowania o architekturze systemu oraz podejmowania decyzji projektowych.

Zabezpieczenia powiązane: Brak.

Referencje: [FIPS 199], [NIST SP 800-60-1], [NIST SP 800-60-2].

CM-13 MAPOWANIE DZIAŁAŃ NA DANYCH

Zabezpieczenie podstawowe: Opracowanie i udokumentowanie mapy działań dotyczących danych systemowych.

Omówienie: Działania związane z danymi to operacje systemowe, które przetwarzają dane osobowe. Przetwarzanie takich informacji obejmuje pełny cykl życia informacji, który obejmuje ich gromadzenie, generowanie, przekształcanie, wykorzystywanie, ujawnianie, zatrzymywanie i usuwanie. Mapa działań dotyczących danych systemowych obejmuje działania dotyczące danych dyskretnych, przetwarzanych danych osobowych umożliwiających identyfikację osób, komponentów systemu zaangażowanych w działania dotyczące danych oraz właścicieli lub administratorów komponentów systemu. Zrozumienie, jakie dane osobowe są przetwarzane (np. wrażliwość danych osobowych), w jaki sposób przetwarzane są dane osobowe (np. czy dane są widoczne przez osoby lub przetwarzane w innej części systemu) oraz przez kogo (np. osoby mogą mieć różne sposoby postrzegania prywatności w zależności od podmiotu przetwarzającego dane osobowe) dostarcza wielu czynników kontekstowych, które są ważne dla oceny stopnia zagrożenia prywatności stworzonego przez system. Mapy danych mogą być ilustrowane na różne sposoby, a poziom szczegółowości może się różnić w zależności od misji i potrzeb biznesowych organizacji. Mapa danych może być nakładką na dowolny artefakt projektu systemu, który organizacja wykorzystuje. Opracowanie tej mapy może wymagać koordynacji między programami ochrony prywatności i bezpieczeństwa w zakresie działań obejmujących dane i komponenty, które są identyfikowane, jako część systemu.

Zabezpieczenia powiązane: AC-3, CM-4, CM-12, PM-5, PM-27, PT-2, PT-3, RA-3, RA-8.

CM-14 PODPISYWANIE KOMPONENTÓW

Zabezpieczenie podstawowe: Zapobieganie instalacji [*Realizacja: zdefiniowane przez organizację komponenty aplikacji i oprogramowania układowego*] bez weryfikacji, czy komponent został podpisany cyfrowo za pomocą certyfikatu, który jest uznawany i zatwierdzony przez organizację.

Omówienie: Składniki aplikacji i oprogramowania układowego, które nie mogą być instalowane, jeśli nie zostały podpisane uznanymi i zatwierdzonymi certyfikatami, obejmują aktualizacje wersji aplikacji i oprogramowania układowego, poprawki, dodatki Service Pack, sterowniki urządzeń oraz podstawowe aktualizacje systemu wejścia/wyjścia. Organizacje mogą zidentyfikować odpowiednie składniki aplikacji i oprogramowania układowego według typu, konkretnych elementów lub kombinacji obu tych elementów. Podpisy cyfrowe i organizacyjna weryfikacja tych podpisów jest metodą uwierzytelniania kodu.

Zabezpieczenia powiązane: CM-7, SC-12, SC-13, SI-7.

KATEGORIA CP - PLANOWANIE AWARYJNE / CIĄGŁOŚĆ DZIAŁANIA

CP-1 POLITYKA I PROCEDURY

Zabezpieczenie podstawowe:

a. Opracowywanie, dokumentowanie i rozpowszechnianie wśród [*Realizacja: personel lub role określone przez organizację*]*:*

   1. [*Wybór (jeden lub więcej): poziom organizacji; poziom misji/procesu biznesowego; poziom systemu*] polityki planowania awaryjnego, która:

      (a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami; oraz

      (b) Jest zgodna z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi; oraz

   2. Procedur ułatwiających wdrożenie polityki planowania awaryjnego oraz powiązanych zabezpieczeń w zakresie planowania awaryjnego;

b. Wyznaczanie [*Realizacja: osoba wyznaczona przez organizację*] do zarządzania przygotowaniem, opracowaniem oraz rozpowszechnianiem polityki i procedur planowania awaryjnego; oraz

c. Przeglądanie i aktualizacja bieżącej:

   1. Polityki planowania awaryjnego z [Realizacja: *częstotliwość określona przez organizację*] i następujących [*Realizacja: zdarzenia określone przez organizację*]; oraz

   2. Procedur planowania awaryjnego z [Realizacja: *częstotliwość określona przez organizację*] i następujących [*Realizacja: zdarzenia określone przez organizację*].

Omówienie: Polityka i procedury w zakresie planowania awaryjnego dotyczą zabezpieczeń w kategorii *Planowanie awaryjne* (CP), które są wdrażane w ramach

systemów i organizacji. Strategia zarządzania ryzykiem jest ważnym czynnikiem przy tworzeniu takich polityk i procedur. Polityki i procedury przyczyniają się do zapewnienia bezpieczeństwa i ochrony prywatności. Dlatego ważne jest, aby programy bezpieczeństwa i ochrony prywatności były opracowywane wspólnie przy kształtowaniu polityki i procedur planowania awaryjnego. Polityki i procedury dotyczące programów bezpieczeństwa i ochrony prywatności na poziomie organizacji są ogólnie rzecz biorąc preferowane i mogą eliminować potrzeby tworzenia polityk i procedur specyficznych dla danej misji lub systemu. Polityka może być włączona, jako część ogólnej polityki bezpieczeństwa i ochrony prywatności lub reprezentowana przez wiele polityk odzwierciedlających złożony charakter organizacji. Procedury mogą być ustanowione dla programów bezpieczeństwa i ochrony prywatności, dla misji lub procesów biznesowych oraz dla systemów, jeśli to konieczne. Procedury opisują sposób wdrażania zasad lub zabezpieczeń i mogą być skierowane do osoby lub roli, która jest przedmiotem procedury. Procedury mogą być udokumentowane w planach bezpieczeństwa i ochrony prywatności systemu w jednym lub kilku oddzielnych dokumentach.

Zdarzenia, które mogą spowodować konieczność aktualizacji polityki i procedur planowania awaryjnego, obejmują wyniki oceny lub audytu, incydenty lub naruszenia bezpieczeństwa, lub zmiany w przepisach prawa, zarządzeniach, dyrektywach, rozporządzeniach, zasadach, standardach i wytycznych.

Oświadczenie o wprowadzeniu zabezpieczeń nie jest równoznaczne z ustanowieniem polityki lub procedury organizacyjnej.

Zabezpieczenia powiązane: PM-9, PS-8, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [NIST SP 800-12], [NIST SP 800-30], [NIST SP 800-34], [NIST SP 800-39], [NIST SP 800-50], [NIST SP 800-100].

CP-2 PLAN CIĄGŁOŚCI DZIAŁANIA

Zabezpieczenie podstawowe:

a. Opracowanie planu awaryjnego dla systemu, który:

   1. Identyfikuje istotne misje i funkcje biznesowe oraz związane z nimi wymagania awaryjne;
   2. Przedstawia cele odzyskiwania, priorytety przywracania i metryki odbudowy;
   3. Adresuje role i obowiązki w sytuacjach awaryjnych, przypisuje osoby z danymi kontaktowymi;
   4. Określa podstawowe funkcje biznesowe i misyjne utrzymywane pomimo zakłócenia pracy systemu, incydentu lub awarii;
   5. Wskazuje środki prowadzące do końcowego pełnego przywrócenia systemu bez pogorszenia pierwotnie zaplanowanych i wdrożonych zabezpieczeń;
   6. Uwzględnienia wymianę informacji dotyczących sytuacji kryzysowych; oraz
   7. Jest weryfikowany i zatwierdzany przez [*Realizacja: personel lub role określone przez organizację*];

b. Przekazywanie kopii planu awaryjnego do [*Realizacja: określony przez organizację kluczowy personel do działań awaryjnych (identyfikowany na podstawie nazwiska i/lub roli) oraz elementy organizacyjne*];

c. Koordynowanie działań w zakresie planowania awaryjnego z działaniami związanymi z obsługą incydentów;

d. Przeglądanie planu awaryjnego systemu [*Realizacja: częstotliwość określona przez organizację*];

e. Aktualizowanie planu awaryjnego w celu uwzględnienia zmian w organizacji, systemie lub środowisku działania oraz problemów napotkanych podczas wdrażania, wykonywania lub testowania planu awaryjnego;

f. Przekazywanie zmian w planie awaryjnym do [*Realizacja: zdefiniowany przez organizację kluczowy personel do działań awaryjnych (identyfikowany na podstawie nazwiska i/lub roli) oraz elementy organizacyjne*];

g. Włączanie do testów i szkoleń awaryjnych doświadczenia zdobytego podczas testowania planu awaryjnego, szkolenia lub rzeczywistych działań awaryjnych; oraz

h. Ochrona planu awaryjnego przed nieautoryzowanym ujawnieniem i modyfikacją.

Omówienie: Planowanie awaryjne / ciągłość działania systemów jest częścią ogólnego programu osiągania ciągłości działania misji organizacji i funkcji biznesowych. Planowanie awaryjne / ciągłość działania dotyczy przywracania systemów i wdrażania alternatywnych misji lub procesów biznesowych, gdy systemy są zagrożone lub naruszone. Planowanie awaryjne / ciągłość działania jest brane pod uwagę w całym cyklu życia systemu i stanowi zasadniczą część projektowania systemu. Systemy mogą być projektowane pod kątem redundancji, zapewnienia możliwości tworzenia kopii zapasowych i odporności. Plany awaryjne odzwierciedlają stopień odtworzenia wymagany dla systemów organizacyjnych, ponieważ nie wszystkie systemy muszą być w pełni odtworzone, aby osiągnąć pożądany poziom ciągłości działania. Cele w zakresie przywracania systemów odzwierciedlają obowiązujące przepisy prawa, rozporządzenia, dyrektywy, regulacje, zasady, normy, wytyczne, tolerancję na ryzyko organizacyjne oraz poziom wpływu systemu.

Działania uwzględnione w planach awaryjnych obejmują kontrolowaną degradację systemu, wyłączenie systemu, powrót do trybu ręcznego, naprzemienny przepływ informacji oraz pracę w trybach zalecanych w przypadku ataku na system. Koordynując planowanie awaryjne / ciągłość działania z czynnościami związanymi z obsługą incydentów, organizacje zapewniają, że niezbędne działania planistyczne są realizowane i aktywowane w przypadku wystąpienia incydentu. Organizacje rozważają, czy ciągłość operacji podczas incydentu nie koliduje z możliwością automatycznego wyłączenia systemu, jak określono w zabezpieczeniu IR-4(5).

Planowanie reagowania na incydenty jest częścią planowania awaryjnego organizacji i jest uwzględnione w kategorii *Reagowanie na incydenty* (IR).

Zabezpieczenia powiązane: CP-3, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13, IR-4, IR-6, IR-8, IR-9, MA-6, MP-2, MP-4, MP-5, PL-2, PM-8, PM-11, SA-15, SA-20, SC-7, SC-23, SI-12.

Zabezpieczenia rozszerzone:

(1) PLAN CIĄGŁOŚCI DZIAŁANIA | KOORDYNACJA Z POWIĄZANYMI PLANAMI

Koordynacja opracowywania planów awaryjnych z elementami organizacyjnymi odpowiedzialnymi za powiązane plany.

Omówienie: Plany powiązane z planami awaryjnymi obejmują plany ciągłości działania, plany odtworzenia po katastrofie, plany dotyczące infrastruktury krytycznej, plany kontynuacji operacji, plany komunikacji kryzysowej, plany przeciwdziałania wewnętrznym zagrożeniom, plany reagowania na przypadki naruszenia danych, plany odpowiedzi na cyberincydenty, plany reagowania na przypadki naruszenia i plany ewakuacyjne.

Zabezpieczenia powiązane: Brak.

(2) PLAN CIĄGŁOŚCI DZIAŁANIA | PLANOWANIE ZDOLNOŚCI FUNKCJONOWANIA

Prowadzenie planowania zdolności funkcjonowania tak, aby podczas stanów awaryjnych istniała niezbędna zdolność do przetwarzania informacji, telekomunikacji i wsparcia środowiskowego.

Omówienie: Planowanie zdolności funkcjonowania jest wymagane, ponieważ różne zagrożenia mogą spowodować ograniczenie dostępnych usług w zakresie przetwarzania, telekomunikacji i wsparcia, mających na celu wspieranie podstawowych misji i funkcji biznesowych. Organizacje przewidują, że podczas operacji awaryjnych będą działać w trybie obniżonej wydajności i uwzględniają to w planowaniu zdolności funkcjonowania. W przypadku planowania zdolności funkcjonowania, wsparcie środowiskowe odnosi się do każdego czynnika

środowiskowego, wobec którego organizacja postanawia, że musi zapewnić wsparcie w sytuacji awaryjnej, nawet, jeśli jest on w stanie obniżonej wydajności. Ustalenia takie opierają się na ocenie ryzyka organizacji, kategoryzacji systemu (poziomu wpływu) oraz tolerancji ryzyka organizacji.

Zabezpieczenia powiązane: PE-11, PE-12, PE-13, PE-14, PE-18, SC-5.

(3) PLAN CIĄGŁOŚCI DZIAŁANIA | WZNAWIANIE PODSTAWOWYCH DZIAŁAŃ I FUNKCJI BIZNESOWYCH

Planowanie wznowienia [***Wybór: wszystkie; zasadnicze***] **funkcje misyjne i biznesowe w ciągu** [***Realizacja: określony przez organizację okres***] **od momentu aktywacji planu awaryjnego.**

Omówienie: Organizacje mogą przeprowadzić działania wynikające z planowania awaryjnego w celu wznowienia misji i funkcji biznesowych, jako część planowania ciągłości działania lub jako część analizy wpływu na działalność. Organizacje ustalają priorytety wznowienia misji i funkcji biznesowych. Czas wznowienia misji i funkcji biznesowych może być uzależniony od skali i zakresu zakłóceń w systemie i jego infrastrukturze wspierającej.

Zabezpieczenia powiązane: Brak.

(4) PLAN CIĄGŁOŚCI DZIAŁANIA | PRZYWRÓCENIE DZIAŁANIA WSZYSTKICH FUNKCJI BIZNESOWYCH

[Wycofane: Włączone do CP-2(3)]

(5) PLAN CIĄGŁOŚCI DZIAŁANIA | KONTYNUACJA NIEZBĘDNYCH DZIAŁAŃ I FUNKCJI BIZNESOWYCH

Planowanie kontynuacji [***Wybór: wszystkie; zasadnicze***] **funkcji misyjnych i biznesowych z minimalną ciągłością operacyjną lub bez jej utraty i utrzymywanie tej ciągłości aż do pełnego przywrócenia pierwotnego działania systemu w miejscach pierwotnego przetwarzania i/lub składowania.**

Omówienie: Organizacje mogą zdecydować się na przeprowadzenie działań z zakresu planowania awaryjnego w celu kontynuowania misji i funkcji biznesowych w ramach planowania ciągłości działania lub analiz wpływu na działalność. Podstawowe miejsca przetwarzania i/lub składowania zdefiniowane przez organizacje w ramach planowania awaryjnego mogą ulec zmianie w zależności od okoliczności związanych z awarią.

Zabezpieczenia powiązane: Brak.

(6) PLAN CIĄGŁOŚCI DZIAŁANIA | PROCESY ALTERNATYWNE / ZAPASOWE MIEJSCA PRZETWARZANIA

Planowanie przeniesienia [***Wybór: wszystkie; zasadnicze***] **funkcji misyjnych i biznesowych do alternatywnych miejsc przetwarzania i/lub składowania z minimalną ciągłością operacyjną lub bez jej utraty i utrzymywanie tej ciągłości aż do pełnego przywrócenia pierwotnego działania systemu w miejscach pierwotnego przetwarzania i/lub składowania.**

Omówienie: Organizacje mogą zdecydować się na wykonywanie działań planowania awaryjnego w celu kontynuowania misji i funkcji biznesowych w ramach planowania ciągłości działania lub analiz wpływu na działalność. Podstawowe miejsca przetwarzania i/lub przechowywania zdefiniowane przez organizacje w ramach planowania awaryjnego mogą ulec zmianie w zależności od okoliczności związanych z sytuacją awaryjną.

Zabezpieczenia powiązane: Brak.

(7) PLAN CIĄGŁOŚCI DZIAŁANIA | KOORDYNACJA Z USŁUGODAWCAMI ZEWNĘTRZNYMI

Koordynowanie planu awaryjnego z planami awaryjnymi zewnętrznych dostawców usług w celu zapewnienia spełnienia wymagań ciągłości działania.

Omówienie: W sytuacji uzależnienia zdolności organizacji do realizacji jej misji i funkcji biznesowych od zewnętrznych dostawców usług, opracowanie

kompleksowego i aktualnego planu awaryjnego może stać się większym wyzwaniem. Jeżeli misje i funkcje biznesowe organizacji są zależne od zewnętrznych dostawców usług, organizacje koordynują działania związane z planowaniem awaryjnym z podmiotami zewnętrznymi, aby zapewnić, że poszczególne plany odzwierciedlają całościowe potrzeby organizacji w sytuacjach awaryjnych.

Zabezpieczenia powiązane: SA-9.

(8) PLAN CIĄGŁOŚCI DZIAŁANIA | IDENTYFIKACJA ZASOBÓW KRYTYCZNYCH

Identyfikacja krytycznych zasobów systemowych wspierających [***Wybór: wszystkie; istotne***] **misje i funkcje biznesowe.**

Omówienie: Organizacje mogą zdecydować się na identyfikację krytycznych aktywów w ramach analizy krytyczności, planowania ciągłości działania lub analizy wpływu na działalność. Organizacje identyfikują krytyczne zasoby systemowe w celu zastosowania dodatkowych zabezpieczeń (poza rutynowo wdrażanymi środkami bezpieczeństwa), które pomogą zapewnić kontynuację misji i funkcji biznesowych organizacji podczas operacji awaryjnych. Identyfikacja krytycznych zasobów informatycznych ułatwia również ustalenie priorytetów w zakresie zasobów organizacyjnych. Krytyczne zasoby systemu obejmują aspekty techniczne i operacyjne. Aspekty techniczne obejmują komponenty systemu, usługi, produkty i mechanizmy informatyczne. Aspekty operacyjne obejmują procedury (tj. operacje wykonywane ręcznie) i personel (tj. osoby obsługujące zabezpieczenia techniczne i/lub wykonujące procedury ręczne). Plany organizacyjnego programu ochrony mogą pomóc w identyfikacji krytycznych zasobów. Jeżeli aktywa krytyczne są zlokalizowane w organizacji lub obsługiwane przez zewnętrznych dostawców usług, organizacje rozważają wdrożenie zabezpieczenia rozszerzonego CP-2(7).

Zabezpieczenia powiązane: CM-8, RA-9.

Referencje: [NIST SP 800-34], [IR 8179].

CP-3 SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA

Zabezpieczenie podstawowe:

a. Zapewnienie użytkownikom systemu szkolenia awaryjnego zgodnego z przydzielonymi rolami i obowiązkami:

   1. W ramach [*Realizacja: okres czasu określony przez organizację*] od przyjęcia roli lub odpowiedzialności w sytuacjach awaryjnych;

   2. W przypadku wystąpienia zmian w systemie; oraz

   3. Z częstotliwością [*Realizacja: częstotliwość określona przez organizację*]; oraz

b. Przeglądanie i aktualizacja materiałów szkoleniowych dotyczących sytuacji awaryjnych [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*].

Omówienie: Prowadzone przez organizację szkolenie dotyczące sytuacji awaryjnych jest powiązane z przydzielonymi rolami i obowiązkami personelu organizacji w celu zapewnienia, że odpowiednia treść i poziom szczegółowości jest zawarta w takim szkoleniu. Na przykład niektóre osoby mogą potrzebować jedynie informacji o tym, kiedy i gdzie zgłosić się podczas wykonywania operacji awaryjnych i czy ma to wpływ na wykonywanie standardowych obowiązków; administratorzy systemów mogą potrzebować dodatkowego szkolenia na temat tego, jak ustanowić systemy w alternatywnych miejscach przetwarzania danych; personel organizacyjny może przejść bardziej szczegółowe szkolenie na temat tego, jak prowadzić funkcje istotne dla misji w wyznaczonych miejscach poza siedzibą oraz jak ustanowić komunikację z innymi organizacjami w celu koordynacji działań związanych z sytuacjami awaryjnymi. Szkolenie w zakresie ról lub obowiązków w sytuacjach awaryjnych odzwierciedla szczególne wymogi dotyczące ciągłości określone w planie awaryjnym. Zdarzenia, które mogą spowodować konieczność aktualizacji treści szkoleń w zakresie reagowania kryzysowego obejmują między innymi testowanie planu awaryjnego lub rzeczywistą sytuację kryzysową (zdobyte doświadczenia), wyniki oceny lub audytu,

incydenty lub naruszenia bezpieczeństwa, a także zmiany w prawie, zarządzeniach, dyrektywach, rozporządzeniach, politykach, standardach i wytycznych. Według uznania organizacji, uczestnictwo w teście lub ćwiczeniu planu awaryjnego, w tym w sesjach dotyczących doświadczeń zdobytych w trakcie testu lub ćwiczenia, może spełniać wymagania dotyczące szkolenia w zakresie planowania awaryjnego.

Zabezpieczenia powiązane: AT-2, AT-3, AT-4, CP-2, CP-4, CP-8, IR-2, IR-4, IR-9.

Zabezpieczenia rozszerzone:

(1) SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA | WYDARZENIA SYMULOWANE

Wprowadzenie symulowanych zdarzeń do szkolenia w zakresie planowania ciągłości działania w celu ułatwienia skutecznego reagowania personelu w sytuacjach kryzysowych.

Omówienie: Wykorzystanie symulowanych zdarzeń tworzy środowisko, w którym personel może doświadczyć rzeczywistych zagrożeń, w tym cyberataków, które wyłączają strony internetowe i ataków wymuszających okup (*ang. ransomware attacks*) szyfrujących dane organizacyjne na serwerach; zjawisk pogodowych, które uszkadzają lub niszczą obiekty organizacyjne; a także awarii sprzętu lub oprogramowania.

Zabezpieczenia powiązane: Brak.

(2) SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA | ZAUTOMATYZOWANE ŚRODOWISKA SZKOLENIOWE

Stosowanie mechanizmów operacyjnych w celu zapewnienia bardziej dokładnego i realistycznego środowiska szkoleniowego w zakresie planowania ciągłości działania.

Omówienie: Mechanizmy operacyjne odnoszą się do procesów, które zostały ustanowione w celu osiągnięcia celu organizacyjnego, lub do systemu, który wspiera daną misję organizacyjną lub cel biznesowy. Rzeczywiste procesy,

systemy i/lub obiekty związane z misją i działalnością mogą być wykorzystywane do generowania zdarzeń symulowanych i zwiększania poziomu realizmu zdarzeń symulowanych podczas szkolenia w sytuacjach awaryjnych.

Zabezpieczenia powiązane: Brak.

Referencje: [NIST SP 800-50].

CP-4 TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA

Zabezpieczenie podstawowe:

a. Testowanie planu awaryjnego systemu z częstotliwością [*Realizacja*: *częstotliwość zdefiniowana przez organizację*] za pomocą następujących testów: [*Realizacja*: *testy określone przez organizację*] w celu określenia skuteczności planu i gotowości do jego realizacji.

b. Przeglądanie wyników testu planu awaryjnego; oraz

c. Inicjowanie działań naprawczych (w razie takiej potrzeby).

Omówienie: Metody testowania planów awaryjnych w celu określenia skuteczności planów i zidentyfikowania potencjalnych słabych punktów obejmują listy kontrolne, ćwiczenia typu „walk-through" oraz „tabletop", symulacje (równoległe lub z pełnym przerwaniem) oraz ćwiczenia kompleksowe. Organizacje przeprowadzają testy w oparciu o wymagania zawarte w planach awaryjnych i obejmujące określenie wpływu na działania organizacyjne, zasoby i osoby związane z działaniami awaryjnymi. Organizacje dysponują elastycznością i swobodą w zakresie skali, szczegółowości i harmonogramu podejmowania działań naprawczych.

Zabezpieczenia powiązane: AT-3, CP-2, CP-3, CP-8, CP-9, IR-3, IR-4, PL-2, PM-14, SR-2.

Zabezpieczenia rozszerzone:

(1) TESTOWANIE PLANU AWARYJNEGO | KOORDYNACJA Z POWIĄZANYMI PLANAMI

Koordynowanie prowadzenia testów planów awaryjnych z jednostkami organizacyjnymi odpowiedzialnymi za powiązane plany.

Omówienie: Plany powiązane z planami awaryjnymi obejmują plany ciągłości działania, plany odtworzenia po katastrofie, plany dotyczące infrastruktury krytycznej, plany kontynuacji operacji, plany komunikacji kryzysowej, plany przeciwdziałania wewnętrznym zagrożeniom, plany reagowania na przypadki naruszenia danych, plany odpowiedzi na cyberincydenty, plany reagowania na przypadki naruszenia i plany ewakuacyjne. Koordynacja testowania planów

awaryjnych nie wymaga od organizacji tworzenia struktur organizacyjnych zajmujących się planami pokrewnymi, ani dopasowywania takich struktur do konkretnych planów. Wymaga jednak, aby w przypadku, gdy takie komórki organizacyjne są odpowiedzialne za plany pokrewne, organizacje koordynowały działania z tymi komórkami.

Zabezpieczenia powiązane: IR-8, PM-8.

(2) TESTOWANIE PLANU AWARYJNEGO | ZAPASOWE MIEJSCE PRZETWARZANIA

Testowanie planu awaryjnego w zapasowym miejscu przetwarzania w celu:

(a) Zapoznania personelu awaryjnego z obiektem i dostępnymi zasobami; oraz

(b) Oceny możliwości zapasowego miejsca przetwarzania do obsługi operacji awaryjnych.

Omówienie: Warunki w zapasowym miejscu przetwarzania mogą być znacząco różne od warunków w miejscu głównym. Możliwość zapoznania się z warunkami panującymi w alternatywnym miejscu przetwarzania może dostarczyć cennych informacji na temat potencjalnych słabych punktów, które mogą mieć wpływ na kluczowe zadania i funkcje biznesowe organizacji. Inspekcja miejsca zapasowego może również stanowić okazję do dopracowania planu awaryjnego w celu wyeliminowania podatności zidentyfikowanych podczas testów.

Zabezpieczenia powiązane: CP-7.

(3) TESTOWANIE PLANU AWARYJNEGO | AUTOMATYCZNE TESTOWANIE

Testowanie planu awaryjnego za pomocą [***Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację***]**.**

Omówienie: Zautomatyzowane mechanizmy umożliwiają gruntowne i efektywne testowanie planów awaryjnych dzięki dokładniejszemu odwzorowaniu sytuacji awaryjnych, dobraniu bardziej realistycznych scenariuszy i środowisk testowych, oraz efektywne obciążanie systemu i wspieranych zadań i funkcji biznesowych.

Zabezpieczenia powiązane: Brak.

(4) TESTOWANIE PLANU AWARYJNEGO | PEŁNE ODZYSKIWANIE I ODTWARZANIE

Przeprowadzenie pełnego przywrócenia i odtworzenia systemu do znanego pierwotnego stanu w ramach testowania planu awaryjnego.

Omówienie: Odzyskiwanie to przeprowadzanie działań w ramach planu awaryjnego w celu odtworzenia funkcji biznesowych i misji organizacji. Odtwarzanie odbywa się po odzyskaniu i obejmuje działania mające na celu przywrócenie systemów do stanu pełnej operacyjności. Organizacje ustanawiają znany stan systemów, który obejmuje informacje o stanie sprzętu, oprogramowania i danych. Zachowanie informacji o stanie systemu ułatwia restart systemu i powrót do trybu operacyjnego organizacji z mniejszymi zakłóceniami misji i procesów biznesowych.

Zabezpieczenia powiązane: CP-10, SC-24.

(5) TESTOWANIE PLANU AWARYJNEGO | PRÓBNE AWARIE

Wykorzystanie [***Realizacja: mechanizmy zdefiniowane przez organizację***] **do zakłócania i wywierania niekorzystnego wpływu na system lub komponent systemu** [***Realizacja: zdefiniowany przez organizację system lub komponent systemu***]**.**

Omówienie: Często najlepszą metodą oceny odporności systemu jest jego zakłócenie przez określone działanie. Mechanizmy stosowane przez organizację mogą zakłócać funkcje systemu lub usługi systemowe na wiele sposobów, m.in. przerywając lub wyłączając działanie krytycznych komponentów systemu, zmieniając konfigurację komponentów systemu, pogarszając funkcjonalności krytyczne (np. ograniczając przepustowość sieci), czy zmieniając uprawnienia. Zautomatyzowane, ciągłe i symulowane cyberataki i zakłócenia usług mogą ujawnić nieoczekiwane zależności funkcjonalne i pomóc organizacji w określeniu jej zdolności do zapewnienia odporności w obliczu rzeczywistego cyberataku.

Zabezpieczenia powiązane: Brak.

Referencje: [FIPS 199], [NIST SP 800-34], [NIST SP 800-84], [NIST SP 800-160-2].

CP-5 AKTUALIZACJA PLANU AWARYJNEGO

[Wycofane: Włączone do CP-2].

CP-6 ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII

Zabezpieczenie podstawowe:

a. Ustanowienie alternatywnego miejsca przechowywania, w tym zawarcie niezbędnych umów umożliwiających przechowywanie i wyszukiwanie informacji dotyczących kopii zapasowych systemu; oraz

b. Zagwarantowanie, że zapasowe miejsce przechowywania zapewnia środki bezpieczeństwa równoważne z zabezpieczeniami stosowanymi w miejscu głównym (podstawowym).

Omówienie: Architektury rozproszone geograficznie, które spełniają wymagania ciągłości działania, mogą być uważane za zapasowe miejsca przechowywania danych. Kwestie objęte umowami dotyczącymi alternatywnych miejsc przechowywania obejmują warunki środowiskowe w zapasowych lokalizacjach, zasady dostępu do systemów i obiektów, wymagania dotyczące ochrony fizycznej i środowiskowej oraz koordynację dostarczania i pobierania nośników kopii zapasowych. Alternatywne miejsca przechowywania danych odzwierciedlają wymagania zawarte w planach awaryjnych, dzięki czemu organizacje mogą utrzymać podstawowe funkcje misji i działalności biznesowej pomimo naruszenia, awarii lub zakłóceń w systemach organizacyjnych.

Zabezpieczenia powiązane: CP-2, CP-7, CP-8, CP-9, CP-10, MP-4, MP-5, PE-3, SC-36, SI-13.

Zabezpieczenia rozszerzone:

(1) ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII | SEPARACJA OD MIEJSCA GŁÓWNEGO

Zidentyfikowanie zapasowego miejsca przechowywania, które jest odpowiednio oddzielone od głównego miejsca przechowywania, celem zmniejszenia podatność na oddziaływanie tego samego rodzaju zagrożenia.

Omówienie: Zagrożenia, które mają wpływ na zapasowe miejsca przechowywania są zdefiniowane w organizacyjnej ocenie ryzyka i obejmują klęski żywiołowe, awarie strukturalne, wrogie ataki oraz błędy zaniechania lub działania z własnej winy. Organizacje określają, co uznaje się za wystarczający stopień separacji głównego miejsca przechowywania od zapasowego, na podstawie rodzajów zagrożeń, które stanowią przedmiot zainteresowania. W przypadku takich zagrożeń, jak wrogie ataki, stopień separacji składowisk jest mniej istotny.

Zabezpieczenia powiązane: RA-3.

(2) ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII | CZAS ODZYSKIWANIA I PUNKT ODTWORZENIA DANYCH

Skonfigurowanie zapasowego miejsca przechowywania w celu ułatwienia przeprowadzania operacji odzyskiwania zgodnie z czasem odzyskiwania i punktem odtworzenia danych.

Omówienie: W ramach planowania awaryjnego organizacje ustalają czas odzyskiwania i punkt odtworzenia danych . Konfiguracja zapasowego miejsca przechowywania obejmuje obiekty fizyczne i systemy wspierające operacje odzyskiwania, które zapewniają dostępność i prawidłowe wykonanie.

Zabezpieczenia powiązane: Brak.

(3) ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII | DOSTĘPNOŚĆ

Określenie potencjalnych problemów z dostępnością do zapasowego miejsca przechowywania w przypadku wystąpienia zakłóceń lub katastrofy na całym obszarze oraz określenie jednoznacznych działań łagodzących.

Omówienie: Zakłócenia na całym obszarze odnoszą się do tych rodzajów zakłóceń, które mają szeroki zakres geograficzny, przy czym ustalenia te są dokonywane przez organizacje w oparciu o organizacyjne oceny ryzyka. Wyraźne działania łagodzące obejmują powielanie informacji zapasowych w innych alternatywnych miejscach przechowywania, jeśli wystąpią problemy z dostępem

w pierwotnie wyznaczonych zapasowych miejscach przechowywania, lub planowanie fizycznego dostępu w celu odzyskania informacji zapasowych, jeśli dostęp elektroniczny do lokalizacji zapasowej zostanie zakłócony.

Zabezpieczenia powiązane: RA-3.

Referencje: [NIST SP 800-34].

CP-7 ZAPASOWE MIEJSCE PRZETWARZANIA

Zabezpieczenie podstawowe:

a. Ustanowienie zapasowego miejsca przetwarzania, w tym zawarcie niezbędnych umów umożliwiających przeniesienie i wznowienie [*Realizacja: zdefiniowanych przez organizację operacji systemowych*] podstawowych misji i funkcji biznesowych w ciągu [*Realizacja: zdefiniowany przez organizację okres czasu zgodny z czasem odzyskiwania i celami punktu odzyskiwania danych*], w przypadku niedostępności podstawowych możliwości przetwarzania;

b. Udostępnienie w zapasowym miejscu przetwarzania zastępczego sprzętu i materiałów niezbędnych do przeniesienia i wznowienia operacji lub ustanowienie umów wspierających dostawy do zapasowego miejsca przetwarzania w określonym przez organizację terminie transferu / wznowienia; oraz

c. Zapewnienie zabezpieczeń w zapasowym miejscu przetwarzania, które są równoważne ze środkami bezpieczeństwa w podstawowym miejscu przetwarzania.

Omówienie: Zapasowe miejsca przetwarzania są położone w rejonach geograficznych innych niż pierwotne miejsca przetwarzania i zapewniają możliwość przetwarzania, jeśli pierwotne miejsce przetwarzania jest niedostępne. Alternatywna zdolność przetwarzania może być realizowana przy wykorzystaniu fizycznego miejsca przetwarzania lub innych rozwiązań, takich jak awaryjne przełączanie na dostawcę usług chmurowych lub inną wewnętrzną lub zewnętrzną usługę przetwarzania. Architektury rozproszone geograficznie, które spełniają wymagania ciągłości działania, mogą być uważane za zapasowe miejsca przetwarzania danych. Zabezpieczenia, które są objęte umowami dotyczącymi zapasowych miejsc przetwarzania, uwzględniają warunki środowiskowe w zapasowych miejscach przetwarzania, zasady dostępu, wymogi dotyczące ochrony fizycznej i ochrony środowiska oraz koordynację transferu i przydzielania personelu. Wymagania są

przydzielane do zapasowych miejsc przetwarzania, które odzwierciedlają wymagania zawarte w planach awaryjnych, dzięki czemu organizacje mogą utrzymać podstawowe funkcje misji i działalności biznesowej pomimo naruszenia, awarii lub zakłóceń w systemach organizacyjnych.

Zabezpieczenia powiązane: CP-2, CP-6, CP-8, CP-9, CP-10, MA-6, PE-3, PE-11, PE-12, PE-17, SC-36, SI-13.

Zabezpieczenia rozszerzone:

(1) ZAPASOWE MIEJSCE PRZETWARZANIA | ODSEPAROWANIE OD LOKALIZACJI PODSTAWOWEJ

Zidentyfikowanie zapasowego miejsca przetwarzania, które jest odpowiednio oddzielone od głównego miejsca przetwarzania, celem zmniejszenia podatność na oddziaływanie tego samego rodzaju zagrożenia.

Omówienie: Zagrożenia, które mają wpływ na zapasowe miejsce przetwarzania, są zdefiniowane w organizacyjnej ocenie ryzyka i obejmują klęski żywiołowe, awarie strukturalne, wrogie ataki oraz błędy zaniechania lub działania z własnej winy. Organizacje określają, co uznaje się za wystarczający stopień separacji głównego miejsca przetwarzania od zapasowego, na podstawie rodzajów zagrożeń, które stanowią przedmiot zainteresowania. W przypadku takich zagrożeń, jak wrogie ataki, stopień separacji składowisk jest mniej istotny.

Zabezpieczenia powiązane: RA-3.

(2) ZAPASOWE MIEJSCE PRZETWARZANIA | DOSTĘPNOŚĆ

Określenie potencjalnych problemów z dostępnością do zapasowych miejsc przetwarzania danych w przypadku zakłóceń na danym obszarze lub katastrofy oraz nakreślenie jednoznacznych działań łagodzących.

Omówienie: Zakłócenia na całym obszarze odnoszą się do tych rodzajów zakłóceń, które mają szeroki zakres geograficzny, przy czym ustalenia te są dokonywane przez organizacje w oparciu o organizacyjne oceny ryzyka.

Zabezpieczenia powiązane: RA-3.

(3) ZAPASOWE MIEJSCE PRZETWARZANIA | PRIORYTET USŁUG

Opracowanie umów dotyczących zapasowych miejsca przetwarzania, które zawierają postanowienia dotyczące pierwszeństwa usług zgodnie z wymogami dostępności organizacji (w tym celów dotyczących czasu odzyskiwania).

Omówienie: Umowy dotyczące priorytetów usług odnoszą się do wynegocjowanych umów z dostawcami usług, które zapewniają, że organizacje traktowane są priorytetowo zgodnie z ich wymaganiami dostępności oraz osiągalności zasobów informacyjnych w logicznym i/lub fizycznym zapasowym miejscu przetwarzania. Organizacje ustalają cele dotyczące czasu odzyskiwania, jako część planowania awaryjnego.

Zabezpieczenia powiązane: Brak.

(4) ZAPASOWE MIEJSCE PRZETWARZANIA | GOTOWOŚĆ DO UŻYCIA

Przygotowanie zapasowego miejsca przetwarzania tak, aby mogło ono służyć, jako miejsce operacyjne obsługujące podstawowe działania i funkcje biznesowe.

Omówienie: Przygotowanie miejsca przetwarzania obejmuje określenie ustawień konfiguracyjnych systemów w zapasowym miejscu przetwarzania zgodnych z wymogami dotyczącymi tych ustawień w głównym miejscu przetwarzania oraz zapewnienie niezbędnych dostaw i rozwiązań logistycznych.

Zabezpieczenia powiązane: CM-2, CM-6, CP-4.

(5) ZAPASOWE MIEJSCE PRZETWARZANIA | ZASTĘPCZE ŚRODKI BEZPIECZEŃSTWA

[Wycofane: Włączone do CP-7].

(6) ZAPASOWE MIEJSCE PRZETWARZANIA | BRAK MOŻLIWOŚCI POWROTU DO LOKALIZACJI PODSTAWOWEJ

Zaplanowanie i przygotowanie się na okoliczności uniemożliwiające powrót do głównego miejsca przetwarzania.

Omówienie: Mogą zaistnieć sytuacje, które uniemożliwiają organizacji powrót do głównego miejsca przetwarzania, np. jeżeli klęska żywiołowa (np. powódź lub wiatr) uszkodziła lub zniszczyła lokalizację organizacji i stwierdzono, że odbudowa w tej samej lokalizacji nie jest możliwa (opłacalna).

Zabezpieczenia powiązane: Brak.

Referencje: [NIST SP 800-34].

CP-8 USŁUGI TELEKOMUNIKACYJNE

Zabezpieczenie podstawowe: Ustanowienie alternatywnych usług telekomunikacyjnych, łącznie z niezbędnymi umowami umożliwiającymi wznowienie [*Realizacja: operacje systemowe określone przez organizację*] niezbędnych działań i funkcji biznesowych w ciągu [*Realizacja: okres czasu określony przez organizację*], w przypadku niedostępności podstawowych usług telekomunikacyjnych w głównym lub zapasowym miejscu przetwarzania lub przechowywania.

Omówienie: Usługi telekomunikacyjne (transmisja danych i głosu) w głównych i zapasowych miejscach przetwarzania i przechowywania wchodzą w zakres zabezpieczenia CP-8. Alternatywne usługi telekomunikacyjne odzwierciedlają wymogi ciągłości zawarte w planach awaryjnych w celu utrzymania podstawowych misji i funkcji biznesowych, pomimo utraty podstawowych usług telekomunikacyjnych. Organizacje mogą określić różne okresy czasu odnoszące się do głównych lub zapasowych miejsc przetwarzania i przechowywania. Alternatywne usługi telekomunikacyjne obejmują dodatkowe organizacyjne lub komercyjne naziemne węzły lub linie telekomunikacyjne, łączność radiową (GSM) lub satelitarną. Zawierając umowy o świadczenie alternatywnych usług telekomunikacyjnych organizacje biorą pod uwagę czynniki takie jak dostępność, jakość i zasięg usług.

Zabezpieczenia powiązane: CP-2, CP-6, CP-7, CP-11, SC-7.

Zabezpieczenia rozszerzone:

(1) USŁUGI TELEKOMUNIKACYJNE | PRIORYTETY ŚWIADCZENIA USŁUG

(a) Opracowanie umów o świadczenie podstawowych i alternatywnych usług telekomunikacyjnych, które zawierają postanowienia dotyczące pierwszeństwa usług zgodnie z wymogami dostępności (w tym celów dotyczących czasu odzyskiwania); oraz

(b) Żądanie zapewnienia pierwszeństwa świadczenia usługi telekomunikacyjnej dla wszystkich usług telekomunikacyjnych wykorzystywanych w celu

zapewnienia, w przypadku wystąpienia awarii, wykonywania obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego w sytuacji, gdy podstawowe i / lub alternatywne usługi telekomunikacyjne są świadczone przez wspólnego operatora.

Omówienie: Organizacje biorą pod uwagę potencjalny wpływ na prowadzoną przez nich działalność w sytuacjach, gdy przedsiębiorcy telekomunikacyjni obsługują inne organizacje przy zastosowaniu takich samych przepisów dotyczących pierwszeństwa usług. Stosowne przepisy prawne nakazują przedsiębiorcom telekomunikacyjnych pierwszeństwo świadczenia usług telekomunikacyjnych na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego i rezerwację stosownych zasobów na ich realizację.

Zabezpieczenia powiązane: Brak.

(2) USŁUGI TELEKOMUNIKACYJNE | POJEDYNCZE PUNKTY AWARII

Ustanowienie alternatywnych usług telekomunikacyjnych w celu zmniejszenia prawdopodobieństwa wpływu jednostkowej awarii na świadczenie podstawowych usług telekomunikacyjnych.

Omówienie: W pewnych okolicznościach przedsiębiorcy telekomunikacyjni mogą korzystać z tych samych fizycznych łączy / węzłów telekomunikacyjnych, co zwiększa podatność na zakłócenie świadczonych usług w przypadku awarii tego samego medium transmisyjnego. Ważne jest, aby przedsiębiorca telekomunikacyjny posiadał redundantne drogi obejściowe, umożliwiające świadczenie usług telekomunikacyjnych. Możliwe jest także świadczenie usług telekomunikacyjnych przez alternatywnego przedsiębiorcę telekomunikacyjnego, niekorzystającego z tych samych fizycznych łączy / węzłów telekomunikacyjnych, co główny przedsiębiorca telekomunikacyjny.

Zabezpieczenia powiązane: Brak.

(3) USŁUGI TELEKOMUNIKACYJNE | ROZDZIELENIE DOSTAWCÓW PODSTAWOWYCH I ALTERNATYWNYCH

Nabywanie przez organizacje alternatywnych usług telekomunikacyjnych od przedsiębiorców telekomunikacyjnych, którzy nie są powiązani z głównym przedsiębiorcą telekomunikacyjnym świadczącym usługi organizacji, celem zmniejszenia podatność na oddziaływanie tych samych zagrożeń w stosunku do usług telekomunikacyjnych.

Omówienie: Zagrożenia mające wpływ na usługi telekomunikacyjne są definiowane w organizacyjnej ocenie ryzyka i obejmują klęski żywiołowe, awarie strukturalne, cyberataki lub ataki fizyczne, a także błędy zaniechania lub działania z własnej winy. Organizacje mogą zmniejszyć wzajemną podatność na zagrożenia poprzez minimalizację eksploatacji wspólnej infrastruktury przedsiębiorców telekomunikacyjnych i osiągnięcie wystarczającej separacji geograficznej pomiędzy mediami wykorzystywanymi do świadczenia usług. Organizacje mogą rozważyć korzystanie z usług jednego przedsiębiorcy telekomunikacyjnego w sytuacjach, w których przedsiębiorca telekomunikacyjny może świadczyć alternatywne usługi telekomunikacyjne, które spełniają wymagania w zakresie rozdziału usług uwzględnione w ocenie ryzyka.

Zabezpieczenia powiązane: Brak.

(4) USŁUGI TELEKOMUNIKACYJNE | PLAN AWARYJNY DOSTAWCY

(a) Wymaganie posiadania planów awaryjnych przez głównych i alternatywnych dostawców usług telekomunikacyjnych;

(b) Przeglądanie planów awaryjnych dostawców w celu upewnienia się, że plany te spełniają stawiane przez organizację wymogi dotyczące awaryjności; oraz

(c) Uzyskanie dowodów potwierdzających przeprowadzenie testów awaryjnych i szkoleń przez dostawców z częstotliwością [***Realizacja: częstotliwość określona przez organizację***]**.**

Omówienie: W recenzjach planów awaryjnych dostawców uwzględnia się ich własnościowy charakter. W niektórych sytuacjach, podsumowanie planów awaryjnych dostawcy może być wystarczającym dowodem na to, że organizacje spełniają wymóg przeglądu. Dostawcy usług telekomunikacyjnych mogą również uczestniczyć w ćwiczeniach usuwania skutków awarii. Organizacje mogą wykorzystać tego typu działania w celu spełnienia wymagań dowodowych związanych z przeglądami, testami i szkoleniami dotyczącymi planów awaryjnych dostawców usług.

Zabezpieczenia powiązane: CP-3, CP-4.

(5) USŁUGI TELEKOMUNIKACYJNE | ALTERNATYWNE TESTOWANIE USŁUG TELEKOMUNIKACYJNYCH

Testowanie alternatywnych usług telekomunikacyjnych z częstotliwością [***Realizacja: częstotliwość określona przez organizację***]**.**

Omówienie: Testowanie alternatywnych usług telekomunikacyjnych odbywa się na podstawie umów zawieranych z dostawcami usług. Testowanie może odbywać się równolegle z operacyjnym funkcjonowaniem, aby zapewnić, że nie dojdzie do obniżenia jakości zadań lub funkcji organizacji.

Zabezpieczenia powiązane: CP-3.

Referencje: [NIST SP 800-34].

CP-9 KOPIA ZAPASOWA

Zabezpieczenie podstawowe:

a. Wykonywanie kopii zapasowych informacji na poziomie użytkownika zawartych w [*Realizacja: zdefiniowane przez organizację komponenty systemu*] z częstotliwością [*Realizacja: zdefiniowana przez organizację częstotliwość, zgodna z czasem odzyskiwania i celami punktu odzyskiwania*];

b. Wykonywanie kopii zapasowych informacji na poziomie systemu przetwarzanych w systemie z częstotliwością [*Realizacja: zdefiniowana przez organizację częstotliwość zgodna, z czasem odzyskiwania i celami punktu odzyskiwania*];

c. Wykonywanie kopii zapasowych dokumentacji systemowej, w tym dokumentacji związanej z bezpieczeństwem i ochroną prywatności systemie z częstotliwością [*Realizacja: częstotliwość określona przez organizację, zgodnie z czasem odzyskiwania i celami punktów odzyskiwania*]; oraz

d. Zapewnienie poufności, integralności i dostępności kopii zapasowych w miejscach przechowywania.

Omówienie: Informacje na poziomie systemu obejmują informacje o stanie systemu, oprogramowanie systemu operacyjnego, oprogramowanie pośredniczące, aplikacje i licencje. Informacje na poziomie użytkownika obejmują informacje inne niż informacje na poziomie systemu. Mechanizmy stosowane do ochrony integralności kopii zapasowych systemu obejmują podpisy cyfrowe i skróty kryptograficzne. Ochrona kopii zapasowych systemu podczas przesyłu (transportu) jest realizowana przez zabezpieczenia MP-5 i SC-8. Kopie zapasowe systemu odzwierciedlają wymagania zawarte w planach awaryjnych, a także inne wymagania organizacyjne dotyczące tworzenia kopii zapasowych informacji. Organizacje stosują przepisy prawa, zarządzenia, dyrektywy, rozporządzenia lub zasady zawierające wymagania dotyczące określonych kategorii informacji (np. danych osobowych dotyczących

zdrowia). Personel organizacji konsultuje się z SAOP[45] i radcą prawnym w zakresie powyższych wymagań.

Zabezpieczenia powiązane: CP-2, CP-6, CP-10, MP-4, MP-5, SC-8, SC-12, SC-13, SI-4, SI-13.

Zabezpieczenia rozszerzone:

(1) KOPIA ZAPASOWA | BADANIE NIEZAWODNOŚCI NOŚNIKÓW / INTEGRALNOŚCI INFORMACJI

Testowanie kopii zapasowych z częstotliwością [***Realizacja: częstotliwość określona przez organizację***] ***w*** **celu zweryfikowania niezawodności nośnika danych i integralności informacji.**

Omówienie: Organizacje powinny mieć pewność, że kopie zapasowe mogą być niezawodnie odtworzone. Niezawodność dotyczy systemów i komponentów systemów, w których przechowywane są kopie zapasowe, procesów stosowanych do odtwarzania informacji oraz integralności odtwarzanych informacji. Do każdego z aspektów niezawodności można zastosować niezależne i specjalistyczne testy. Na przykład, odszyfrowanie i przetransportowanie (lub przesłanie) losowo wybranej próbki plików kopii zapasowej z miejsca przechowywania kopii zapasowej oraz jej porównanie z tymi samymi informacjami w głównym miejscu przetwarzania może dać taką pewność.

Zabezpieczenia powiązane: CP-4.

(2) KOPIA ZAPASOWA | TESTY ODTWORZENIOWE Z WYKORZYSTANIEM PRÓBEK DANYCH

W ramach testowania planu awaryjnego należy wykorzystać próbkę informacji zapasowej przy przywracaniu wybranych funkcji systemu.

[45] Patrz: NSC 800-37; NSC 7298.

Omówienie: Organizacje wymagają zapewnienia, że funkcje systemu mogą być przywrócone prawidłowo i mogą wspierać ustalone misje organizacyjne. Aby upewnić się, że wybrane funkcje systemu są dokładnie wykonywane podczas testowania planu awaryjnego, pobierana jest próbka kopii zapasowej w celu określenia, czy funkcje działają zgodnie z założeniami. Organizacje mogą określić wielkość próbki funkcji i informacji zapasowej w oparciu o wymagany poziom pewności.

Zabezpieczenia powiązane: CP-4.

(3) KOPIA ZAPASOWA | SEPARACJA PRZECHOWYWANIA INFORMACJI KRYTYCZNYCH

Przechowywanie kopii zapasowych [***Realizacja: zdefiniowane przez organizację oprogramowanie systemu krytycznego i inne informacje dotyczące bezpieczeństwa***] **w oddzielnym obiekcie lub w ognioodpornym kontenerze, który nie jest umieszczony razem z systemem operacyjnym.**

Omówienie: Oddzielna pamięć dla informacji krytycznych dotyczy wszystkich informacji krytycznych, niezależnie od typu nośnika kopii zapasowej. Oprogramowanie systemów o znaczeniu krytycznym obejmuje systemy operacyjne, oprogramowanie pośredniczące, systemy zarządzania kluczami kryptograficznymi oraz systemy wykrywania włamań. Informacje dotyczące bezpieczeństwa obejmują wykazy sprzętu, oprogramowania i komponentów oprogramowania układowego. Alternatywne miejsca przechowywania danych, w tym rozproszone geograficznie architektury, służą, jako oddzielne miejsca przechowywania kopii zapasowych. Organizacje mogą zapewnić osobną pamięć masową poprzez wdrożenie zautomatyzowanych procesów tworzenia kopii zapasowych w alternatywnych miejscach przechowywania danych (np. w centrach danych).

Zabezpieczenia powiązane: CM-2, CM-6, CM-8.

(4) KOPIA ZAPASOWA | OCHRONA PRZED NIEAUTORYZOWANĄ MODYFIKACJĄ

[Wycofane: Włączone do CP-9].

(5) KOPIA ZAPASOWA | PRZEKAZANIE KOPII DO ALTERNATYWNEJ LOKALIZACJI

Przekazanie kopii zapasowej systemu do alternatywnego miejsca przechowywania [***Realizacja: okres czasu określony przez organizację i szybkość transferu zgodna z czasem odzyskiwania i celami punktu odzyskiwania***]**.**

Omówienie: Informacje dotyczące kopii zapasowych systemu mogą być przekazywane do alternatywnych miejsc przechowywania w formie elektronicznej lub poprzez fizyczną wysyłkę nośników danych.

Zabezpieczenia powiązane: CP-7, MP-3, MP-4, MP-5.

(6) KOPIA ZAPASOWA | REDUNDANCJA (NADMIAROWOŚĆ) SYSTEMU

Wykonanie kopii zapasowej systemu poprzez utrzymanie redundantnego systemu wtórnego, który nie jest kolokowany z systemem podstawowym i który może być aktywowany bez utraty informacji lub zakłóceń w działaniu.

Omówienie: Kopię zapasową systemu można uzyskać poprzez utrzymywanie redundantnego systemu wtórnego, który jest lustrzanym odbiciem systemu pierwotnego, łącznie z replikacją informacji. Jeśli ten rodzaj redundancji jest wdrożony i istnieje wystarczająca separacja geograficzna między dwoma systemami, system wtórny może również służyć, jako alternatywne miejsce przetwarzania.

Zabezpieczenia powiązane: CP-7.

(7) KOPIA ZAPASOWA | PODWÓJNA AUTORYZACJA

Egzekwowanie podwójnej autoryzacji w celu usuwania lub niszczenia [***Realizacja: informacje o kopii zapasowej zdefiniowane przez organizację***]**.**

Omówienie: Podwójna autoryzacja gwarantuje, że usunięcie lub zniszczenie kopii zapasowej może nastąpić tylko wtedy, gdy zadanie to wykonają dwie uprawnione osoby. Osoby usuwające lub niszczące kopie zapasowe posiadają umiejętności lub

wiedzę specjalistyczną pozwalające ustalić, czy proponowane usunięcie lub zniszczenie informacji odzwierciedla zasady i procedury organizacyjne. Podwójna autoryzacja może być również znana, jako dwuosobowe zabezpieczenie. W celu zmniejszenia ryzyka zmowy, organizacje rozważają rotację obowiązków związanych z podwójną autoryzacją na inne osoby.

Zabezpieczenia powiązane: AC-3, AC-5, MP-2.

(8) KOPIA ZAPASOWA | OCHRONA KRYPTOGRAFICZNA

Zaimplementowanie mechanizmów kryptograficznych zapobiegających nieautoryzowanemu ujawnieniu i modyfikacji [Realizacja: *informacje o kopii zapasowej zdefiniowane przez organizację*].

Omówienie: Wybór mechanizmów kryptograficznych opiera się na potrzebie ochrony poufności i integralności kopii zapasowych. Siła wybranych mechanizmów jest współmierna do kategorii bezpieczeństwa lub klasyfikacji informacji. Ochrona kryptograficzna dotyczy informacji o kopiach zapasowych systemu przechowywanych zarówno w lokalizacjach podstawowych, jak i alternatywnych. Organizacje, które wdrażają mechanizmy kryptograficzne w celu ochrony informacji w spoczynku, rozważają również stosowanie rozwiązań w zakresie zarządzania kluczami kryptograficznymi.

Zabezpieczenia powiązane: SC-12, SC-13, SC-28.

Referencje: [FIPS 140-3], [FIPS 186-4], [NIST SP 800-34], [NIST SP 800-130], [NIST SP 800-152].

CP-10 ODZYSKIWANIE I ODTWARZANIE SYSTEMU

Zabezpieczenie podstawowe: Zapewnienie przywrócenia i odtworzenia systemu do znanego stanu w ramach [*Realizacja: określony przez organizację okres czasu zgodny z czasem odzyskiwania i punktem odtworzenia danych*] po wystąpieniu zakłócenia, kompromitacji/naruszenia zasad ochrony lub awarii.

Omówienie: Odzyskiwanie/odtwarzanie to wykonywanie zaplanowanych w planie awaryjnym działań w celu przywrócenia misji organizacji i funkcji biznesowych. Rekonstrukcja odbywa się po odzyskaniu/odtworzeniu i obejmuje działania mające na celu przywrócenie systemów do stanu pełnej operacyjności. Operacje odzyskiwania/odtwarzania i rekonstrukcji odzwierciedlają priorytety misji i funkcji biznesowych; punkt odtworzenia, czas odzyskania i cele odtworzenia; oraz wskaźniki organizacyjne zgodne z wymaganiami planu awaryjnego. Rekonstrukcja obejmuje dezaktywację tymczasowych zdolności systemu, które mogły być wykorzystywane podczas operacji odzyskiwania. Rekonstrukcja obejmuje również ocenę w pełni przywróconych możliwości systemu, przywrócenie działań ciągłego monitorowania, ponowną autoryzację systemu (jeśli jest wymagana) oraz działania mające na celu przygotowanie systemu i organizacji na przyszłe zakłócenia, naruszenia, kompromitacje lub awarie. Możliwości odzyskiwania/odtworzenia i rekonstrukcji mogą obejmować automatyczne mechanizmy i procedury ręczne. Organizacje ustalają czas i cele punktów odtworzenia danych w ramach planowania awaryjnego.

Zabezpieczenia powiązane: CP-2, CP-4, CP-6, CP-7, CP-9, IR-4, SA-8, SC-24, SI-13.

Zabezpieczenia rozszerzone:

(1) ODZYSKIWANIE I ODTWARZANIE SYSTEMU | TESTOWANIE PLANU AWARYJNEGO

[Wycofane: Włączone do CP-4].

(2) ODZYSKIWANIE I ODTWARZANIE SYSTEMU | ODTWARZANIE TRANSAKCJI

Wdrożenie odtwarzania transakcji w systemach opartych na transakcjach.

Omówienie: Systemy oparte na transakcjach obejmują systemy zarządzania bazami danych i systemy przetwarzania transakcji. Mechanizmy wspomagające odzyskiwanie transakcji obejmują wycofywanie transakcji i rejestrowanie transakcji.

Zabezpieczenia powiązane: Brak.

(3) ODZYSKIWANIE I ODTWARZANIE SYSTEMU | KOMPENSACYJNE ŚRODKI BEZPIECZEŃSTWA

[Wycofane: omawiane w procesie dostosowywania zabezpieczeń].

(4) ODZYSKIWANIE I ODTWARZANIE SYSTEMU | PRZYWRACANIE W OKREŚLONYM PRZEDZIALE CZASOWYM

Zapewnienie możliwości przywracania komponentów systemu w ramach [***Realizacja: zdefiniowane przez organizację okresy przywracania***] **z informacji kontrolowanych przez konfigurację i chronionych pod kątem integralności, reprezentujących znany stan operacyjny komponentów.**

Omówienie: Przywracanie komponentów systemu obejmuje ponowne odwzorowanie, które przywraca komponenty do znanych, operacyjnych stanów.

Zabezpieczenia powiązane: CM-2, CM-6.

(5) ODZYSKIWANIE I ODTWARZANIE SYSTEMU |PRACE AWARYJNE

[Wycofane: Włączone do SI-13].

(6) ODZYSKIWANIE I ODTWARZANIE SYSTEMU | OCHRONA KOMPONENTÓW

Ochrona komponentów systemu używanych do odzyskiwania i rekonstrukcji.

Omówienie: Ochrona elementów odzyskiwania i rekonstrukcji systemu (tj. sprzętu, oprogramowania układowego oraz aplikacji) obejmuje zabezpieczenia fizyczne i techniczne. Komponenty tworzenia kopii zapasowych i przywracania

wykorzystywane do odzyskiwania i rekonstrukcji systemów obejmują tabele routingowe, kompilatory i inne oprogramowanie systemowe.

Zabezpieczenia powiązane: AC-3, AC-6, MP-2, MP-4, PE-3, PE-6.

Referencje: [NIST SP 800-34].

CP-11 ALTERNATYWNE PROTOKOŁY KOMUNIKACJI

Zabezpieczenie podstawowe: Zapewnienie zdolności do stosowania [*Realizacja: zdefiniowane przez organizację alternatywne protokoły komunikacyjne*] w celu utrzymania ciągłości działania.

Omówienie: Plany awaryjne oraz szkolenia lub testy awaryjne związane z tymi planami zawierają funkcję alternatywnych protokołów komunikacyjnych, jako część ustalania odporności systemów organizacyjnych. Przełączanie protokołów komunikacyjnych może mieć wpływ na aplikacje programowe i aspekty operacyjne systemów. Organizacje oceniają potencjalne skutki uboczne wprowadzenia alternatywnych protokołów komunikacyjnych przed ich wdrożeniem.

Zabezpieczenia powiązane: CP-2, CP-8, CP-13.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

CP-12 TRYB BEZPIECZNY

Zabezpieczenie podstawowe: W przypadku wykrycia [*Realizacja: warunki zdefiniowane przez organizację*], *należy* wprowadzić bezpieczny tryb pracy z [*Realizacja: ograniczenia bezpiecznego trybu pracy zdefiniowane przez organizację*].

Omówienie: W przypadku systemów, które wspierają krytyczne misje i funkcje biznesowe - w tym operacje wojskowe, cywilne operacje w przestrzeni kosmicznej, działalność elektrowni jądrowych i kontroli ruchu lotniczego (zwłaszcza w środowiskach operacyjnych czasu rzeczywistego) - organizacje mogą określić pewne warunki, w których systemy te powracają do wcześniej zdefiniowanego bezpiecznego trybu pracy. Bezpieczny tryb pracy, który może być uruchamiany automatycznie lub ręcznie, ogranicza operacje, które systemy mogą wykonywać w tych warunkach. Ograniczenie obejmuje zezwolenie na wykonywanie tylko wybranych funkcji, które mogą być wykonywane przy ograniczonej mocy lub przy ograniczonej szerokości pasma przenoszenia.

Zabezpieczenia powiązane: CM-2, SA-8, SC-24, SI-13, SI-17.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

CP-13 ALTERNATYWNE MECHANIZMY BEZPIECZEŃSTWA

Zabezpieczenie podstawowe: Stosowanie [Realizacja: *alternatywne lub dodatkowe mechanizmy zabezpieczające zdefiniowane przez organizację*] *w* celu spełnienia [*Realizacja: alternatywne lub dodatkowe funkcje bezpieczeństwa zdefiniowane przez organizację*] w przypadku, gdy podstawowe środki implementacji funkcji bezpieczeństwa są niedostępne lub zagrożone.

Omówienie: Wykorzystanie alternatywnych mechanizmów bezpieczeństwa wspiera odporność systemu, planowanie awaryjne i ciągłość działania. W celu zapewnienia misji i ciągłość działania, organizacje mogą wdrażać alternatywne lub uzupełniające mechanizmy bezpieczeństwa. Mechanizmy te mogą być mniej skuteczne niż mechanizmy pierwotne. Jednakże zdolność do natychmiastowego zastosowania alternatywnych lub uzupełniających mechanizmów zwiększa ciągłość wykonywania zadań i prowadzenia działalności, które w przeciwnym razie mogłyby zostać zakłócone, gdyby trzeba było ograniczyć operacje do czasu przywrócenia podstawowego sposobu realizacji funkcji. Biorąc pod uwagę koszty i poziom wysiłku wymaganego do zapewnienia takich alternatywnych możliwości, mechanizmy alternatywne lub uzupełniające są stosowane wyłącznie w odniesieniu do krytycznych funkcji bezpieczeństwa zapewnianych przez systemy, komponenty systemu lub usługi systemowe. Na przykład, organizacja może wydawać wyższej kadrze kierowniczej i administratorom systemów zestawy jednorazowych kluczy szyfrujących, jeżeli wielopoziomowe tokeny uwierzytelniające - standardowe środki służące do uzyskiwania bezpiecznego uwierzytelnienia - narażone są na kompromitację.

Zabezpieczenia powiązane: CP-2, CP-11, SI-13.

Zabezpieczenia rozszerzone: Brak

KATEGORIA IA - IDENTYFIKACJA I UWIERZYTELNIANIE

IA-1 POLITYKA I PROCEDURY

Zabezpieczenie podstawowe:

a. Opracowywanie, dokumentowanie i rozpowszechnianie wśród [Realizacja: *personel lub role określone przez organizację*]:

   1. [*Wybór (jeden lub więcej): poziom organizacji; poziom misji/procesu biznesowego; poziom systemu*] polityki identyfikacji i uwierzytelniania, która:

      (a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami; oraz

      (b) Jest zgodna z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi; oraz

   2. Procedur ułatwiających wdrożenie polityki identyfikacji i uwierzytelniania oraz powiązanych zabezpieczeń w zakresie identyfikacji i uwierzytelniania;

b. Wyznaczanie [Realizacja: *osoba wyznaczona przez organizację*] do zarządzania rozwojem, dokumentacją i rozpowszechnianiem polityki i procedur identyfikacji i uwierzytelniania; oraz

c. Przeglądanie i aktualizacja bieżącej:

   1. Polityki identyfikacji i uwierzytelniania z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*]; oraz

   2. Procedur identyfikacji i uwierzytelniania z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*].

Omówienie: Polityka i procedury w zakresie identyfikacji i uwierzytelniania dotyczą zabezpieczeń w kategorii *Identyfikacja i uwierzytelnianie* (IA), które są wdrażane w ramach systemów i organizacji. Strategia zarządzania ryzykiem jest ważnym czynnikiem przy tworzeniu takich polityk i procedur. Polityki i procedury przyczyniają się do zapewnienia bezpieczeństwa i ochrony prywatności. Dlatego ważne jest, aby programy bezpieczeństwa i ochrony prywatności były opracowywane wspólnie przy kształtowaniu polityki i procedur identyfikacji i uwierzytelniania. Polityki i procedury dotyczące programów bezpieczeństwa i ochrony prywatności na poziomie organizacji są ogólnie rzecz biorąc preferowane i mogą eliminować potrzeby tworzenia polityk i procedur specyficznych dla danej misji lub systemu. Polityka może być włączona, jako część ogólnej polityki bezpieczeństwa i ochrony prywatności lub reprezentowana przez wiele polityk odzwierciedlających złożony charakter organizacji. Procedury mogą być ustanowione dla programów bezpieczeństwa i ochrony prywatności, dla misji lub procesów biznesowych oraz dla systemów, jeśli to konieczne. Procedury opisują sposób wdrażania zasad lub zabezpieczeń i mogą być skierowane do osoby lub roli, która jest przedmiotem procedury. Procedury mogą być udokumentowane w planach bezpieczeństwa i ochrony prywatności systemu w jednym lub kilku oddzielnych dokumentach.

Zdarzenia, które mogą spowodować konieczność aktualizacji polityki i procedur identyfikacji i uwierzytelniania, obejmują wyniki oceny lub audytu, incydenty lub naruszenia bezpieczeństwa, lub zmiany w przepisach prawa, zarządzeniach, dyrektywach, rozporządzeniach, zasadach, standardach i wytycznych.

Oświadczenie o wprowadzeniu zabezpieczeń nie jest równoznaczne z ustanowieniem polityki lub procedury organizacyjnej.

Zabezpieczenia powiązane: AC-1, PM-9, PS-8, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [FIPS 201-2], [NIST SP 800-12], [NIST SP 800-30], [NIST SP 800-39], [NIST SP 800-63-3], [NIST SP 800-73-4], [NIST SP 800-76-2], [NIST SP 800-78-4], [NIST SP 800-100], [IR 7874].

IA-2 IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI)

Zabezpieczenie podstawowe: Jednoznaczna identyfikacja i uwierzytelnianie użytkowników organizacyjnych oraz kojarzenie tej unikalnej identyfikacji z procesami działającymi w imieniu tych użytkowników.

Omówienie: Organizacje mogą spełnić wymagania dotyczące identyfikacji i uwierzytelniania poprzez spełnienie wymagań zawartych w [HSPD 12]. Użytkownikami organizacji są pracownicy lub osoby, które organizacje uważają za mające status równoważny z pracownikami (np. podwykonawcy). Jednoznaczna identyfikacja i uwierzytelnianie użytkowników dotyczy wszystkich dostępów innych niż te, które są wyraźnie określone w zabezpieczeniu AC-14 i które odbywają się poprzez uprawnione korzystanie z autoryzacji grupowej bez uwierzytelniania indywidualnego. Ponieważ procesy realizowane są w imieniu grup i ról, organizacje mogą wymagać unikalnej identyfikacji osób na kontach grupowych lub szczegółowego rozliczania poszczególnych działań.

Organizacje stosują hasła, autoryzację fizyczną lub dane biometryczne do uwierzytelniania tożsamości użytkowników lub, w przypadku uwierzytelniania wieloskładnikowego, określoną ich kombinację. Dostęp do systemów organizacyjnych definiowany jest, jako dostęp lokalny lub dostęp sieciowy. Dostęp lokalny to każdy dostęp do systemów organizacyjnych przez użytkowników lub procesy działające w ich imieniu, gdzie dostęp jest uzyskiwany poprzez bezpośrednie połączenia bez użycia sieci. Dostęp sieciowy to dostęp do systemów organizacyjnych przez użytkowników (lub procesy działające w ich imieniu), gdzie dostęp jest uzyskiwany poprzez połączenia sieciowe (tj. dostępy nielokalne). Dostęp zdalny jest rodzajem dostępu sieciowego, który polega na komunikacji poprzez sieci zewnętrzne. Do sieci wewnętrznych należą sieci lokalne oraz sieci rozległe.

Zaszyfrowane wirtualne sieci prywatne wykorzystane do połączeń sieciowych pomiędzy kontrolowanymi przez organizację punktami końcowymi, a punktami końcowymi niekontrolowanymi przez organizację, mogą być traktowane jako sieci

wewnętrzne w odniesieniu do ochrony poufności i integralności informacji przechodzących przez sieć. Wymagania dotyczące identyfikacji i uwierzytelniania użytkowników nieorganizacyjnych są opisane w zabezpieczeniu IA-8.

Zabezpieczenia powiązane: AC-2, AC-3, AC-4, AC-14, AC-17, AC-18, AU-1, AU-6, IA-4, IA-5, IA-8, MA-4, MA- 5, PE-2, PL-4, SA-4, SA-8.

Zabezpieczenia rozszerzone:

(1) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) | UWIERZYTELNIANIE WIELOSKŁADNIKOWE DOSTĘPU DO KONT UPRZYWILEJOWANYCH

Wdrożenie wieloskładnikowego uwierzytelniania w celu uzyskania dostępu do kont uprzywilejowanych.

Omówienie: Uwierzytelnianie wieloskładnikowe wymaga użycia dwóch lub więcej różnych współczynników w celu uzyskania uwierzytelnienia. Współczynniki uwierzytelniające definiuje się w następujący sposób: coś, co znasz (np. osobisty numer identyfikacyjny [PIN]), coś, co posiadasz (np. fizyczny element uwierzytelniający, taki jak kryptograficzny klucz prywatny) lub coś, czym jesteś (np. biometryczny). Do rozwiązań w zakresie uwierzytelniania wieloskładnikowego, w których stosowane są urządzenia do uwierzytelniania fizycznego, należą urządzenia do uwierzytelniania sprzętowego, które dostarczają dane wyjściowe w oparciu o czas lub odpowiedź na wezwanie, oraz karty inteligentne, takie jak osobista karta identyfikacyjna (*ang. Personal Identity Verification - PIV*) lub karta powszechnego dostępu (*ang. Common Access Card - CAC*). Oprócz uwierzytelniania użytkowników na poziomie systemu (tj. podczas logowania), organizacje mogą stosować mechanizmy uwierzytelniania na poziomie aplikacji, według własnego uznania, w celu zapewnienia większego bezpieczeństwa. Niezależnie od rodzaju dostępu (lokalny, sieciowy, zdalny), uwierzytelnianie uprzywilejowanych kont odbywa się za pomocą opcji wieloskładnikowych odpowiednich do poziomu ryzyka. Organizacje mogą

zapewnić uzupełniające środki bezpieczeństwa, takie jak dodatkowe lub bardziej rygorystyczne mechanizmy uwierzytelniania dla określonych rodzajów dostępu.

Zabezpieczenia powiązane: AC-5, AC-6.

(2) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) | UWIERZYTELNIANIE WIELOSKŁADNIKOWE DOSTĘPU DO KONT NIEUPRZYWILEJOWANYCH

Wdrożenie wieloskładnikowego uwierzytelniania w celu uzyskania dostępu do kont nieuprzywilejowanych.

Omówienie: Uwierzytelnianie wieloskładnikowe wymaga użycia dwóch lub więcej różnych współczynników w celu uzyskania uwierzytelnienia. Współczynniki uwierzytelniające definiuje się w następujący sposób: coś, co znasz (np. osobisty numer identyfikacyjny [PIN]), coś, co posiadasz (np. fizyczny element uwierzytelniający, taki jak kryptograficzny klucz prywatny) lub coś, czym jesteś (np. biometryczny). Do rozwiązań w zakresie uwierzytelniania wieloskładnikowego, w których stosowane są urządzenia do uwierzytelniania fizycznego, należą urządzenia do uwierzytelniania sprzętowego, które dostarczają dane wyjściowe w oparciu o czas lub odpowiedź na wezwanie, oraz karty inteligentne, takie jak osobista karta identyfikacyjna (PIV) lub karta powszechnego dostępu (*ang. Common Access Card - CAC*). Oprócz uwierzytelniania użytkowników na poziomie systemu (tj. podczas logowania), organizacje mogą stosować mechanizmy uwierzytelniania na poziomie aplikacji, według własnego uznania, w celu zapewnienia większego bezpieczeństwa. Niezależnie od rodzaju dostępu (lokalny, sieciowy, zdalny), konta nieuprzywilejowane są uwierzytelniane za pomocą opcji wieloskładnikowych odpowiednich do poziomu ryzyka. Organizacje mogą zapewnić uzupełniające środki bezpieczeństwa, takie jak dodatkowe lub bardziej rygorystyczne mechanizmy uwierzytelniania dla określonych rodzajów dostępu.

Zabezpieczenia powiązane: AC-5.

(3) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) | DOSTĘP LOKALNY DO KONT UPRZYWILEJOWANYCH

[Wycofane: Włączone do IA-2(1)]

(4) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) | DOSTĘP LOKALNY DO KONT NIEUPRZYWILEJOWANYCH

[Wycofane: Włączone do IA-2(2)]

(5) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) | UWIERZYTELNIANIE INDYWIDUALNE PRZED UWIERZYTELNIANIEM GRUPOWYM

W przypadku korzystania z kont grupowych lub wystawców uwierzytelnienia, przed udzieleniem dostępu do wspólnych kont lub zasobów należy dokonać indywidualnego uwierzytelnienia użytkowników.

Omówienie: Uwierzytelnianie indywidualne przed uwierzytelnieniem grupowym ogranicza ryzyko związane z korzystaniem z kont grupowych lub wystawców uwierzytelnienia.

Zabezpieczenia powiązane: Brak.

(6) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) | DOSTĘP DO KONT - ODSEPAROWANE URZĄDZENIE

Zaimplementowanie wieloskładnikowego uwierzytelniania w celu uzyskania [Wybór *(jedno lub więcej): lokalny; sieciowy; zdalny*] dostępu do [*Wybór (jedno lub więcej): konta uprzywilejowane; konta nieuprzywilejowane*], w którym:

(a) Jeden z czynników jest zapewniony przez urządzenie niezależne od systemu uzyskującego dostęp; oraz

(b) Urządzenie spełnia [*Realizacja: zdefiniowana przez organizację siła mechanizmu uwierzytelniania*].

Omówienie: Zadaniem zastosowania urządzenia, które jest oddzielone od systemu, do którego użytkownik stara się uzyskać dostęp do jednego z czynników

podczas uwierzytelniania wieloskładnikowego, jest zmniejszenie prawdopodobieństwa narażenia na szwank czynników uwierzytelniających lub poświadczeń przechowywanych w systemie. Nieuczciwe osoby mogą być w stanie naruszyć takie autentyfikatory lub poświadczenia, a następnie podszywać się pod uprawnionych użytkowników. Implementacja jednego z czynników na oddzielnym urządzeniu (np. tokenie sprzętowym), zapewnia wyższą odporność mechanizmu i zwiększony poziom pewności w procesie uwierzytelniania.

Zabezpieczenia powiązane: AC-6.

(7) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) | DOSTĘP SIECIOWY DO NIEUPRZYWILEJOWANYCH KONT - ODSEPAROWANE URZĄDZENIE

[Wycofane: Włączone do IA-2(6)]

(8) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) | DOSTĘP DO KONT – ODPONOŚĆ NA POWTARZANIE

Wdrożenie odpornych na przetwarzanie mechanizmów uwierzytelniania w celu uzyskania dostępu do [***Wybór (jedno lub więcej): konta uprzywilejowane; konta nieuprzywilejowane***]**.**

Omówienie: Procesy uwierzytelniania są odporne na powtórne ataki, jeśli nie jest możliwe uzyskanie pomyślnego uwierzytelnienia poprzez powtórzenie wcześniejszych wiadomości uwierzytelniających. Do technik odpornych na powtórne przetwarzanie należą protokoły wykorzystujące jednorazowe lub synchronizowane czasowo lub kryptograficznie identyfikatory.

Zabezpieczenia powiązane: Brak.

(9) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) | DOSTĘP SIECIOWY DO KONT NIEUPRZYWILEJOWANYCH - ODPONOŚĆ NA POWTARZANIE

[Wycofane: Włączone do IA-2(8)]

(10) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) | LOGOWANIE POJEDYNCZE (Single Sign-On)

Zapewnienie możliwości pojedynczego logowania do [Realizacja: *zdefiniowane przez organizację konta systemowe i usługi*].

Omówienie: Pojedyncze logowanie umożliwia użytkownikom jednorazowe zalogowanie się i uzyskanie dostępu do wielu zasobów systemowych. Organizacje biorą pod uwagę wydajność operacyjną wynikającą z możliwości pojedynczego logowania oraz ryzyko związane z umożliwieniem dostępu do wielu systemów za pomocą jednego zdarzenia uwierzytelniającego. Pojedyncze logowanie może zwiększyć bezpieczeństwo systemu, na przykład dzięki możliwości dodania uwierzytelniania wieloskładnikowego do aplikacji i systemów (istniejących i tworzonych), które mogą nie być w stanie samodzielnie obsługiwać uwierzytelniania wieloskładnikowego.

Zabezpieczenia powiązane: Brak.

(11) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) | ZDALNY DOSTĘP - ODSEPAROWANE URZĄDZENIE

[Wycofane: Włączone do IA-2(6)]

(12) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) | AUTORYZACJA DANYCH DOSTĘPOWYCH

Akceptowanie i elektroniczne weryfikowanie danych identyfikacyjnych karty dostępowej.

Omówienie:[46] Akceptacja i weryfikacja danych identyfikacyjnych karty dostępowej dotyczy organizacji wdrażających logiczne zabezpieczanie dostępu i systemy fizycznej kontroli dostępu. Poświadczenia zgodne z PIV wydane są przez agencje rządowe, które są zgodne z Publikacją FIPS 201 i dodatkowymi wytycznymi. Adekwatność i wiarygodność wydawców kart PIV są autoryzowane przy użyciu [NIST SP 800-79-2]. Akceptacja danych uwierzytelniających zgodnych z dyrektywą

[46] Omówienie dotyczy rynku USA.

PIV obejmuje pochodne dane uwierzytelniające zgodne z dyrektywą PIV, których wykorzystanie omówiono w publikacji [NIST SP 800-166]. Przykładem poświadczenia PIV jest karta powszechnego dostępu DOD Common Access Card (CAC).

Zabezpieczenia powiązane: Brak.

(13) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) | UWIERZYTELNIANIE "POZA PASMEM" (Z WYKORZYSTANIEM DWÓCH ODDZIELNYCH ŚCIEŻEK)

Wdrażanie następujących mechanizmów uwierzytelniania „poza pasmem" w ramach [Realizacja: *uwierzytelnianie „poza pasmem" zdefiniowane przez organizację*] w [*Realizacja: warunki określone przez organizację*].

Omówienie: Uwierzytelnianie „poza pasmem" odnosi się do wykorzystania dwóch oddzielnych ścieżek komunikacyjnych do identyfikacji i uwierzytelniania użytkowników lub urządzeń w systemie informatycznym. Pierwsza ścieżka (tj. ścieżka wewnątrzpasmowa) jest wykorzystywana do identyfikacji i uwierzytelniania użytkowników lub urządzeń i jest zasadniczo ścieżką, przez którą przepływają informacje. Druga ścieżka (tj. ścieżka „poza pasmem") jest wykorzystywana do niezależnej weryfikacji uwierzytelnienia i/lub wymaganych działań. Na przykład użytkownik uwierzytelnia się za pośrednictwem komputera przenośnego do zdalnego serwera, do którego chce uzyskać dostęp i żąda podjęcia pewnych działań przez serwer za pośrednictwem tej ścieżki komunikacyjnej. Następnie serwer kontaktuje się z użytkownikiem za pośrednictwem jego telefonu komórkowego, aby zweryfikować, czy żądana akcja pochodzi od użytkownika. Użytkownik może potwierdzić przez telefon zamierzoną czynność osobie dokonującej uwierzytelnienia lub podać kod uwierzytelniający. Uwierzytelnianie „poza pasmem" może być wykorzystywane do łagodzenia rzeczywistych lub podejrzanych ataków typu "man-in the middle". Warunki lub kryteria aktywacji obejmują podejrzane działania, nowe wskaźniki

zagrożenia, podwyższone poziomy zagrożenia lub wpływ lub poziom klasyfikacji informacji w żądanych transakcjach.

Zabezpieczenia powiązane: IA-10, IA-11, SC-37.

Referencje: [FIPS 140-3], [FIPS 201-2], [FIPS 202], [NIST SP 800-63-3], [NIST SP 800-73-4], [NIST SP 800-76-2], [NIST SP 800-78-4], [NIST SP 800-79-2], [NIST SP 800-156], [NIST SP 800-166], [IR 7539], [IR 7676], [IR 7817], [IR 7849], [IR 7870], [IR 7874], [IR 7966].

IA-3 IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA

Zabezpieczenie podstawowe: Unikalna identyfikacja i uwierzytelnianie [*Realizacja: urządzenia określone przez organizację i/lub typy urządzeń*] przed ustanowieniem dostępu [*Wybór (jedno lub więcej): lokalne; zdalne; sieciowe*].

Omówienie: Urządzenia, które wymagają unikalnej identyfikacji i uwierzytelniania typu urządzenie-urządzenie, są definiowane według typu, urządzenia lub kombinacji typu i urządzenia. Typy urządzeń definiowane przez organizację obejmują urządzenia, które nie są własnością organizacji. Systemy wykorzystują wspólne znane informacje (np. Media Access Control [MAC], protokół zabezpieczeń transmisji/protokół internetowy [TCP/IP]) do identyfikacji urządzeń lub rozwiązań uwierzytelniania organizacyjnego (np. Institute of Electrical and Electronics Engineers (IEEE) 802.1x i Extensible Authentication Protocol [EAP], serwer RADIUS z uwierzytelnianiem EAP-Transport Layer Security [TLS], Kerberos) do identyfikacji i uwierzytelniania urządzeń w sieciach lokalnych i rozległych. Organizacje określają wymaganą siłę mechanizmów uwierzytelniania na podstawie kategorii bezpieczeństwa systemów i misji lub wymagań biznesowych. Ze względu na wyzwania związane z wdrażaniem uwierzytelniania urządzeń na dużą skalę, organizacje mogą zredukować zastosowanie zabezpieczeń do ograniczonej liczby/typu urządzeń w oparciu o misję lub potrzeby biznesowe.

Zabezpieczenia powiązane: AC-17, AC-18, AC-19, AU-6, CA-3, CA-9, IA-4, IA-5, IA-9, IA-11, SI-4.

Zabezpieczenia rozszerzone:

(1) IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA | DWUKIERUNKOWE UWIERZYTELNIANIE KRYPTOGRAFICZNE

Uwierzytelnianie [***Realizacja: urządzenia określone przez organizację i/lub typy urządzeń***] **przed ustanowieniem połączenia** [***Wybór (jeden lub więcej): lokalne; zdalne; sieciowe***] **przy użyciu uwierzytelniania dwukierunkowego opartego na kryptografii.**

Omówienie: Połączenie lokalne to połączenie z urządzeniem, które komunikuje się bez użycia sieci. Połączenie sieciowe to połączenie z urządzeniem, które komunikuje się za pomocą sieci. Połączenie zdalne to połączenie z urządzeniem, które komunikuje się za pomocą sieci zewnętrznej. Uwierzytelnianie dwukierunkowe (kolejne lub jednoczesne uwierzytelnieniu obu podmiotów, które są wzajemnie i naprzemiennie uwierzytelnianym oraz uwierzytelniającym) zapewnia silniejszą ochronę w celu sprawdzenia tożsamości innych urządzeń w przypadku połączeń o podwyższonym ryzyku.

Zabezpieczenia powiązane: SC-8, SC-12, SC-13.

(2) IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA | DWUKIERUNKOWE SIECIOWE UWIERZYTELNIANIE KRYPTOGRAFICZNE

[Wycofane: Włączone do IA-3(1)]

(3) IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA | ALOKACJA ADRESU DYNAMICZNEGO

(a) W przypadku, gdy adresy przydzielane są dynamicznie, należy znormalizować informacje o dzierżawie dynamicznej alokacji adresu oraz czasie trwania dzierżawy przypisanego do urządzeń zgodnie z [Realizacja: zdefiniowane przez organizację informacje o dzierżawie i czasie trwania dzierżawy]; oraz

(b) Przeprowadzanie audytu informacji o dzierżawie adresów dynamicznych, przypisanych do urządzenia.

Omówienie: Protokół dynamicznego konfigurowania hostów (*ang. Dynamic Host Configuration Protocol - DHCP*) jest przykładem sposobu, za pomocą którego klienci mogą dynamicznie uzyskiwać przydziały adresów sieciowych.

Zabezpieczenia powiązane: AU-2.

(4) IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA | ATESTACJA URZĄDZENIA

Identyfikacja i uwierzytelnianie urządzeń na podstawie atestacji przez [***Realizacja: zdefiniowany przez organizację proces zarządzania konfiguracją***]**.**

Omówienie: Atestacja urządzenia odnosi się do identyfikacji i uwierzytelnienia urządzenia na podstawie jego konfiguracji i znanego stanu pracy. Atestacja urządzenia może być określone za pomocą kryptograficznego skrótu (hash-u) urządzenia. Jeżeli atestacja urządzenia jest środkiem identyfikacji i uwierzytelniania, ważne jest, aby poprawki i aktualizacje urządzenia były obsługiwane w ramach procesu zarządzania konfiguracją tak, aby poprawki i aktualizacje były wykonywane w sposób bezpieczny i nie zakłócały identyfikacji i uwierzytelniania innych urządzeń.

Zabezpieczenia powiązane: CM-2, CM-3, CM-6.

Referencje: Brak.

IA-4 ZARZĄDZANIE IDENTYFIKATOREM

Zabezpieczenie podstawowe: Zarządzanie identyfikatorami systemu poprzez:

a. Otrzymywanie upoważnienia od [*Realizacja: personel lub role zdefiniowane przez organizację*] do przypisania unikalnego identyfikatora osobie, grupie, roli, usłudze lub urządzeniu;

b. Wybór identyfikatora, który identyfikuje osobę, grupę, rolę, usługę lub urządzenie;

c. Przypisanie identyfikatora do konkretnej osoby, grupy, roli, usługi lub urządzenia; oraz

d. Zapobieganie ponownemu użyciu identyfikatorów po [*Realizacja: okres czasu określony przez organizację*].

Omówienie: Powszechne identyfikatory urządzeń obejmują adresy MAC, adresy protokołu internetowego (IP) lub unikalne identyfikatory tokenów urządzeń. Zarządzanie poszczególnymi identyfikatorami nie ma zastosowania do wspólnych kont systemowych. Zazwyczaj indywidualne identyfikatory są nazwami użytkowników kont systemowych przypisanymi do tych osób. W takich przypadkach w operacjach zarządzania kontami AC-2 wykorzystuje się nazwy kont dostarczone przez IA-4. Zarządzanie identyfikatorami dotyczy również indywidualnych identyfikatorów, niekoniecznie związanych z kontami systemowymi. Zapobieganie ponownemu użyciu identyfikatorów oznacza zapobieganie przypisaniu poprzednio używanych identyfikatorów indywidualnych, grupowych, ról, usług lub urządzeń do różnych osób, grup, ról, usług lub urządzeń.

Zabezpieczenia powiązane: AC-5, IA-2, IA-3, IA-5, IA-8, IA-9, IA-12, MA-4, PE-2, PE-3, PE-4, PL-4, PM-12, PS- 3, PS-4, PS-5, SC-37.

Zabezpieczenia rozszerzone:

(1) ZARZĄDZANIE IDENTYFIKATOREM | ZAKAZ UŻYWANIA IDENTYFIKATORÓW KONT, JAKO IDENTYFIKATORÓW PUBLICZNYCH

Zakazanie stosowania identyfikatorów kont systemowych, które są takie same jak stosowane w indywidualnych kontach poczty elektronicznej.

Omówienie: Zakaz stosowania identyfikatorów kont, jako publicznych identyfikatorów ma zastosowanie do wszelkich publicznie ujawnionych identyfikatorów kont używanych do komunikacji, takich jak poczta elektroniczna i komunikatory internetowe. Zakaz używania identyfikatorów kont systemowych, które są takie same jak identyfikatory publiczne, takie jak indywidualny fragment identyfikatora w adresie poczty elektronicznej, utrudnia osobom niepowołanym odgadywanie identyfikatorów użytkowników. Zakaz stosowania identyfikatorów kont, jako identyfikatorów publicznych bez wdrożenia innych wspierających mechanizmów zabezpieczających jedynie utrudnia odgadnięcie identyfikatorów. W celu ochrony konta wymagane są dodatkowe zabezpieczenia dotyczące uwierzytelniania i danych poświadczających.

Zabezpieczenia powiązane: AT-2, PT-7.

(2) ZARZĄDZANIE IDENTYFIKATOREM | AUTORYZACJA PRZEŁOŻONEGO

[Wycofane: Włączone do IA-12(1)]

(3) ZARZĄDZANIE IDENTYFIKATOREM | WIELE FORM CERTYFIKACJI

[Wycofane: Włączone do IA-12(2)]

(4) ZARZĄDZANIE IDENTYFIKATOREM | IDENTYFIKACJA STATUSU UŻYTKOWNIKA

Zarządzanie indywidualnymi identyfikatorami poprzez jednoznaczną identyfikację każdej osoby, jako [***Realizacja: zdefiniowana przez organizację cecha identyfikująca status indywidualny***]**.**

Omówienie: Cechy charakterystyczne określające status osób fizycznych obejmują kontrahentów, obcokrajowców i użytkowników niezrzeszonych. Identyfikacja statusu osób na podstawie tych cech dostarcza dodatkowych informacji o osobach, z którymi komunikuje się personel organizacji. Na przykład, przydatne może być, aby urzędnik państwowy wiedział, że jedna z osób znajdujących się w wiadomości e-mail jest kontrahentem.

Zabezpieczenia powiązane: Brak.

(5) ZARZĄDZANIE IDENTYFIKATOREM | ZARZĄDZANIE DYNAMICZNE

Dynamiczne zarządzanie indywidualnymi identyfikatorami zgodnie z [***Realizacja: zdefiniowana przez organizację polityka dynamicznego zarządzania identyfikatorami***]**.**

Omówienie: W przeciwieństwie do konwencjonalnych podejść do identyfikacji, które zakładają statyczne konta dla wstępnie zarejestrowanych użytkowników, wiele systemów rozproszonych ustanawia identyfikatory w czasie rzeczywistym dla podmiotów, które były wcześniej nieznane. Kiedy identyfikatory są ustanawiane w czasie funkcjonowania dla podmiotów, które były wcześniej nieznane, organizacje mogą przewidzieć i zapewnić dynamiczne ustanawianie identyfikatorów. Zasadnicze znaczenie mają wcześniej ustanowione relacje i mechanizmy zaufania z odpowiednimi władzami w celu walidacji danych uwierzytelniających i związanych z nimi identyfikatorów.

Zabezpieczenia powiązane: AC-16.

(6) ZARZĄDZANIE IDENTYFIKATOREM | ZARZĄDZANIE MIĘDZYORGANIZACYJNE

Koordynacja z następującymi organizacjami zewnętrznymi w zakresie zarządzania identyfikatorami w różnych organizacjach: [***Realizacja: organizacje zewnętrzne zdefiniowane przez organizację***]***.***

Omówienie: Zarządzanie identyfikatorami organizacji zapewnia możliwość identyfikacji osób, grup, ról lub urządzeń podczas prowadzenia działań

międzybranżowych obejmujących przetwarzanie, przechowywanie lub przekazywanie informacji.

Zabezpieczenia powiązane: AU-16, IA-2, IA-5.

(7) ZARZĄDZANIE IDENTYFIKATOREM | REJESTRACJA OSOBISTA

[Wycofane: Włączone do IA-12(4)]

(8) ZARZĄDZANIE IDENTYFIKATOREM | PAROWANIE IDENTYFIKATORÓW PODCZAS PSEUDONIMIZACJI

Generowanie parami identyfikatorów pseudonimowych.

Omówienie: Para stanowiąca pseudonim i nazwę właściwą jest nieczytelnym, trudnym do odgadnięcia identyfikatorem użytkownika generowanym przez dostawcę tożsamości do wykorzystania przez konkretną indywidualną stronę ufającą. Generowanie odrębnych parami pseudonimowych identyfikatorów bez informacji identyfikujących użytkownika zniechęca do śledzenia aktywności użytkownika i profilowania wykraczającego poza wymagania operacyjne ustalone przez organizację. Pseudonimowe identyfikatory są unikatowe dla każdej strony ufającej, z wyjątkiem sytuacji, w których strony ufające mogą wykazać dającą się udowodnić relację uzasadniającą operacyjną potrzebę korelacji lub wszystkie strony wyrażają zgodę na taką korelację.

Zabezpieczenia powiązane: IA-5.

(9) ZARZĄDZANIE IDENTYFIKATOREM | UTRZYMANIE I OCHRONA ATRYBUTÓW

Utrzymanie atrybutów dla każdej jednoznacznie zidentyfikowanej osoby, urządzenia lub usługi w [***Realizacja: chroniony magazyn centralny zdefiniowany przez organizację***]**.**

Omówienie: Dla każdego z podmiotów objętych zabezpieczeniami IA-2, IA-3, IA-8 i IA-9 ważne jest stałe utrzymywanie atrybutów dla każdego uwierzytelnionego podmiotu w centralnym (chronionym) magazynie.

Zabezpieczenia powiązane: Brak.

Referencje: [FIPS 201-2], [NIST SP 800-63-3], [NIST SP 800-73-4], [NIST SP 800-76-2], [NIST SP 800-78-4].

IA-5 ZARZĄDZANIE METODAMI UWIERZYTELNIANIA

Zabezpieczenie podstawowe: Zarządzanie autoryzacją systemu poprzez:

a. Weryfikację, w ramach wstępnej dystrybucji podmiotu uwierzytelniającego, tożsamości osoby, grupy, roli, usługi lub urządzenia uczestniczącego w procesie uwierzytelniania;

b. Ustalanie wstępnej treści uwierzytelniającej dla wszystkich wydawanych przez organizację mechanizmów uwierzytelniających;

c. Zagwarantowanie, aby mechanizmy uwierzytelniające posiadały siłę odpowiednią do ich docelowego zastosowania;

d. Ustanowienie i wdrożenie procedur administracyjnych w zakresie wstępnej dystrybucji mechanizmów uwierzytelniających, utraconych, naruszonych lub uszkodzonych mechanizmów uwierzytelniających oraz unieważniania mechanizmów uwierzytelniających;

e. Zmiana domyślnych elementów uwierzytelniających przed pierwszym użyciem;

f. Zmiana lub uaktualnianie autentyfikatorów [*Realizacja: zdefiniowany przez organizację okres czasu według typu autentyfikatora*] lub w przypadku wystąpienia [*Realizacja: zdefiniowane przez organizację zdarzenia*];

g. Ochrona treści autentyfikatorów przed nieuprawnionym ujawnieniem i modyfikacją;

h. Wymaganie, aby osoby podjęły, a urządzenia wdrożyły, określone zabezpieczenia w celu ochrony autentyfikatorów; oraz

i. Zmiana danych uwierzytelniających.

Omówienie: Elementami uwierzytelniającymi (autenyfikatorami) są hasła, urządzenia kryptograficzne, biometryka, certyfikaty, urządzenia z hasłem jednorazowym i identyfikatory. Urządzenia uwierzytelniające zawierają certyfikaty i hasła. Początkowy kontent uwierzytelniania to rzeczywista treść autentyfikacji (np. hasło

początkowe). Natomiast wymogi dotyczące treści uwierzytelniającej zawierają określone kryteria lub cechy (np. minimalną długość hasła). Deweloperzy mogą dostarczyć komponenty systemu z domyślnymi fabrycznymi danymi uwierzytelniającymi (tj. hasłami), które umożliwią wstępną instalację i konfigurację. Domyślne dane uwierzytelniające są często dobrze znane, łatwo wykrywalne i stanowią znaczące ryzyko. Wymóg ochrony poszczególnych autentyfikatorów może być realizowany za pomocą zabezpieczeń PL-4 lub PS-6 dla autentyfikatorów będących w posiadaniu osób oraz za pomocą zabezpieczeń AC-3, AC-6 i SC-28 dla autentyfikatorów przechowywanych w systemach organizacyjnych, w tym haseł przechowywanych w zahaszowanych lub zaszyfrowanych formatach lub plików zawierających zahaszowane lub zaszyfrowane hasła dostępne z poziomu uprawnień administratora.

Systemy wspierają zarządzanie autentyfikatorami poprzez zdefiniowane organizacyjnie ustawienia i ograniczenia dla różnych cech uwierzytelniania (np. minimalna długość hasła, okno czasowe walidacji dla synchronicznych czasowo tokenów jednorazowych oraz liczba dopuszczalnych odrzuceń na etapie weryfikacji uwierzytelniania biometrycznego). Możliwe jest podjęcie działań mających na celu ochronę poszczególnych elementów uwierzytelniających, w tym utrzymywanie ich tylko w swoim posiadaniu, nieudostępnianie ich innym podmiotom, a także natychmiastowe zgłaszanie zagubionych, skradzionych lub naruszonych elementów uwierzytelniających. Zarządzanie elementami uwierzytelniającymi obejmuje wydawanie i unieważnianie autentyfikatorów umożliwiających tymczasowy dostęp, gdy nie są już wymagane.

Zabezpieczenia powiązane: AC-3, AC-6, CM-6, IA-2, IA-4, IA-7, IA-8, IA-9, MA-4, PE-2, PL-4, SC-12, SC-13.

Zabezpieczenia rozszerzone:

(1) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | UWIERZYTELNIANIE OPARTE O HASŁA

Dokonując uwierzytelniania na podstawie hasła:

(a) Zachowywanie listy haseł powszechnie używanych, oczekiwanych lub ujawnionych i ich aktualizowanie [***Realizacja: częstotliwość zdefiniowana przez organizację***] **oraz gdy istnieje podejrzenie, że hasła organizacyjne zostały bezpośrednio lub pośrednio narażone na skompromitowanie;**

(b) Sprawdzanie, czy podczas tworzenia lub aktualizacji haseł użytkowników zgodnie z IA-5(1)(a), nie znajdują się one na liście haseł powszechnie używanych, oczekiwanych lub ujawnionych;

(c) Przesyłanie haseł tylko przez kanały chronione kryptograficznie;

(d) Przechowywanie haseł przy użyciu zatwierdzonej „zasolonej" funkcji wyprowadzania kluczy, najlepiej przy użyciu skrótu klawiszowego;

(e) Wymaganie natychmiastowego wyboru nowego hasła po odzyskaniu konta;

(f) Umożliwienie użytkownikowi wyboru długich haseł i zwrotów kluczowych, w tym spacji i wszystkich możliwych do wprowadzenia znaków;

(g) Stosowanie zautomatyzowanych narzędzi wspomagających użytkownika w wyborze silnych haseł uwierzytelniających; oraz

(h) Egzekwowanie następujących zasad struktury i złożoności: [***Realizacja: określone przez organizację zasady dotyczące struktury i złożoności***]**.**

Omówienie: Uwierzytelnianie oparte na hasłach dotyczy haseł niezależnie od tego, czy są one używane w uwierzytelnianiu jedno- czy wieloskładnikowym. Długie hasła lub frazy są lepsze od krótszych haseł. Wymuszone struktury haseł zapewniają znikome korzyści w zakresie bezpieczeństwa zmniejszając jednocześnie użyteczność. Organizacje mogą jednak zdecydować się na

ustanowienie pewnych zasad generowania haseł (np. minimalna ilość znaków dla długich haseł) w pewnych okolicznościach i mogą egzekwować ten wymóg w zabezpieczeniu IA-5(1)(h). Odzyskiwanie konta może mieć miejsce na przykład w sytuacjach, gdy hasło zostanie zapomniane. Hasła chronione kryptograficznie obejmują "zasolone" jednokierunkowe kryptograficzne skróty haseł. Lista powszechnie stosowanych, zagrożonych lub oczekiwanych haseł obejmuje hasła uzyskane z poprzednich zbiorów naruszeń, słowa ze słowników oraz powtarzające się lub sekwencyjne znaki. Lista zawiera słowa specyficzne dla danego kontekstu, takie jak nazwa usługi, nazwa użytkownika i ich pochodne.

Zabezpieczenia powiązane: IA-6.

(2) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | UWIERZYTELNIANIE OPARTE O INFRASTRUKTURĘ KLUCZA PUBLICZNEGO

(a) W przypadku uwierzytelniania opartego na kluczu publicznym organizacja:

(1) Wymusza autoryzowany dostęp do odpowiedniego klucza prywatnego; oraz

(2) Dokonuje mapowania uwierzytelnionej tożsamości do konta indywidualnego lub grupy; oraz

(b) W przypadku korzystania z infrastruktury klucza publicznego (PKI) organizacja:

(1) Zatwierdza certyfikaty oraz sprawdza informacje o statusie certyfikatu, konstruując i weryfikując ścieżkę certyfikacji do zaakceptowanej „kotwicy zaufania" (*ang. Trust Anchor*); oraz

(2) Implementuje lokalną pamięć podręczną unieważnionych danych w celu obsługi ścieżki wykrywania i sprawdzania.

Omówienie: Kryptografia klucza publicznego jest ważnym mechanizmem uwierzytelniania osób, maszyn i urządzeń. W przypadku rozwiązań PKI, informacje o statusie ścieżek certyfikacji zawierają listy unieważnień certyfikatów lub

komunikaty o zgodności certyfikatu. W przypadku kart PIV, walidacja certyfikatów obejmuje budowę i weryfikację ścieżki certyfikacji do kotwicy zaufania *Common Policy Root*, która obejmuje przetwarzanie polityki certyfikacyjnej. Wdrożenie lokalnego pamięci podręcznej o unieważnieniu danych w celu wsparcia wyszukiwania i walidacji ścieżek wspiera również dostępność systemu w sytuacjach, gdy organizacje nie mają dostępu sieciowego do unieważnionych informacji.

Zabezpieczenia powiązane: IA-3, SC-17.

(3) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | REJESTRACJA OSOBISTA LUB PRZEZ ZAUFANĄ TRZECIĄ STRONĘ

[Wycofane: Włączone do IA-12(4)].

(4) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | AUTOMATYCZNE WSPARCIE OKREŚLANIA SIŁY HASŁA

[Wycofane: Włączone do IA-5(1)]

(5) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | ZMIANA METODY UWIERZYTELNIANIA PRZED DOSTAWĄ

Wymaga od programistów i instalatorów komponentów systemu dostarczania unikalnych uwierzytelnień lub zmiany domyślnych uwierzytelnień przed dostawą i instalacją.

Omówienie: Zmiana elementów uwierzytelniających przed dostawą i instalacją komponentów systemu rozszerza nałożony na organizacje wymóg zmiany domyślnych elementów uwierzytelniających przy instalacji systemu, wymagając od programistów i/lub instalatorów dostarczania niepowtarzalnych elementów uwierzytelniających lub zmiany domyślnych elementów uwierzytelniających przed dostawą i/lub instalacją. Jednak zazwyczaj nie ma to zastosowania do deweloperów produktów informatycznych dostępnych komercyjnie. Wymagania dotyczące niepowtarzalnych elementów uwierzytelniających mogą być zawarte w

dokumentach zakupu przygotowywanych przez organizację podczas zamawiania systemów lub ich komponentów.

Zabezpieczenia powiązane: Brak.

(6) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | OCHRONA METOD UWIERZYTELNIANIA

Ochrona elementów uwierzytelniających współmiernie do kategorii bezpieczeństwa informacji, do których dostęp jest możliwy dzięki zastosowaniu danego elementu uwierzytelniającego.

Omówienie: W przypadku systemów wymagających zastosowania wielu kategorii bezpieczeństwa informacji bez wiarygodnego fizycznego lub logicznego rozdzielenia poszczególnych kategorii, elementy uwierzytelniające wykorzystywane do przyznawania dostępu do systemów są chronione proporcjonalnie do najwyższej kategorii bezpieczeństwa informacji znajdujących się w tych systemach. Kategorie bezpieczeństwa informacji są określane w ramach procesu nadawania kategorii bezpieczeństwa.

Zabezpieczenia powiązane: RA-2.

(7) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | BRAK WBUDOWANYCH NIEZASZYFROWANYCH STATYCZNYCH ELEMENTÓW UWIERZYTELNIANIA

Zapewnienie, że niezaszyfrowane statyczne elementy uwierzytelniające nie są osadzone w aplikacjach lub innych formach statycznego magazynu danych.

Omówienie: Oprócz aplikacji, inne formy statycznego przechowywania obejmują skrypty dostępu i klawisze funkcyjne. Organizacje zachowują ostrożność przy ustalaniu, czy wbudowane lub przechowywane elementy uwierzytelniające są w formie zaszyfrowanej czy niezaszyfrowanej. Jeśli mechanizmy uwierzytelniające są wykorzystywane w sposób, w jaki są przechowywane, wówczas te reprezentacje są uznawane za niezaszyfrowane mechanizmy uwierzytelniające.

Zabezpieczenia powiązane: Brak.

(8) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | JEDNO KONTO W WIELU SYSTEMACH INFORMACYJNYCH

Wdrożenie [***Realizacja: określone przez organizację środki bezpieczeństwa***] ***w* celu zarządzania ryzykiem naruszenia bezpieczeństwa z powodu posiadania przez personel tych samych kont w wielu systemach.**

Omówienie: W przypadku, gdy personel organizacji posiada te same konta w wielu systemach i korzysta z tych samych elementów uwierzytelniających, takich jak hasła, istnieje ryzyko, że naruszenie jednego konta może doprowadzić do naruszenia innych kont. Alternatywne podejścia obejmują posiadanie różnych elementów uwierzytelniających (haseł) we wszystkich systemach, stosowanie mechanizmu jednego logowania lub federacji mechanizmu logowania lub stosowanie określonej formy haseł jednorazowych we wszystkich systemach. Organizacje mogą również stosować zasady postępowania (zob. zabezpieczenie PL-4) i umowy współpracy (zob. zabezpieczenie PS-6) w celu ograniczenia ryzyka związanego z wieloma kontami systemowymi.

Zabezpieczenia powiązane: PS-6.

(9) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | ZARZĄDZANIE DANYMI UWIERZYTELNIAJĄCYMI MIĘDZY ORGANIZACJAMI

Koordynuje działania z [***Realizacja: organizacje zewnętrzne zdefiniowane przez organizację***] **w zakresie zarządzania metodami uwierzytelniania między organizacjami.**

Omówienie: Koordynacja działań między organizacjami zapewnia organizacjom możliwość uwierzytelniania osób i urządzeń podczas prowadzenia działań międzybranżowych związanych z przetwarzaniem, przechowywaniem lub przekazywaniem informacji. Wykorzystanie specjalnej listy zatwierdzonych

organizacji zewnętrznych do uwierzytelniania pomaga zapewnić, że organizacje te są sprawdzone i godne zaufania.

Zabezpieczenia powiązane: AU-7, AU-16.

(10) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | DYNAMICZNE KOJARZENIE DANYCH UWIERZYTELNIAJĄCYCH

Dynamiczne kojarzenie tożsamości i uwierzytelniania za pomocą następujących zasad: [***Realizacja: zasady weryfikujące tożsamość określone przez organizację***]**.**

Omówienie: Uwierzytelnienie wymaga pewnej formy powiązania między tożsamością, a jednostką uwierzytelniającą, która jest wykorzystywana do potwierdzenia tożsamości. W konwencjonalnych podejściach kojarzenie ustanawia się poprzez uprzednie wprowadzenie do systemu zarówno tożsamości, jak i podmiotu uwierzytelniającego. Na przykład, kojarzenie między nazwą użytkownika (tzn. tożsamością), a hasłem (tzn. uwierzytelnianiem) odbywa się poprzez dostarczenie tożsamości i uwierzytelniania, jako pary w systemie. Nowe techniki uwierzytelniania pozwalają na kojarzenie między tożsamością, a podmiotem uwierzytelniającym poza systemem. Na przykład, w przypadku uwierzytelnienia za pomocą karty elektronicznej, tożsamość i podmiot uwierzytelniający są powiązane ze sobą na karcie elektronicznej. Korzystając z tych poświadczeń, systemy mogą uwierzytelniać tożsamość, która nie została wcześniej określona, dynamicznie dostarczając tożsamość po uwierzytelnieniu. W takich sytuacjach, organizacje mogą przewidzieć dynamiczne dostarczanie tożsamości. Niezbędne jest wcześniejsze ustanowienie relacji i mechanizmów zaufania z odpowiednimi organami w celu potwierdzenia tożsamości i powiązanych danych uwierzytelniających.

Zabezpieczenia powiązane: AU-16, IA-5.

(11) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | UWIERZYTELNIANIE PRZY UŻYCIU TOKENA

[Wycofane: Włączone do IA-2(1) i IA-2(2)].

(12) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | WYDAJNOŚĆ UWIERZYTELNIANIA BIOMETRYCZNEGO

W przypadku uwierzytelniania na podstawie danych biometrycznych należy stosować mechanizmy, które spełniają następujące wymagania jakości biometrycznej [***Realizacja: zdefiniowane przez organizację wymagania jakości identyfikacji biometrycznej***]**.**

Omówienie: W odróżnieniu od uwierzytelniania opartego na hasłach, które zapewnia dokładne dopasowanie wprowadzonych przez użytkownika haseł do przechowywanych haseł, uwierzytelnianie biometryczne nie zapewnia ścisłego dopasowania. W zależności od rodzaju danych biometrycznych i rodzaju mechanizmu ich pobierania, istnieje prawdopodobieństwo wystąpienia pewnych rozbieżności w stosunku do przedstawionych danych biometrycznych i przechowywanych danych biometrycznych, które służą jako podstawa do porównania. Skuteczność dopasowania to współczynnik, przy którym algorytm biometryczny prawidłowo doprowadza do dopasowania w przypadku prawdziwego użytkownika i odrzuca innych użytkowników. Wymagania dotyczące wyników biometrycznych obejmują wskaźnik dopasowania, który odzwierciedla dokładność algorytmu dopasowania biometrycznego stosowanego w systemie.

Zabezpieczenia powiązane: AC-7.

(13) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | PRZEDAWNIENIE BUFOROWANYCH ELEMENTÓW UWIERZYTELNIANIA

Zabronienie używania buforowanych elementów uwierzytelniania po [***Realizacja: okres czasu określony przez organizację***]**.**

Omówienie: Buforowanie elementów uwierzytelniających jest używane do uwierzytelniania na komputerze lokalnym, gdy sieć nie jest dostępna. Jeżeli

informacje uwierzytelniające buforowane w pamięci podręcznej są nieaktualne, ważność informacji o uwierzytelnianiu może być wątpliwa.

Zabezpieczenia powiązane: Brak.

(14) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | ZARZĄDZANIE ZAWARTOŚCIĄ ZAUFANYCH MAGAZYNÓW INFRASTRUKTURY KLUCZA PUBLICZNEGO

W przypadku uwierzytelniania opartego na infrastrukturze klucza publicznego, stosuje się metodologię zarządzania zawartością magazynów zaufania infrastruktury klucza publicznego zainstalowanych na wszystkich platformach w całej organizacji, w tym w sieciach, systemach operacyjnych, przeglądarkach i aplikacjach.

Omówienie: Obejmująca całą organizację metodologia zarządzania zawartością magazynów zaufania infrastruktury klucza publicznego (PKI) pomaga zwiększyć dokładność i aktualność poświadczeń uwierzytelniania opartych na infrastrukturze PKI w organizacji.

Zabezpieczenia powiązane: Brak.

(15) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | ZATWIERDZANIE PRODUKÓW I USŁUG WEDŁUG Z GÓRY USTALONYCH REGUŁ

Używanie wyłącznie produktów i usług zatwierdzonych przez stosowne organy do zarządzania tożsamością, wiarygodnością i dostępem.

Omówienie: Produkty i usługi zatwierdzone przez stosowne organy to produkty i usługi, które zostały zatwierdzone w ramach programu zgodności, tam gdzie ma to zastosowanie, i umieszczone na liście zatwierdzonych produktów[47].

[47] Np. Lista produktów zatwierdzonych przez General Services Administration (GSA Approved Products List). GSA zapewnia wytyczne dla zespołów projektujących i budujących funkcjonalne i bezpieczne systemy, które są zgodne z polityką, technologiami i wzorcami implementacji Federal Identity, Credential, and Access Management (FICAM).

Zabezpieczenia powiązane: Brak.

(16) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | WYDAWANIE POŚWIADCZEŃ UWIERZYTELNIAJĄCYCH OSOBIŚCIE LUB PRZEZ ZAUFANĄ TRZECIĄ STRONĘ

Wymaganie, aby wydawanie [*Realizacja: określone przez organizację rodzaje poświadczeń uwierzytelniających*] *było* przeprowadzane [*Wybór: osobiście; przez zaufaną trzecią stronę*] przed [*Realizacja: określony przez organizację organ rejestracyjny*] przez upoważniony (posiadający pełnomocnictwo) [*Realizacja: określony przez organizację personel lub role*].

Omówienie: Wydawanie autoryzacji osobiście lub przez zaufaną trzecią stronę zwiększa i wzmacnia wiarygodność procesu potwierdzania tożsamości.

Zabezpieczenia powiązane: IA-12.

(17) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | WYKRYWANIE ATAKÓW PREZENTACYJNYCH PODCZAS UWIERZYTELNIANIA BIOMETRYCZNEGO

Zastosowanie mechanizmów wykrywania ataków prezentacyjnych podczas uwierzytelniania biometrycznego.

Omówienie: Cechy biometryczne nie stanowią tajemnic. Cechy te można uzyskać poprzez dostęp do Internetu, zrobienie zdjęcia komuś telefonem z aparatem fotograficznym w celu uzyskania obrazów twarzy za jego wiedzą lub bez niej, pobranie z przedmiotów, których ktoś dotknął (np. ukryty odcisk palca), lub uchwycenie obrazu o wysokiej rozdzielczości (np. wzór tęczówki). Technologie wykrywania ataków prezentacyjnych, w tym rozpoznawania żywotności twarzy, mogą zmniejszyć ryzyko tego typu ataków, utrudniając tworzenie artefaktów mających na celu zakłócenie czujnika biometrycznego.

Zabezpieczenia powiązane: AC-7.

(18) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | MENEDŻER HASEŁ

(a) Wykorzystywanie [***Realizacja: menedżer haseł zdefiniowany przez organizację***] **do generowania i zarządzania hasłami; oraz**

(b) Zabezpieczanie haseł przy użyciu [***Realizacja: środki bezpieczeństwa zdefiniowane przez organizację***]**.**

Omówienie: W przypadku systemów, w których stosowane są hasła statyczne, często wyzwaniem jest zapewnienie, aby hasła były odpowiednio złożone i aby te same hasła nie były stosowane w wielu systemach. Rozwiązaniem tego problemu jest menedżer haseł, który automatycznie generuje i przechowuje silne i różne hasła dla różnych kont. Potencjalne ryzyko związane z korzystania z menedżera haseł polega na tym, że przeciwnicy mogą zaatakować zbiór haseł wygenerowanych przez menedżera haseł. W związku z tym zbiór haseł wymaga ochrony obejmującej szyfrowanie haseł (zob. zabezpieczenie IA-5(1)(d)) oraz przechowywanie zbioru w trybie offline w tokenie.

Zabezpieczenia powiązane: Brak.

Referencje: [FIPS 140-3], [FIPS 180-4], [FIPS 201-2], [FIPS 202], [NIST SP 800-63-3], [NIST SP 800-73-4], [NIST SP 800-76-2], [NIST SP 800-78-4], [IR 7539], [IR 7817], [IR 7849], [IR 7870], [IR 8040].

IA-6 OCHRONA PROCESU UWIERZYTELNIANIA

Zabezpieczenie podstawowe: Ukrywanie informacji zwrotnych dotyczących uwierzytelniania podczas procesu uwierzytelniania w celu ochrony tych informacji przed ewentualnym wykorzystaniem przez osoby nieuprawnione.

Omówienie: Informacje zwrotne z systemów uwierzytelniania nie dostarczają informacji, które pozwoliłyby osobom nieupoważnionym na naruszenie mechanizmów uwierzytelniania. W przypadku niektórych rodzajów systemów, takich jak komputery stacjonarne lub notebooki ze stosunkowo dużymi monitorami, zagrożenie (określane jako "surfowanie po ramionach") może być znaczące. W przypadku innych rodzajów systemów, takich jak urządzenia przenośne z małymi wyświetlaczami, zagrożenie może być mniej znaczące i jest zrównoważone przez zwiększone prawdopodobieństwo błędów typograficznych przy wprowadzaniu danych z powodu małych klawiatur. W związku z tym odpowiednio dobiera się środki służące do ukrywania (maskowania) informacji zwrotnych dotyczących uwierzytelniania. Ukrywanie informacji zwrotnych dotyczących uwierzytelniania to między innymi wyświetlanie gwiazdek podczas wpisywania przez użytkowników haseł na urządzeniach wejściowych lub wyświetlanie informacji zwrotnych przez bardzo ograniczony czas przed ich ukryciem.

Zabezpieczenia powiązane: AC-3.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

IA-7 UWIERZYTELNIANIE MODUŁU KRYPTOGRAFICZNEGO

Zabezpieczenie podstawowe: Wdrożenie w module kryptograficznym mechanizmów uwierzytelniania, które spełniają wymagania obowiązujących przepisów, rozporządzeń, dyrektyw, polityk, regulacji, standardów i wytycznych dotyczących takiego uwierzytelniania.

Omówienie: Mechanizmy uwierzytelniania mogą być wymagane w ramach modułu kryptograficznego w celu uwierzytelnienia operatora uzyskującego dostęp do modułu i sprawdzenia, czy operator jest uprawniony do przyjęcia żądanej roli i wykonywania usług w ramach tej roli.

Zabezpieczenia powiązane: AC-3, IA-5, SA-4, SC-12, SC-13.

Zabezpieczenia rozszerzone: Brak.

Referencje: [FIPS 140-3].

IA-8 IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI)

Zabezpieczenie podstawowe: Unikalna identyfikacja i uwierzytelnianie użytkowników spoza organizacji lub procesów działających w imieniu tych użytkowników.

Omówienie: Do użytkowników nieorganizacyjnych zaliczają się użytkownicy systemu inni niż użytkownicy organizacyjni określeni jednoznacznie w zabezpieczeniu IA-2. Użytkownicy spoza organizacji są jednoznacznie identyfikowani i uwierzytelniani w zakresie dostępu innego niż wyraźnie określony i udokumentowany w zabezpieczeniu AC-14. Identyfikacja i uwierzytelnienie użytkowników spoza organizacji mających dostęp do systemów federacji może być wymagana w celu ochrony informacji federacji, zastrzeżonych lub związanych z prywatnością (z wyjątkami określonymi dla krajowych systemów cyberbezpieczeństwa). Organizacje biorą pod uwagę wiele czynników - w tym bezpieczeństwo, prywatność, skalowalność i praktyczność - przy równoważeniu potrzeby zapewnienia łatwości dostępu do informacji i systemów federacji z potrzebą ochrony i odpowiedniego ograniczenia ryzyka.

Zabezpieczenia powiązane: AC-2, AC-6, AC-14, AC-17, AC-18, AU-6, IA-2, IA-4, IA-5, IA-10, IA-11, MA-4, RA-3, SA-4, SC-8.

Zabezpieczenia rozszerzone:

(1) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI) | AKCEPTACJA POŚWIADCZEŃ TOŻSAMOŚCI WYDANYCH PRZEZ INNE ORGANIZACJE

Akceptacja i elektroniczna weryfikacja danych identyfikacyjnych karty dostępowej przedstawicieli innych organizacji.

Omówienie:[48] Akceptacja poświadczeń weryfikacji danych identyfikacyjnych karty dostępowej przedstawicieli innych organizacji ma zastosowanie zarówno do logicznych, jak i fizycznych systemów kontroli dostępu. Poświadczenia PIV to

[48] Omówienie dotyczy rynku USA.

poświadczenia wydane przez agencje federalne, które są zgodne z publikacją FIPS nr 201 i dodatkowymi wytycznymi. Adekwatność i wiarygodność wystawców kart PIV są przedmiotem rozważań i autoryzacji przy użyciu [NIST SP 800-79-2].

Zabezpieczenia powiązane: PE-3.

(2) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI) | AKCEPTACJA POŚWIADCZEŃ STRON TRZECICH[49]

(a) Akceptowanie wyłącznie zewnętrznych podmiotów uwierzytelniających, spełniających wymogi NIST; oraz

(b) Dokumentowanie i prowadzenie wykazu akceptowanych zewnętrznych podmiotów uwierzytelniających.

Omówienie: Akceptacja wyłącznie zewnętrznych podmiotów uwierzytelniających spełniających wymagania NIST dotyczy systemów organizacyjnych, które są dostępne publicznie (np. strony internetowe skierowane do społeczeństwa). Zewnętrzne uwierzytelnienia są wydawane przez niefederalne podmioty rządowe i są zgodne z [SP 800-63B]. Zatwierdzone uwierzytelnienia zewnętrzne spełniają lub przekraczają minimalne wymagania techniczne, bezpieczeństwa, prywatności i dojrzałości organizacyjnej obowiązujące na poziomie Rządu Federalnego. Spełnienie lub przekroczenie wymogów federalnych pozwala stronom ufającym administracji federalnej na zaufanie zewnętrznym podmiotom uwierzytelniającym w związku z transakcją uwierzytelniania na określonym poziomie wiarygodności podmiotu uwierzytelniającego.

Zabezpieczenia powiązane: Brak.

[49] Dotyczy rynku USA.

(3) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI) | WYKORZYSTANIE CERTYFIKOWANYCH PRODUKTÓW

[Wycofane: Włączone do IA-8(2)]

(4) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI) | WYKORZYSTANIE PROFILI WYDAWANYCH PRZEZ STOSOWNE INSTYTUCJE

Przestrzeganie następujących profili zarządzania tożsamością [*Realizacja*: profile zarządzania tożsamością zdefiniowane przez organizację].

Omówienie: Organizacje definiują profile zarządzania tożsamością w oparciu o otwarte standardy zarządzania tożsamością. Aby zapewnić, że standardy zarządzania otwartą tożsamością są wykonalne, solidne, niezawodne, trwałe i interoperacyjne, jak udokumentowano, organizacja ocenia i określa zakres standardów i wdrożeń technologicznych w odniesieniu do obowiązujących przepisów prawa, rozporządzeń, dyrektyw, polityk, regulacji, standardów i wytycznych.

Zabezpieczenia powiązane: Brak.

(5) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI) | AKCEPTACJA POŚWIADCZEŃ OSOBISTEJ WERYFIKACJI TOŻSAMOŚCI[50]

Akceptacja i weryfikacja poświadczeń osobistej weryfikacji tożsamości, które spełniają [*Realizacja: polityka określona przez organizację*].

Omówienie: Akceptacja poświadczeń osobistej weryfikacji tożsamości może być realizowana przez komercyjnych lub zewnętrznych dostawców tożsamości.

Akceptacja poświadczeń PIV-I może być realizowana przez PIV, PIV-I oraz innych komercyjnych lub zewnętrznych dostawców tożsamości. Akceptacja i weryfikacja danych uwierzytelniających zgodnych z PIV-I ma zastosowanie zarówno do

[50] Dotyczy rynku USA.

logicznych, jak i fizycznych systemów kontroli dostępu. Akceptacja i weryfikacja poświadczeń PIV-I dotyczy niefederalnych wydawców dowodów tożsamości, którzy chcą współpracować z systemami PIV rządu Stanów Zjednoczonych i którym mogą zaufać strony ufające rządowi federalnemu. Polityka certyfikatów X.509 dla Federal Bridge Certification Authority (FBCA) odnosi się do wymagań PIV-I. Karta PIV-I jest współmierna do danych uwierzytelniających PIV, jak określono w cytowanych źródłach. Poświadczenia PIV-I są poświadczeniami wydawanymi przez dostawcę PIV-I, którego polityka certyfikatów PIV-I odwzorowuje politykę certyfikatów Federal Bridge PIV-I. Dostawca PIV-I posiada certyfikat krzyżowy z FBCA (bezpośrednio lub poprzez inny most PKI) obejmujący polityki, które zostały zmapowane i zatwierdzone, jako spełniające wymagania reguł PIV-I zdefiniowane w polityce certyfikacji FBCA.

Zabezpieczenia powiązane: Brak.

(6) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI) | NIEPOŁĄCZALNOŚĆ (DEZASOCJACYJNOŚĆ)

Wdrożenie następujących środków mających na celu rozdzielenie atrybutów użytkownika lub relacji między osobami, dostawcami usług uwierzytelniających i stronami ufającymi: [***Realizacja: środki określone przez organizację***]**.**

Omówienie: Rozwiązania oparte na tożsamości federacyjnej mogą stwarzać zwiększone ryzyko dla prywatności z powodu śledzenia i profilowania osób. Stosowanie tabel odwzorowania identyfikatorów lub technik kryptograficznych w celu ukrycia dostawców usług uwierzytelniania i stron ufających przed sobą nawzajem lub w celu uczynienia atrybutów tożsamości mniej widocznymi dla stron przekazujących, może zmniejszyć te zagrożenia prywatności.

Zabezpieczenia powiązane: Brak.

Referencje: [OMB A-130], [FED PKI], [FIPS 201-2], [NIST SP 800-63-3], [NIST SP 800-79-2], [NIST SP 800-116], [IR 8062].

IA-9 IDENTYFIKACJA I UWIERZYTELNIANIE USŁUG

Zabezpieczenie podstawowe: Unikalna identyfikacja i uwierzytelnianie [*Realizacja: usługi i aplikacje systemowe zdefiniowane przez organizację*] przed nawiązaniem komunikacji z urządzeniami, użytkownikami lub innymi usługami lub aplikacjami.

Omówienie: Usługi, które mogą wymagać identyfikacji i uwierzytelniania, obejmują aplikacje internetowe wykorzystujące certyfikaty cyfrowe lub usługi albo aplikacje zapytujące o bazę danych. Metody identyfikacji i uwierzytelniania dla usług i aplikacji systemowych obejmują podpisywanie informacji lub kodów, wykresy danych źródłowych i podpisy elektroniczne wskazujące źródła usług. Decyzje dotyczące ważności wniosków o identyfikację i uwierzytelnienie mogą być podejmowane przez usługi odrębne od usług działających na podstawie tych decyzji. Może to mieć miejsce w rozproszonych architekturach systemowych. W takich sytuacjach decyzje dotyczące identyfikacji i uwierzytelniania (zamiast faktycznych identyfikatorów i danych uwierzytelniających) są dostarczane do usług, które muszą działać na podstawie tych decyzji.

Zabezpieczenia powiązane: IA-3, IA-4, IA-5, SC-8.

Zabezpieczenia rozszerzone:

(1) IDENTYFIKACJA I UWIERZYTELNIANIE USŁUG | WYMIANA INFORMACJI

[Wycofane: Włączone do IA-9].

(2) IDENTYFIKACJA I UWIERZYTELNIANIE USŁUG | PRZEKAZYWANIE DECYZJI O POZYTYWNEJ IDENTYFIKACJI I UWIERZYTELNIENIU

[Wycofane: Włączone do IA-9].

Referencje: Brak.

IA-10 UWIERZYTELNIANIE ADAPTACYJNE

Zabezpieczenie podstawowe: Wymaganie, aby osoby mające dostęp do systemu stosowały [Realizacja: *określone przez organizację dodatkowe techniki lub mechanizmy uwierzytelniania*] w określonych [*Realizacja: określone przez organizację okoliczności lub sytuacje*].

Omówienie: Adwersarze mogą naruszać indywidualne mechanizmy uwierzytelniania stosowane przez organizacje, a następnie próbować podszywać się pod legalnych użytkowników. Aby przeciwdziałać temu zagrożeniu, organizacje mogą stosować określone techniki lub mechanizmy i tworzyć protokoły do oceny podejrzanego zachowania. Podejrzane zachowanie może polegać na uzyskiwaniu dostępu do informacji, do których osoby zazwyczaj nie mają dostępu w ramach swoich obowiązków, ról lub odpowiedzialności; uzyskiwaniu dostępu do większej ilości informacji niż te, do których osoby miałyby rutynowo dostęp; lub na próbach uzyskania dostępu do informacji z podejrzanych adresów sieciowych. W przypadku wystąpienia uprzednio ustalonych warunków lub czynników wyzwalających, organizacje mogą wymagać od osób dostarczenia dodatkowych informacji uwierzytelniających. Innym potencjalnym zastosowaniem uwierzytelniania adaptacyjnego jest zwiększenie siły mechanizmu opartego na liczbie lub rodzajach rekordów, do których uzyskuje się dostęp. Uwierzytelnianie adaptacyjne nie zastępuje i nie jest stosowane w celu uniknięcia stosowania mechanizmów uwierzytelniania wieloskładnikowego, ale może wspierać implementacje uwierzytelniania wieloskładnikowego.

Zabezpieczenia powiązane: IA-2, IA-8.

Zabezpieczenia rozszerzone: Brak.

Referencje: [NIST SP 800-63-3].

IA-11 PONOWNE UWIERZYTELNIENIE

Zabezpieczenie podstawowe: Wymaganie od użytkowników ponownego uwierzytelnienia w przypadku wystąpienia [*Realizacja: okoliczności lub sytuacje określone przez organizację, wymagające ponownego uwierzytelnienia*].

Omówienie: Oprócz wymagań dotyczących ponownego uwierzytelniania związanych z blokadami urządzeń, organizacje mogą wymagać ponownego uwierzytelnienia osób w pewnych sytuacjach, w tym w przypadku zmiany ról, podmiotów uwierzytelniających lub danych uwierzytelniających, zmiany kategorii zabezpieczeń systemów, wykonywania funkcji uprzywilejowanych, po określonym czasie lub okresowo.

Zabezpieczenia powiązane: AC-3, AC-11, IA-2, IA-3, IA-4, IA-8.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

IA-12 POTWIERDZENIE TOŻSAMOŚCI

Zabezpieczenie podstawowe:

a. Sprawdzanie tożsamości użytkowników, którzy wymagają kont do logicznego dostępu do systemów w oparciu o odpowiednie wymagania dotyczące poziomu zapewnienia tożsamości, zgodnie z obowiązującymi normami i wytycznymi;

b. Rozwiązywanie problemów związanych z identyfikacją użytkownika dla konkretnej osoby; oraz

c. Zbieranie, zatwierdzanie i weryfikacja dowodów tożsamości.

Omówienie: Sprawdzanie tożsamości to proces zbierania, walidacji i weryfikacji informacji o tożsamości użytkownika w celu ustalenia uprawnień dostępu do systemu. Sprawdzanie tożsamości ma na celu zmniejszenie zagrożeń podczas rejestracji użytkowników i zakładania ich kont. Normy i wytyczne określające poziomy gwarancji tożsamości w odniesieniu do potwierdzania tożsamości obejmują np. [NIST SP 800-63-3] i [NIST SP 800-63A]. Organizacje podlegają przepisom, zarządzeniom wykonawczym, dyrektywom, rozporządzeniom lub zasadom, które dotyczą gromadzenia dowodów tożsamości. Personel organizacji konsultuje się SAOP[51] i radcą prawnym w sprawie takich wymagań.

Zabezpieczenia powiązane: AC-5, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-8.

Zabezpieczenia rozszerzone:

(1) POTWIERDZENIE TOŻSAMOŚCI | AUTORYZACJA PRZEŁOŻONEGO

Wymaganie, aby proces rejestracji w celu otrzymania konta dostępu logicznego obejmował autoryzację przełożonego lub sponsora systemu.

Omówienie: Włączenie autoryzacji przełożonego lub sponsora, jako części procesu rejestracji, zapewnia dodatkowy poziom weryfikacji w celu zapewnienia,

[51] Patrz: NSC 800-37; NSC 7298.

że łańcuch zarządzania użytkownikiem jest informowany o koncie, konto jest niezbędne do realizacji misji i funkcji organizacyjnych, a uprawnienia użytkownika są odpowiednie do przewidywanego zakresu odpowiedzialności i uprawnień w organizacji.

Zabezpieczenia powiązane: Brak.

(2) POTWIERDZENIE TOŻSAMOŚCI | DOWODZENIE TOŻSAMOŚCI

Wymaganie przedstawienia organowi rejestracyjnemu dowodu identyfikacji osobistej.

Omówienie: Dowody tożsamości, takie jak dokumenty dowodowe lub połączenie dokumentów i danych biometrycznych, zmniejszają prawdopodobieństwo wykorzystania fałszywej identyfikacji w celu ustalenia tożsamości lub przynajmniej zwiększają nakład pracy potencjalnych przeciwników. Formy akceptowalnych dowodów są zgodne z zagrożeniami dla systemów, ról i przywilejów związanych z kontem użytkownika.

Zabezpieczenia powiązane: Brak.

(3) POTWIERDZANIE TOŻSAMOŚCI | POTWIERDZANIE I WERYFIKACJA DOWODÓW TOŻSAMOŚCI

Wymaganie potwierdzania i weryfikacji przedstawionych dowodów tożsamości poprzez [***Realizacja: określone organizacyjnie metody potwierdzania i weryfikacji***]**.**

Omówienie: Potwierdzanie i weryfikacja dowodów tożsamości zwiększa pewność, że konta i identyfikatory są tworzone dla właściwego użytkownika, a podmioty uwierzytelniające są z nim związane. Potwierdzenie odnosi się do procesu identyfikacji, że dowody są prawdziwe i autentyczne, a dane zawarte w dowodach są prawidłowe, aktualne i związane z osobą. Weryfikacja potwierdza i ustala związek między deklarowaną tożsamością, a rzeczywistym istnieniem użytkownika przedstawiającego dowody. Dopuszczalne metody potwierdzania

i weryfikacji dowodów tożsamości są zgodne z zagrożeniami dla systemów, ról i przywilejów związanych z kontem użytkownika.

Zabezpieczenia powiązane: Brak.

(4) POTWIERDZANIE TOŻSAMOŚCI | OSOBISTE ZATWIERDZENIE I WERYFIKACJA

Wymaganie, aby potwierdzenie i weryfikacja dowodów tożsamości były przeprowadzane osobiście przed wyznaczonym organem rejestracyjnym.

Omówienie: Osobiste potwierdzanie tożsamości zmniejsza prawdopodobieństwo wystawienia fałszywych poświadczeń, ponieważ wymagana jest fizyczna obecności osób, przedstawienia fizycznych dokumentów tożsamości oraz rzeczywistych kontaktów twarzą w twarz z wyznaczonymi organami rejestracyjnymi.

Zabezpieczenia powiązane: Brak.

(5) POTWIERDZENIE TOŻSAMOŚCI | POTWIERDZENIE ADRESU

Wymaganie, aby [***Wybór: kod rejestracyjny; zawiadomienie o potwierdzeniu odbioru***] ***zostało*** **dostarczone „poza pasmem" w celu weryfikacji adresu użytkownika (fizycznego lub cyfrowego).**

Omówienie: W celu utrudnienia adwersarzom podawania się za prawowitych użytkowników podczas procesu potwierdzania tożsamości, organizacje mogą stosować metody „poza pasmem", aby upewnić się, że osoba powiązana z zarejestrowanym adresem jest tą samą osobą, która uczestniczyła w rejestracji. Potwierdzenie może przybrać formę tymczasowego kodu rejestracyjnego lub powiadomienia o potwierdzeniu. Adres dostawy dla tych artefaktów jest uzyskiwany z rejestrów, a niepodawany samodzielnie przez użytkownika. Adres może obejmować adres fizyczny lub cyfrowy. Przykładem adresu fizycznego jest adres domowy. Adresy e-mail i numery telefonów są przykładami adresów cyfrowych.

Zabezpieczenia powiązane: IA-12.

(6) POTWIERDZANIE TOŻSAMOŚCI | AKCEPTACJA ZEWNETRZNYCH TOŻSAMOŚCI

Akceptowanie zewnętrznie potwierdzonych tożsamości na [[***Realizacja: poziom zapewnienia tożsamości zdefiniowany przez organizację***]**.**

Omówienie: W celu ograniczenia zbędnego ponownego sprawdzania tożsamości, w szczególności użytkowników nie będących użytkownikami kart identyfikacyjnych, organizacje akceptują sprawdzanie przeprowadzone na odpowiednim poziomie wiarygodności przez inne organizacje. Weryfikacja jest zgodna z polityką bezpieczeństwa organizacji i poziomem zapewnienia tożsamości właściwym dla systemu, aplikacji lub udostępnianych informacji. Akceptacja zewnętrznie sprawdzonych tożsamości jest podstawowym elementem zarządzania tożsamością federacyjną we wszystkich organizacjach.

Zabezpieczenia powiązane: IA-3, IA-4, IA-5, IA-8.

Referencje: [FIPS 201-2], [NIST SP 800-63-3], [NIST SP 800-63A], [NIST SP 800-79-2].

KATEGORIA IR - REAGOWANIE NA INCYDENTY

IR-1 POLITYKA I PROCEDURY

Zabezpieczenie podstawowe:

a. Opracowywanie, dokumentowanie i rozpowszechnianie wśród [Realizacja: *personel lub role określone przez organizację*]:

1. [*Wybór (jeden lub więcej): poziom organizacji; poziom misji/procesu biznesowego; poziom systemu*] polityki reagowania na incydenty, która:

(a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami; oraz

(b) Jest zgodna z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi; oraz

2. Procedur ułatwiających wdrożenie polityki reagowania na incydenty oraz powiązanych zabezpieczeń w zakresie reagowania na incydenty;

b. Wyznaczanie [Realizacja: *osoba wyznaczona przez organizację*] do zarządzania rozwojem, dokumentacją i rozpowszechnianiem polityki i procedur reagowania na incydenty; oraz

c. Przeglądanie i aktualizacja bieżącej:

1. Polityki reagowania na incydenty z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*]; oraz

2. Procedur reagowania na incydenty z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*].

Omówienie: Polityka i procedury w zakresie reagowania na incydenty dotyczą zabezpieczeń w kategorii *Reagowanie na incydenty* (IR), które są wdrażane w ramach systemów i organizacji. Strategia zarządzania ryzykiem jest ważnym czynnikiem przy

tworzeniu takich polityk i procedur. Polityki i procedury przyczyniają się do zapewnienia bezpieczeństwa i ochrony prywatności. Dlatego ważne jest, aby programy bezpieczeństwa i ochrony prywatności były opracowywane wspólnie przy kształtowaniu polityki i procedur reagowania na incydenty. Polityki i procedury dotyczące programów bezpieczeństwa i ochrony prywatności na poziomie organizacji są ogólnie rzecz biorąc preferowane i mogą eliminować potrzeby tworzenia polityk i procedur specyficznych dla danej misji lub systemu. Polityka może być włączona, jako część ogólnej polityki bezpieczeństwa i ochrony prywatności lub reprezentowana przez wiele polityk odzwierciedlających złożony charakter organizacji. Procedury mogą być ustanowione dla programów bezpieczeństwa i ochrony prywatności, dla misji lub procesów biznesowych oraz dla systemów, jeśli to konieczne. Procedury opisują sposób wdrażania zasad lub zabezpieczeń i mogą być skierowane do osoby lub roli, która jest przedmiotem procedury. Procedury mogą być udokumentowane w planach bezpieczeństwa i ochrony prywatności systemu w jednym lub kilku oddzielnych dokumentach.

Zdarzenia, które mogą spowodować konieczność aktualizacji polityki i procedur reagowania na incydenty, obejmują wyniki oceny lub audytu, incydenty lub naruszenia bezpieczeństwa, lub zmiany w przepisach prawa, zarządzeniach, dyrektywach, rozporządzeniach, zasadach, standardach i wytycznych.

Oświadczenie o wprowadzeniu zabezpieczeń nie jest równoznaczne z ustanowieniem polityki lub procedury organizacyjnej.

Zabezpieczenia powiązane: PM-9, PS-8, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [NIST SP 800-12], [NIST SP 800-30], [NIST SP 800-39], [NIST SP 800-50], [NIST SP 800-61], [NIST SP 800-83], [NIST SP 800-100].

IR-2 SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY

Zabezpieczenie podstawowe:

a. Zapewnienie użytkownikom systemu szkolenia w zakresie reagowania na incydenty zgodnie z przydzielonymi im rolami i obowiązkami:

   1. W ciągu [*Realizacja: określony przez organizację okres czasu*] od przejęcia roli lub obowiązków w zakresie reagowania na incydenty lub uzyskania dostępu do systemu;

   2. W przypadku wystąpienia zmian w systemie; oraz

   3. Cyklicznie [*Realizacja: częstotliwość określona przez organizację*]; oraz

b. Przegląda i aktualizuje treści szkolenia dotyczącego reagowania na incydenty [Realizacja: *częstotliwość określona przez organizację*] i następujące po nim [*Realizacja: zdarzenia określone przez organizację*].

Omówienie: Szkolenie w zakresie reagowania na incydenty jest powiązane z przypisanymi rolami i obowiązkami personelu organizacyjnego i ma na celu zapewnienie, że w takim szkoleniu uwzględnione są odpowiednie treści i poziom szczegółowości. Na przykład, użytkownicy mogą potrzebować jedynie informacji o tym, do kogo zadzwonić lub jak rozpoznać incydent; administratorzy systemu mogą wymagać dodatkowego szkolenia na temat obsługi incydentów; osoby reagujące na incydenty mogą przejść bardziej szczegółowe szkolenie z zakresu kryminalistyki, technik gromadzenia danych, raportowania, odzyskiwania i przywracania systemu. Ćwiczenia dotyczące reagowania na incydenty obejmują szkolenia użytkowników w zakresie identyfikowania i zgłaszania podejrzanych działań pochodzących ze źródeł zewnętrznych i wewnętrznych. Szkolenie w zakresie reagowania na incydenty przeznaczone dla użytkowników może być przeprowadzone w ramach zabezpieczenia AT-2 lub AT-3. Zdarzenia, które mogą spowodować aktualizację treści szkolenia w zakresie reagowania na incydenty, obejmują między innymi testowanie planu reagowania na incydenty lub reakcję na rzeczywisty incydent (wnioski wyciągnięte

z dotychczasowych doświadczeń), wyniki oceny i audytu lub zmiany w obowiązujących przepisach prawa, rozporządzeniach wykonawczych, dyrektywach, regulacjach, politykach, standardach i wytycznych.

Zabezpieczenia powiązane: AT-2, AT-3, AT-4, CP-3, IR-3, IR-4, IR-8, IR-9.

Zabezpieczenia rozszerzone:

(1) SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY | WYDARZENIA SYMULOWANE

Włączenie symulowanych zdarzeń do szkolenia w zakresie reagowania na incydenty w celu umożliwienia skutecznej reakcji personelu w sytuacjach kryzysowych.

Omówienie: Organizacje ustalają wymagania dotyczące reagowania na incydenty w planach reagowania na incydenty. Włączenie symulowanych zdarzeń do szkolenia w zakresie reagowania na incydenty pomaga zapewnić, że personel rozumie swoje indywidualne obowiązki i jakie konkretne działania należy podjąć w sytuacjach kryzysowych.

Zabezpieczenia powiązane: Brak.

(2) SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY | ZAUTOMATYZOWANE ŚRODOWISKA SZKOLENIOWE

Zapewnienie środowiska szkoleniowego w zakresie reagowania na incydenty przy użyciu [***Realizacja: zdefiniowane przez organizacje zautomatyzowane mechanizmy***]**.**

Omówienie: Zautomatyzowane mechanizmy mogą zapewnić bardziej dokładne i realistyczne środowisko szkoleniowe w zakresie reagowania na incydenty. Można to osiągnąć na przykład poprzez zapewnienie pełniejszego zakresu zagadnień związanych z reagowaniem na incydenty, wybór bardziej realistycznych scenariuszy i środowisk szkoleniowych oraz podkreślenie zdolności reagowania.

Zabezpieczenia powiązane: Brak.

(3) SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY | NARUSZENIE

Zapewnienie szkolenia w zakresie reagowania na incydenty dotyczące sposobu identyfikacji i reagowania na naruszenia, w tym procesu zgłaszania naruszeń przez organizację.

Omówienie: Incydent, który wiąże się z danymi osobowymi, jest uznawany za naruszenie. Naruszenie skutkuje utratą zabezpieczeń, naruszeniem zasad ochrony/kompromitacją, nieautoryzowanym ujawnieniem, nieautoryzowanym przejęciem lub podobnym zdarzeniem, gdy osoba inna niż autoryzowany użytkownik uzyskuje dostęp lub potencjalnie uzyskuje dostęp do danych osobowych; lub autoryzowany użytkownik uzyskuje dostęp lub potencjalnie uzyskuje dostęp do takich informacji w celach innych niż autoryzowane. Szkolenie w zakresie reagowania na incydenty kładzie nacisk na obowiązek zgłaszania zarówno potwierdzonych, jak i podejrzewanych naruszeń dotyczących informacji w dowolnym nośniku lub formie, w tym papierowej, ustnej i elektronicznej. Szkolenie w zakresie reagowania na incydenty obejmuje ćwiczenia na stole, które symulują naruszenie (patrz: zabezpieczenie IR-2(1).

Zabezpieczenia powiązane: Brak.

Referencje: [OMB M-17-12], [NIST SP 800-50].

IR-3 TESTOWANIE REAGOWANIA NA INCYDENTY

Zabezpieczenie podstawowe: Testowanie skuteczności reakcji systemu na incydenty [*Realizacja: częstotliwość zdefiniowana przez organizację*] *przy* użyciu następujących testów: [Realizacja: *testy określone przez organizację*].

Omówienie: Organizacje testują możliwości reagowania na incydenty, aby określić ich skuteczność i zidentyfikować potencjalne słabe punkty lub braki. Testowanie reakcji na incydenty obejmuje wykorzystanie list zabezpieczeń, ćwiczeń przechodzenia lub ćwiczeń na stole oraz symulacji (równoległych lub pełnych). Testowanie reakcji na incydent może obejmować określenie wpływu reakcji na działania organizacyjne oraz na zasoby i osoby w związku z incydentem. Wykorzystanie jakościowych i ilościowych danych pomaga w określaniu skuteczności procesów reagowania na incydenty.

Zabezpieczenia powiązane: CP-3, CP-4, IR-2, IR-4, IR-8, PM-14.

Zabezpieczenia rozszerzone:

(1) TESTOWANIE REAGOWANIA NA INCYDENTY | AUTOMATYCZNE TESTOWANIE

Testowanie zdolności reagowania na incydenty przy użyciu [***Realizacja: automatyczne mechanizmy zdefiniowane przez organizację***]**.**

Omówienie: Organizacje wykorzystują zautomatyzowane mechanizmy do dokładniejszego i skuteczniejszego testowania możliwości reagowania na incydenty. Można to osiągnąć poprzez pełniejsze uwzględnienie kwestii związanych z reagowaniem na incydenty, wybór realistycznych scenariuszy i środowisk testowych oraz obciążanie możliwości reagowania.

Zabezpieczenia powiązane: Brak.

(2) TESTOWANIE REAGOWANIA NA INCYDENTY | KOORDYNACJA Z POWIĄZANYMI PLANAMI

Koordynacja testów reakcji na incydenty z jednostkami organizacyjnymi odpowiedzialnymi za powiązane plany.

Omówienie: Plany organizacyjne związane z testowaniem reagowania na incydenty obejmują plany ciągłości działania, plany odtworzenia po katastrofie, plany kontynuacji operacji, plany awaryjne, plany komunikacji kryzysowej, plany infrastruktury krytycznej oraz plany ewakuacji.

Zabezpieczenia powiązane: Brak.

(3) TESTOWANIE REAGOWANIA NA INCYDENTY | CIĄGŁE DOSKONALENIE

Wykorzystywanie danych jakościowych i ilościowych z badań do:

(a) Określania skuteczności procesów reagowania na incydenty;

(b) Ciągłego doskonalenia procesów reagowania na incydenty; oraz

(c) Zapewnienia dokładnych, spójnych i powtarzalnych pomiarów i metryk reakcji na incydenty.

Omówienie: W celu usprawnienia funkcjonowania działań związanych z reagowaniem na incydenty, organizacje mogą stosować metryki i kryteria oceny do oceny programów reagowania na incydenty w ramach działań mających na celu ciągłą poprawę wyników reagowania. Wysiłki te ułatwiają poprawę skuteczności reagowania na incydenty i zmniejszają ich wpływ.

Zabezpieczenia powiązane: Brak.

Referencje: [OMB A-130], [NIST SP 800-84], [NIST SP 800-115].

IR-4 OBSŁUGA INCYDENTÓW

Zabezpieczenie podstawowe:

a. Wdrożenie zdolności do obsługi incydentów, która jest zgodna z planem reagowania na incydenty i obejmuje przygotowanie, wykrywanie i analizę, powstrzymywanie, zwalczanie i odzyskiwanie;

b. Koordynowanie działań związanych z obsługą incydentów z działaniami planowania awaryjnego;

c. Włączanie wniosków wyciągniętych z bieżących działań związanych z obsługą incydentów do procedur reagowania na incydenty, szkoleń i testów, a następnie odpowiednie wdrażanie wynikających z nich zmian; oraz

d. Zapewnienie, że rygor, intensywność, zakres i wyniki działań związanych z obsługą incydentów są porównywalne i przewidywalne w całej organizacji.

Omówienie: Organizacje zdają sobie sprawę, że możliwości reagowania na incydenty są zależne od funkcjonalności systemów organizacyjnych oraz misji i procesów biznesowych, które są wspierane przez te systemy. Organizacje biorą pod uwagę reagowanie na incydenty, jako część definicji, projektowania i rozwoju misji oraz procesów i systemów biznesowych. Informacje na temat incydentów można uzyskać z różnych źródeł, w tym z monitoringu audytów, monitoringu dostępu fizycznego i sieci, raportów użytkowników lub administratorów oraz raportów dotyczących zdarzeń w łańcuchu dostaw. Efektywna zdolność do obsługi incydentów obejmuje koordynację pomiędzy wieloma jednostkami organizacyjnymi (np. właścicielami misji lub firm, właścicielami systemów, osobami autoryzującymi, biurami zasobów ludzkich, biurami bezpieczeństwa fizycznego, biurami ochrony personelu, działami prawnymi, funkcję wykonawczą ds. ryzyka (RE)[52], personelem operacyjnym, biurami ds. zamówień). Podejrzane incydenty bezpieczeństwa

[52] Patrz: NSC 800-37; NSC 7298.

obejmują otrzymywanie budzących podejrzenia wiadomości e-mail, które mogą zawierać złośliwy kod. Podejrzane incydenty w łańcuchu dostaw obejmują wprowadzenie podrobionego sprzętu lub złośliwego kodu do systemów organizacyjnych lub komponentów systemu. Incydent, który obejmuje dane osobowe, jest uznawany za naruszenie. Naruszenie skutkuje nieautoryzowanym ujawnieniem, utratą zabezpieczeń, nieautoryzowanym przejęciem, narażeniem na szwank lub podobnym zdarzeniem, gdy osoba inna niż autoryzowany użytkownik uzyskuje dostęp lub potencjalnie uzyskuje dostęp do informacji umożliwiających identyfikację osób lub autoryzowany użytkownik uzyskuje dostęp lub potencjalnie uzyskuje dostęp do takich informacji w celach innych niż autoryzowane.

Zabezpieczenia powiązane: AC-19, AU-6, AU-7, CM-6, CP-2, CP-3, CP-4, IR-2, IR-3, IR-5, IR-6, IR-8, PE-6, PL-2, PM-12, SA-8, SC-5, SC-7, SI-3, SI-4, SI-7.

Zabezpieczenia rozszerzone:

(1) OBSŁUGA INCYDENTÓW | AUTOMATYCZNE PROCESY OBSŁUGI ZDARZEŃ

Wsparcie procesu obsługi incydentów za pomocą [***Realizacja: organizacyjnie zdefiniowane zautomatyzowane mechanizmy***]**.**

Omówienie: Zautomatyzowane mechanizmy wspierające procesy obsługi incydentów obejmują systemy zarządzania incydentami online oraz narzędzia wspierające zbieranie danych o reakcjach na żywo, pełne przechwytywanie pakietów sieciowych oraz analizę kryminalistyczną.

Zabezpieczenia powiązane: Brak.

(2) OBSŁUGA INCYDENTÓW | DYNAMICZNA REKONFIGURACJA

Włączenie następujących rodzajów dynamicznej rekonfiguracji [***Realizacja: zdefiniowane przez organizację komponenty systemu***]**, jako część zdolności reagowania na incydent:** [***Realizacja: zdefiniowane przez organizację typy dynamicznej rekonfiguracji***]**.**

Omówienie: Dynamiczna rekonfiguracja obejmuje zmiany reguł routera, list kontroli dostępu, parametrów systemu wykrywania i zapobiegania włamaniom oraz reguł filtrowania dla strażników bezpieczeństwa lub zapór sieciowych. Organizacje mogą przeprowadzać dynamiczną rekonfigurację systemów w celu powstrzymania ataków, niewłaściwego ukierunkowania napastników oraz odizolowania komponentów systemów, ograniczając w ten sposób zakres szkód wynikających z naruszenia lub kompromitacji. W definicji zdolności do rekonfiguracji organizacje uwzględniają określone ramy czasowe na przeprowadzenie rekonfiguracji systemów, biorąc pod uwagę potencjalną potrzebę szybkiej reakcji w celu skutecznego przeciwdziałania cyberzagrożeniom.

Zabezpieczenia powiązane: AC-2, AC-4, CM-2.

(3) OBSŁUGA INCYDENTÓW | CIĄGŁOŚĆ OPERACJI

Zidentyfikowanie [***Realizacja: zdefiniowane przez organizację kategorie incydentów***] **i podjęcie następujących działań w odpowiedzi na te incydenty, aby zapewnić kontynuację misji organizacyjnej i funkcji biznesowych:** [***Realizacja: zdefiniowane przez organizację działania, które należy podjąć w odpowiedzi na zaistniałe kategorie incydentów***]**.**

Omówienie: Kategorie incydentów obejmują awarie spowodowane błędami i przeoczeniami projektowymi lub wdrożeniowymi, celowymi złośliwymi atakami oraz niecelowymi złośliwymi atakami. Działania podejmowane w odpowiedzi na incydent obejmują uporządkowaną degradację systemu, wyłączenie systemu, powrót do trybu ręcznego lub aktywację alternatywnej technologii, z powodu których system działa w sposób odmienny, stosując środki pozorowane, zmienne przepływy informacji lub działając w trybie zarezerwowanym dla sytuacji, gdy systemy są atakowane. Organizacje rozważają, czy wymagania dotyczące ciągłości działania podczas incydentu nie stoją w sprzeczności z możliwością automatycznego wyłączenia systemu, jak określono w zabezpieczeniu IR-4(5).

Zabezpieczenia powiązane: Brak.

(4) OBSŁUGA INCYDENTÓW | KORELACJA INFORMACJI

Korelowanie informacji o incydentach i indywidualnych reakcji na incydenty w celu osiągnięcia szerokiej perspektywy w zakresie świadomości i reakcji na incydenty.

Omówienie: Czasami zdarzenie zagrażające, takie jak wrogie cyberataki, można zaobserwować jedynie poprzez zebranie informacji z różnych źródeł, w tym różnych raportów i procedur sprawozdawczych ustanowionych przez organizacje.

Zabezpieczenia powiązane: Brak.

(5) OBSŁUGA INCYDENTÓW | AUTOMATYCZNE WYŁĄCZANIE SYSTEMU

Zaimplementowanie konfigurowalnej zdolności do automatycznego wyłączania systemu w przypadku wykrycia [***Realizacja: naruszenie bezpieczeństwa zdefiniowane przez organizację***]**.**

Omówienie: Organizacje rozważają, czy możliwość automatycznego wyłączenia systemu koliduje z wymaganiami dotyczącymi ciągłości działania określonymi w ramach zabezpieczeń CP-2 lub IR-4(3). Naruszenia bezpieczeństwa obejmują cyberataki, które spowodowały kompromitację integralności systemu lub eksfiltrację informacji organizacyjnych oraz poważne błędy w oprogramowaniu, które mogą mieć negatywny wpływ na misje lub funkcje organizacji lub zagrażać bezpieczeństwu osób.

Zabezpieczenia powiązane: Brak.

(6) OBSŁUGA INCYDENTÓW | ZAGROŻENIA WEWNĘTRZNE

Wdrożenie zdolności do obsługi incydentów związanych z zagrożeniami wewnętrznymi.

Omówienie: Skoncentrowanie się w sposób szczególny na obsłudze incydentów związanych z zagrożeniami wewnętrznymi stanowi dodatkowy element podkreślający ten rodzaj zagrożenia oraz konieczność posiadania odpowiednich

zdolności obsługi incydentów w celu zapewnienia odpowiedniej i terminowej reakcji.

Zabezpieczenia powiązane: Brak.

(7) OBSŁUGA INCYDENTÓW | ZAGROŻENIA WEWNĘTRZNE - KOORDYNACJA WEWNĄTRZ ORGANIZACJI

Koordynacja zdolności do obsługi incydentów w zakresie zagrożeń wewnętrznych, która obejmuje następujące podmioty organizacyjne [***Realizacja: podmioty zdefiniowane przez organizację***]**.**

Omówienie: Obsługa incydentów związanych z zagrożeniami wewnętrznymi (np. przygotowanie, wykrywanie i analiza, powstrzymywanie, eliminowanie i usuwanie) wymaga koordynacji działań wielu podmiotów organizacyjnych, w tym właścicieli misji lub firm, właścicieli systemów, biur zasobów ludzkich, biur zaopatrzenia, biur kadrowych, biur bezpieczeństwa fizycznego, personelu operacyjnego, SAISO, RE (funkcja), SAOP[53] i radcy prawnego. Ponadto organizacje mogą wymagać wsparcia zewnętrznego ze strony organów ścigania.

Zabezpieczenia powiązane: Brak.

(8) OBSŁUGA INCYDENTÓW | KOORDYNACJA Z ORGANIZACJAMI ZEWNĘTRZNYMI

Koordynowanie z [***Realizacja: organizacje zewnętrzne zdefiniowane przez organizację***] ***w*** **celu korelowania i dzielenia się** [***Realizacja: informacje o incydentach zdefiniowane przez organizację***] **w celu zbudowania szerokiej międzyorganizacyjnej świadomości dotyczącej incydentów i bardziej efektywnych reakcji na incydenty.**

Omówienie: Koordynacja informacji o incydentach z organizacjami zewnętrznymi - w tym z partnerami misyjnymi lub biznesowymi, wojskowymi lub koalicyjnymi,

[53] Patrz: NSC 800-37; NSC 7298.

klientami i deweloperami - może przynieść znaczące korzyści w zakresie poprawy bezpieczeństwa. Koordynacja międzyorganizacyjna może służyć jako istotna zdolność zarządzania ryzykiem. Zdolność ta pozwala organizacjom na wykorzystanie informacji z różnych źródeł w celu skutecznego reagowania na incydenty i naruszenia, które mogą potencjalnie wpłynąć na działalność organizacji, jej aktywa i osoby.

Zabezpieczenia powiązane: AU-16, PM-16.

(9) OBSŁUGA INCYDENTÓW | ZDOLNOŚĆ DO REAGOWANIA DYNAMICZNEGO

Stosowanie [***Realizacja: funkcje dynamicznego reagowania zdefiniowane przez organizację***] **w celu reagowania na incydenty.**

Omówienie: Zdolność dynamicznego reagowania dotyczy terminowego wdrażania nowych lub zastępczych możliwości organizacyjnych w odpowiedzi na incydenty. Obejmuje to funkcje wdrażane na poziomie misji i procesów biznesowych oraz na poziomie systemu.

Zabezpieczenia powiązane: Brak.

(10) OBSŁUGA INCYDENTÓW | KOORDYNACJA ŁAŃCUCHA DOSTAW

Koordynowanie działań związanych z obsługą incydentów dotyczących zdarzeń w łańcuchu dostaw z innymi organizacjami zaangażowanymi w łańcuch dostaw.

Omówienie: Organizacje zaangażowane w działania związane z łańcuchem dostaw obejmują twórców produktów, integratorów systemów, producentów, pakowaczy, monterów, dystrybutorów, sprzedawców i reselerów. Incydenty w łańcuchu dostaw mogą występować w dowolnym miejscu w obrębie łańcucha dostaw i obejmują kompromitacje lub naruszenia, które dotyczą dostawców podstawowych lub niższego szczebla, produktów informatycznych, komponentów systemów, procesów rozwoju lub personelu oraz procesów dystrybucji lub obiektów magazynowych. Organizacje rozważają włączenie

procesów ochrony i udostępniania informacji o incydentach do umów o wymianie informacji oraz ich obowiązków w zakresie zgłaszania incydentów do właściwych CSITR[54] (CSIRT GOV, CSIR MON, CSIR NASK).

Zabezpieczenia powiązane: CA-3, MA-2, SA-9, SR-8.

(11) OBSŁUGA INCYDENTÓW | ZINTEGROWANY ZESPÓŁ REAGOWANIA NA INCYDENTY

Ustanowienie i utrzymanie zintegrowanego zespołu reagowania na incydenty, który może podjąć działania w dowolnym miejscu określonym przez organizację przez [***Realizacja: okres czasu określony przez organizację***]**.**

Omówienie: Zintegrowany zespół reagowania na incydenty to zespół ekspertów, którzy oceniają, dokumentują i reagują na incydenty, aby systemy i sieci organizacyjne mogły szybko powrócić do normalnego funkcjonowania i wdrażają niezbędne zabezpieczenia w celu uniknięcia przyszłych incydentów. Zespół reagowania na incydenty składa się z analityków kryminalistycznych i analityków złośliwego kodu, programistów narzędzi, SPO i SSO[55] oraz personel operacyjny działający w czasie rzeczywistym. Zdolność obsługi incydentów obejmuje szybkie kryminalistyczne zabezpieczanie dowodów oraz analizę i reagowanie na włamania. W niektórych organizacjach, zespół reagowania na incydenty może być jednostką międzyorganizacyjną.

Zintegrowany zespół reagowania na incydenty ułatwia wymianę informacji i pozwala personelowi organizacyjnemu (np. programistom, wdrożeniowcom i operatorom) wykorzystać wiedzę zespołu o zagrożeniu i wdrożyć środki ochronne, które umożliwiają organizacjom skuteczniejsze powstrzymywanie włamań. Ponadto, zintegrowane zespoły promują szybkie wykrywanie włamań,

[54] CSIRT (Computer Security Incident Response Team) - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego

[55] Patrz: NSC 800-37; NSC 7298.

opracowywanie odpowiednich środków zaradczych oraz wdrażanie skutecznych środków obronnych. Na przykład, w przypadku wykrycia włamania zintegrowany zespół może szybko opracować odpowiednią reakcję operatorów w celu wdrożenia, skorelowania nowego incydentu z informacjami o włamaniach mających miejsce w przeszłości oraz rozszerzenia bieżącego rozwoju cyberprzestrzeni. Zintegrowane zespoły reagowania na incydenty są w stanie lepiej rozpoznawać taktykę, techniki i procedury przeciwników, które są powiązane z tempem operacji lub określonymi zadaniami i funkcjami biznesowymi, a także określać działania reagujące w sposób, który nie zakłóca tych zadań i funkcji biznesowych. Zespoły reagowania na incydenty mogą być rozmieszczone w obrębie organizacji, aby zwiększyć ich odporność.

Zabezpieczenia powiązane: AT-3.

(12) OBSŁUGA INCYDENTÓW | ANALIZA KRYMINALISTYCZNA ZŁOŚLIWEGO KODU

Analizowanie złośliwego kodu i/lub innych artefaktów pozostających w systemie po zdarzeniu.

Omówienie: Analiza złośliwego kodu i innych artefaktów po incydencie lub naruszeniu bezpieczeństwa, przeprowadzona ostrożnie w odizolowanym środowisku, może dać organizacji wgląd w taktykę, techniki i procedury przeciwnika. Może również wskazywać na tożsamość lub pewne cechy definiujące przeciwnika. Ponadto, analiza złośliwego kodu może pomóc organizacji w opracowaniu reakcji na przyszłe incydenty.

Zabezpieczenia powiązane: Brak.

(13) OBSŁUGA INCYDENTÓW | ANALIZA ZACHOWAŃ

Analizowanie anormalnych lub podejrzanych zachowań w / lub związanych z [***Realizacja: środowiska lub zasoby zdefiniowane przez organizację***]**.**

Omówienie: Jeśli organizacja utrzymuje środowisko przechwytujące, analiza zachowań w tym środowisku, w tym zasobów będących celem ataku przeciwnika

oraz czasu wystąpienia incydentu lub zdarzenia, może zapewnić wgląd w taktykę, techniki i procedury przeciwnika. Poza środowiskiem przechwytywania, analiza anomalnych zachowań przeciwnika (np. zmiany w wydajności systemu lub wzorców użytkowania) lub podejrzanych zachowań (np. zmiany w wyszukiwaniu lokalizacji określonych zasobów) może dać organizacji ogólny pogląd o zachowaniu przeciwnika.

Zabezpieczenia powiązane: Brak.

(14) OBSŁUGA INCYDENTÓW | OPERACYJNE CENTRUM BEZPIECZEŃSTWA (SOC)

Założenie i utrzymanie operacyjnego centrum bezpieczeństwa (*SOC*).

Omówienie: Operacyjne centrum bezpieczeństwa (*ang. Security Operations Center - SOC*) jest punktem centralnym dla operacji bezpieczeństwa i obrony sieci komputerowej dla organizacji. Celem SOC jest stała ochrona i monitorowanie systemów i sieci organizacji (tj. infrastruktury cyberbezpieczeństwa). SOC jest również odpowiedzialny za wykrywanie, analizowanie i reagowanie w odpowiednim czasie na incydenty związane z cyberbezpieczeństwem. Organizacja zatrudnia w SOC wykwalifikowany personel techniczny i operacyjny (np. analityków bezpieczeństwa, pracowników zajmujących się reagowaniem na incydenty, inżynierów bezpieczeństwa systemów) i wdraża połączenie zabezpieczeń technicznych, zarządczych i operacyjnych (w tym narzędzi monitorowania, skanowania i kryminalistycznych) w celu monitorowania, zabezpieczania, korelowania, analizowania i reagowania na dane o zagrożeniach i zdarzeniach istotnych dla bezpieczeństwa pochodzące z wielu źródeł. Źródła te obejmują systemy zabezpieczeń granic akredytacji systemu, urządzenia sieciowe (np. routery, przełączniki) oraz wprowadzanie danych do agenta końcowego. SOC zapewnia holistyczną świadomość sytuacyjną, która pomaga organizacjom w określaniu pozycji bezpieczeństwa systemu i organizacji. Funkcjonalność SOC można uzyskać na wiele różnych sposobów. Większe organizacje mogą posiadać

dedykowany SOC, podczas gdy mniejsze mogą korzystać z usług zewnętrznych organizacji, które zapewniają takie możliwości.

Zabezpieczenia powiązane: Brak.

(15) OBSŁUGA INCYDENTÓW | RELACJE PUBLICZNE I NAPRAWA REPUTACJI

(a) Zarządzanie relacjami publicznymi związanymi z incydentem; oraz

(b) Stosowanie środków mających na celu poprawę reputacji organizacji.

Omówienie: Ważne jest, aby organizacja posiadała strategię reagowania na incydenty, które przyciągnęły uwagę opinii publicznej, postawiły organizację w negatywnym świetle lub wpłynęły na jej otoczenie (np. partnerów, klientów). Taki rozgłos może być niezwykle szkodliwy dla organizacji i wpływać na jej zdolność do realizacji misji i funkcji biznesowych. Podjęcie proaktywnych kroków w celu naprawy reputacji organizacji jest istotnym aspektem odbudowy zaufania i pewności siebie jej interesariuszy.

Zabezpieczenia powiązane: Brak.

Referencje: [FASC18], [41 CFR 201], [OMB M-17-12], [NIST SP 800-61], [NIST SP 800-86], [NIST SP 800-101], [NIST SP 800-150], [NIST SP 800-160-2], [NIST SP 800-184], [IR 7559].

IR-5 MONITOROWANIE INCYDENTÓW

Zabezpieczenie podstawowe: Śledzenie i dokumentowanie incydentów.

Omówienie: Dokumentowanie incydentów obejmuje prowadzenie dokumentacji dotyczącej każdego incydentu, statusu incydentu oraz innych istotnych informacji niezbędnych dla postępowania wyjaśniającego, jak również ocenę szczegółów, tendencji i sposobu postępowania z incydentem. Informacje o incydentach można uzyskać z różnych źródeł, w tym z monitoringu sieci, raportów o incydentach, zespołów reagowania na incydenty, skarg użytkowników, partnerów z łańcucha dostaw, monitoringu audytów, monitoringu dostępu fizycznego oraz raportów użytkowników i administratorów. Zabezpieczenie IR-4 dostarcza informacji na temat rodzajów incydentów, które są przeznaczone do monitorowania.

Zabezpieczenia powiązane: AU-6, AU-7, IR-4, IR-6, IR-8, PE-6, PM-5, SC-5, SC-7, SI-3, SI-4, SI-7.

Zabezpieczenia rozszerzone:

(1) MONITOROWANIE INCYDENTÓW | AUTOMATYCZNE ŚLEDZENIE, ZBIERANIE DANYCH I ANALIZA

Śledzenie incydentów oraz zbieranie i analizowanie informacji o incydentach przy użyciu [***Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację***]**.**

Omówienie: Zautomatyzowane mechanizmy śledzenia incydentów oraz zbierania i analizowania informacji o incydentach obejmują właściwy CSIRT lub inne elektroniczne bazy danych o incydentach oraz urządzenia do monitorowania sieci.

Zabezpieczenia powiązane: brak.

Referencje: [NIST SP 800-61].

IR-6 ZGŁASZANIE INCYDENTÓW

Zabezpieczenie podstawowe:

a. Wymaganie od personelu zgłaszania podejrzanych incydentów do odpowiednich komórek zarządzania incydentami w ciągu [*Realizacja: okres czasu określony przez organizację*]*;* oraz

b. Zgłaszanie informacji o incydentach do [*Realizacja: właściwy CSIRT zdefiniowany przez organizację*].

Omówienie: Rodzaje zgłaszanych incydentów, treść i terminowość zgłoszeń oraz właściwy CSIRT zdefiniowany przez organizację odzwierciedlają obowiązujące przepisy, zarządzenia, dyrektywy, rozporządzenia, zasady, standardy i wytyczne. Informacje o incydentach mogą stanowić źródło informacji na temat oceny ryzyka, oceny skuteczności zabezpieczeń, wymogów bezpieczeństwa w procesie zakupów oraz kryteriów wyboru produktów technologicznych.

Zabezpieczenia powiązane: CM-6, CP-2, IR-4, IR-5, IR-8, IR-9.

Zabezpieczenia rozszerzone:

(1) ZGŁASZANIE INCYDENTÓW | ZGŁASZANIE AUTOMATYCZNE

Zgłaszanie incydentów przy użyciu [***Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację***]**.**

Omówienie: Odbiorcy raportów z incydentów są określeni w zabezpieczeniu IR-6b. Zautomatyzowane mechanizmy raportowania obejmują pocztę elektroniczną, zamieszczanie na stronach internetowych (z automatycznymi aktualizacjami) oraz zautomatyzowane narzędzia i programy do reagowania na incydenty.

Zabezpieczenia powiązane: IR-7.

(2) ZGŁASZANIE INCYDENTÓW | PODATNOŚĆ NA INCYDENTY

Powiadamianie o podatności systemu (luki w zabezpieczeniach) powiązanej ze zgłaszanym incydentem do [***Realizacja: personel lub role określone przez organizację***]**.**

Omówienie: Zgłaszane incydenty, które ujawniają luki w zabezpieczeniach systemu, są analizowane przez personel organizacji, w tym właścicieli systemów, właścicieli misji i firm, SAISO, SAOP, AO, i RE.[56] Analiza może posłużyć do ustalenia priorytetów i zainicjowania działań łagodzących skutki wykrytej podatności systemu.

Zabezpieczenia powiązane: Brak.

(3) ZGŁASZANIE INCYDENTÓW | KOORDYNACJA ŁAŃCUCHA DOSTAW

Dostarczanie informacji o incydencie dostawcy produktu lub usługi oraz innym organizacjom uczestniczącym w łańcuchu dostaw lub zarządzaniu łańcuchem dostaw w odniesieniu do systemów lub komponentów systemu powiązanych z incydentem.

Omówienie: Organizacje zaangażowane w działania uczestniczące w łańcuchu dostaw obejmują twórców produktów, integratorów systemów, producentów, pakowaczy, monterów, dystrybutorów, sprzedawców i resellerów. Podmiotami zapewniającymi zarządzanie łańcuchem dostaw są między innymi Federalna Rada Bezpieczeństwa Przejęć (Federal Acquisition Security Council - FASC).[57] Incydenty w łańcuchu dostaw obejmują kompromitacje lub naruszenia, które dotyczą produktów informatycznych, komponentów systemów, procesów rozwoju lub personelu, procesów dystrybucji lub obiektów magazynowych. Organizacje określają, jakimi informacjami mogą się dzielić i biorą pod uwagę

[56] Patrz: NSC 800-37; NSC 7298.

[57] Dotyczy rynku USA.

wartość wynikającą z informowania organizacji zewnętrznych o incydentach w łańcuchu dostaw, w tym możliwość poprawy procesów lub zidentyfikowania pierwotnej przyczyny incydentu.

Zabezpieczenia powiązane: SR-8.

Referencje: [FASC18], [41 CFR 201], [USCERT IR], [NIST SP 800-61].

IR-7 WSPARCIE REAGOWANIA NA INCYDENTY

Zabezpieczenie podstawowe: Zapewnienie zasobów wsparcia w zakresie reagowania na incydenty, stanowiących integralną część organizacyjnych możliwości reagowania na incydenty, oferujących porady i pomoc dla użytkowników systemu w zakresie obsługi i zgłaszania incydentów.

Omówienie: Zasoby wsparcia w zakresie reagowania na incydenty zapewniane przez organizacje obejmują centra pomocy, grupy wsparcia, zautomatyzowane systemy zgłoszeń służące do otwierania i śledzenia zgłoszeń w zakresie reagowania na incydenty oraz dostęp do usług kryminalistycznych lub usług dochodzenia roszczeń konsumentów, jeśli jest to wymagane.

Zabezpieczenia powiązane: AT-2, AT-3, IR-4, IR-6, IR-8, PM-22, PM-26, SA-9, SI-18.

Zabezpieczenia rozszerzone:

(1) WSPARCIE REAGOWANIA NA INCYDENTY | AUTOMATYCZNE WSPARCIE DOSTĘPNOŚCI INFORMACJI / OBSŁUGI

Zwiększenie dostępności informacji i wsparcia w zakresie reagowania na incydenty przy użyciu [***Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację***]**.**

Omówienie: Zautomatyzowane mechanizmy mogą zapewniać użytkownikom możliwość uzyskania pomocy w zakresie reagowania na incydenty w trybie "push" lub "pull". Na przykład, osoby mogą mieć dostęp do strony internetowej, aby zadać pytanie komórce ds. pomocy, lub komórka ds. pomocy może proaktywnie wysyłać informacje o reagowaniu na incydenty do użytkowników (dystrybucja ogólna lub ukierunkowana) w ramach zwiększania zrozumienia bieżących możliwości reagowania i wsparcia.

Zabezpieczenia powiązane: Brak.

(2) WSPARCIE REAGOWANIA NA INCYDENTY | KOORDYNACJA Z DOSTAWCAMI ZEWNĘTRZNYMI

(a) Ustanowienie bezpośredniego, opartego na współpracy związku między własną zdolnością reagowania na incydenty, a zewnętrznymi dostawcami środków ochrony systemu; oraz

(b) Wskazanie zewnętrznym dostawcom członków zespołu reagowania na incydenty.

Omówienie: Zewnętrzni dostawcy środków ochrony pomagają chronić, monitorować, analizować, wykrywać i reagować na nieautoryzowane działania w ramach organizacyjnych systemów informatycznych i sieci. Korzystne może być zawarcie umów z zewnętrznymi dostawcami w celu wyjaśnienia ról i obowiązków każdej ze stron przed wystąpieniem incydentu.

Zabezpieczenia powiązane: Brak.

Referencje: [OMB A-130], [IR 7559].

IR-8 PLAN REAGOWANIA NA INCYDENTY

Zabezpieczenie podstawowe:

a. Opracowanie planu reagowania na incydenty, który:

1. Dostarcza organizacji strategię dotyczącą wdrażania zdolności reagowania na incydenty;
2. Opisuje strukturę i organizację zdolności reagowania na incydenty;
3. Zapewnia ogólne podejście do tego, jak zdolność reagowania na incydenty wpisuje się w ogólne ramy działalności organizacji;
4. Spełnia unikalne wymagania organizacji, które odnoszą się do misji, wielkości, struktury i funkcji;
5. Definiuje incydenty podlegające zgłoszeniu;
6. Dostarcza metryki do pomiaru zdolności reagowania na incydenty w organizacji;
7. Określa zasoby i wsparcie zarządzania potrzebne do skutecznego utrzymania zdolności reagowania na incydenty;
8. Uwzględnia kwestię wymiany informacji o incydentach;
9. Jest weryfikowany i zatwierdzany przez [*Realizacja: personel lub role określone przez organizację*] [*Realizacja: częstotliwość określona przez organizację*]*;* oraz
10. Jednoznacznie określa odpowiedzialność za reakcję na incydent [*Realizacja: podmioty określone przez organizację, personel lub role*].

b. Dystrybuuje kopie planu reagowania na incydenty do [*Realizacja: personel reagujący na incydenty zdefiniowany przez organizację (identyfikowany na podstawie nazwy i/lub roli) oraz elementy organizacyjne*]*;*

c. Aktualizuje plan reagowania na incydenty w celu uwzględnienia zmian systemowych i organizacyjnych lub problemów napotkanych podczas wdrażania, realizacji lub testowania planu;

d. Informuje o zmianach w planie reagowania na incydent [*Realizacja: personel reagujący na incydenty zdefiniowany przez organizację (identyfikowany na podstawie nazwy i/lub roli) oraz elementy organizacyjne*]; oraz

e. Chroni plan reagowania na incydenty przed nieautoryzowanym ujawnieniem i modyfikacją.

Omówienie: Ważne jest, aby organizacje opracowały i wdrożyły skoordynowane podejście do reagowania na incydenty. Misja organizacyjna i funkcje biznesowe determinują strukturę możliwości reagowania na incydenty. W ramach możliwości reagowania na incydenty organizacje rozważają koordynację i dzielenie się informacjami z zewnętrznymi organizacjami, w tym z zewnętrznymi dostawcami usług i innymi organizacjami zaangażowanymi w łańcuch dostaw. W przypadku incydentów dotyczących informacji umożliwiających identyfikację osób (tj. naruszeń), należy uwzględnić proces mający na celu ustalenie, czy powiadomienie organizacji nadzorujących lub osób, których dotyczy dany incydent, jest właściwe i odpowiednio dostarczyć to powiadomienie.

Zabezpieczenia powiązane: AC-2, CP-2, CP-4, IR-4, IR-7, IR-9, PE-6, PL-2, SA-15, SI-12, SR-8.

Zabezpieczenia rozszerzone:

(1) PLAN REAGOWANIA NA INCYDENTY | NARUSZENIA

W planie reagowania na incydenty, w przypadku naruszeń dotyczących danych osobowych, należy uwzględnić następujące elementy:

(a) Proces mający na celu ustalenie, czy konieczne jest powiadomienie osób lub innych organizacji, w tym organizacji nadzorujących;

(b) Proces oceny w celu określenia zakresu szkody, zamętu, niedogodności lub nieuczciwości w stosunku do osób poszkodowanych oraz wszelkich mechanizmów łagodzących takie szkody; oraz

(c) Określenie obowiązujących wymogów w zakresie ochrony prywatności.

Omówienie: Prawo, przepisy lub polityka mogą wymagać od organizacji przestrzegania określonych procedur związanych z naruszeniami, w tym powiadamiania osób, organizacji i organów nadzoru, których one dotyczą, standardów dotyczących szkód oraz łagodzenia skutków lub innych szczególnych wymagań.

Zabezpieczenia powiązane: PKT-1, PKT-2, PKT-3, PT-4, PT-5, PT-7.

Referencje: [OMB A-130], [NIST SP 800-61], [OMB M-17-12].

IR-9 REAKCJA NA WYCIEK / UJAWNIENIE INFORMACJI

Zabezpieczenie podstawowe: Reagowanie na wycieki informacji poprzez:

a. Wyznaczenie [*Realizacja: personel lub role określone przez organizację*] rozliczanego za reagowanie na wycieki informacji;

b. Identyfikację specyficznych informacji mających ujemny wpływ na system;

c. Ostrzeganie [*Realizacja: personel lub role określone przez organizację*] o wycieku informacji, przy użyciu metody komunikacji niezwiązanej z wyciekiem;

d. Izolowanie „zakażonego" systemu lub komponentu systemu;

e. Eliminowanie informacji z „zakażonego" systemu lub komponentu systemu;

f. Identyfikowanie innych systemów lub komponentów systemu, które mogły zostać „zakażone" w przyszłości; oraz

g. Wykonywanie innych dodatkowych czynności: [*Realizacja: działania zdefiniowane przez organizację*].

Omówienie: Wyciek informacji odnosi się do przypadków, w których informacje są umieszczane w systemach, które nie są upoważnione do przetwarzania takich informacji. Wyciek informacji ma miejsce, gdy informacja mającą określoną klauzulę niejawności lub zdefiniowany poziom wpływu została przekazana do systemu przetwarzającego informacje o tym samym poziomie wpływu (klauzuli niejawności), a następnie okazuje się, że posiada wyższą klauzulę niejawności lub wyższy poziom wpływu (jest przetwarzana w systemie nieautoryzowanym do przetwarzania takiej klasyfikacji/poziomu wpływu). W tym momencie konieczne jest podjęcie działań naprawczych. Charakter reakcji jest uzależniony od poziomu klauzuli lub wpływu informacji, które uległy "wyciekowi", zabezpieczeń systemu, szczególnego charakteru „skażonych" nośników informacji oraz uprawnień dostępu osób posiadających autoryzowany wgląd do „skażonego" systemu. Metody stosowane do przekazywania informacji o wycieku po fakcie nie obejmują metod bezpośrednio związanych

z faktycznym wyciekiem w celu zminimalizowania ryzyka dalszego rozprzestrzeniania się „skażenia", zanim takie „skażenie" zostanie wyizolowane i wyeliminowane.

Zabezpieczenia powiązane: CP-2, IR-6, PM-26, PM-27, PT-2, PT-3, PT-7, RA-7.

Zabezpieczenia rozszerzone:

(1) REAKCJA NA WYCIEK / UJAWNIENIE INFORMACJI | ODPOWIEDZIALNY PERSONEL

[Wycofane: Włączone do IR-9].

(2) REAKCJA NA WYCIEK / UJAWNIENIE INFORMACJI | SZKOLENIE

Zapewnienie szkolenia w zakresie reagowania na wycieki informacji [***Realizacja: częstotliwość określona przez organizację***]**.**

Omówienie: Organizacje ustanawiają wymagania dotyczące reagowania na incydenty związane z wyciekiem informacji w planach reagowania na incydenty. Regularne szkolenia w zakresie reagowania na incydenty pomagają zapewnić, że personel organizacji jest świadomy swoich indywidualnych obowiązków i rozumie, jakie konkretne działania należy podjąć w przypadku wystąpienia incydentów związanych z wyciekiem.

Zabezpieczenia powiązane: AT-2, AT-3, CP-3, IR-2.

(3) REAKCJA NA WYCIEK / UJAWNIENIE INFORMACJI | DZIAŁANIA PO UJAWNIENIU

Wdrożenie [***Realizacja: procedury określone przez organizację***] **w celu zapewnienia, że personel organizacyjny dotknięty skutkami wycieku informacji może nadal wykonywać przydzielone mu zadania, podczas gdy „skażone" systemy są poddawane działaniom naprawczym.**

Omówienie: Działania naprawcze w przypadku systemów „skażonych" w wyniku wycieku informacji mogą być czasochłonne. Personel może nie mieć dostępu do „skażonych" systemów w trakcie podejmowania działań naprawczych, co może potencjalnie wpłynąć na jego zdolność do prowadzenia działalności.

Zabezpieczenia powiązane: Brak.

(4) REAKCJA NA WYCIEK / UJAWNIENIE INFORMACJI | WYSTAWIENIE NA DZIAŁANIA OSÓB NIEAUTORYZOWANYCH

Stosowanie [*Realizacja: procedury ochrony bezpieczeństwa zdefiniowane przez organizację*] wobec personelu uzyskującego dostęp do informacji, zapoznanie z którymi nie mieści się w przydzielonych im uprawnieniach dostępu.

Omówienie: Zabezpieczenie obejmuje upewnienie się, że pracownicy narażeni na wycieki informacji są zaznajomieni z przepisami, dyrektywami, rozporządzeniami, polityką, standardami i wytycznymi dotyczącymi informacji i ograniczeniami nałożonymi w związku z narażeniem na wyciek informacji.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

IR-10 ZINTEGROWANY ZESPÓŁ DS. ANALIZY BEZPIECZEŃSTWA INFORMACJI

[Wycofane: Włączone do IR-4(11).]

KATEGORIA MA – UTRZYMANIE I WSPARCIE

MA-1 POLITYKA I PROCEDURY

Zabezpieczenie podstawowe:

a. Opracowywanie, dokumentowanie i rozpowszechnianie wśród [Realizacja: *personel lub role określone przez organizację*]:

   1. [*Wybór (jeden lub więcej): poziom organizacji; poziom misji/procesu biznesowego; poziom systemu*] polityki utrzymania i wsparcia, która:

      (a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami; oraz

      (b) Jest zgodna z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi; oraz

   2. Procedur ułatwiających wdrożenie polityki utrzymania i wsparcia oraz powiązanych zabezpieczeń w zakresie utrzymania i wsparcia;

b. Wyznaczanie [Realizacja: *osoba wyznaczona przez organizację*] do zarządzania rozwojem, dokumentacją i rozpowszechnianiem polityki i procedur utrzymania i wsparcia; oraz

c. Przeglądanie i aktualizacja bieżącej:

   1. Polityki utrzymania i wsparcia z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*]; oraz

   2. Procedur utrzymania i wsparcia z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*].

Omówienie: Polityka i procedury w zakresie utrzymania i wsparcia dotyczą zabezpieczeń w kategorii *Utrzymanie i wsparcie* (MA), które są wdrażane w ramach systemów i organizacji. Strategia zarządzania ryzykiem jest ważnym czynnikiem przy

tworzeniu takich polityk i procedur. Polityki i procedury przyczyniają się do zapewnienia bezpieczeństwa i ochrony prywatności. Dlatego ważne jest, aby programy bezpieczeństwa i ochrony prywatności były opracowywane wspólnie przy kształtowaniu polityki i procedur utrzymania i wsparcia. Polityki i procedury dotyczące programów bezpieczeństwa i ochrony prywatności na poziomie organizacji są ogólnie rzecz biorąc preferowane i mogą eliminować potrzeby tworzenia polityk i procedur specyficznych dla danej misji lub systemu. Polityka może być włączona, jako część ogólnej polityki bezpieczeństwa i ochrony prywatności lub reprezentowana przez wiele polityk odzwierciedlających złożony charakter organizacji. Procedury mogą być ustanowione dla programów bezpieczeństwa i ochrony prywatności, dla misji lub procesów biznesowych oraz dla systemów, jeśli to konieczne. Procedury opisują sposób wdrażania zasad lub zabezpieczeń i mogą być skierowane do osoby lub roli, która jest przedmiotem procedury. Procedury mogą być udokumentowane w planach bezpieczeństwa i ochrony prywatności systemu w jednym lub kilku oddzielnych dokumentach.

Zdarzenia, które mogą spowodować konieczność aktualizacji polityki i procedur utrzymania i wsparcia, obejmują wyniki oceny lub audytu, incydenty lub naruszenia bezpieczeństwa, lub zmiany w przepisach prawa, zarządzeniach, dyrektywach, rozporządzeniach, zasadach, standardach i wytycznych.

Oświadczenie o wprowadzeniu zabezpieczeń nie jest równoznaczne z ustanowieniem polityki lub procedury organizacyjnej.

Zabezpieczenia powiązane: PM-9, PS-8, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [NIST SP 800-12], [NIST SP 800-30], [NIST SP 800-39], [NIST SP 800-100].

MA-2 NADZÓR NAD UTRZYMANIEM

Zabezpieczenie podstawowe:

a. Planowanie, dokumentowanie i przeglądanie dokumentacji dotyczącej konserwacji, napraw i wymiany komponentów systemu zgodnie ze specyfikacją producenta lub sprzedawcy i/lub wymogami organizacyjnymi;

b. Zatwierdzanie i monitorowanie wszystkich czynności związanych z utrzymaniem, niezależnie od tego, czy są one wykonywane na miejscu, czy zdalnie oraz czy system lub jego komponenty są serwisowane na miejscu lub przenoszone do innej lokalizacji;

c. Wymaganie, aby [*Realizacja: personel lub role zdefiniowane przez organizację*] zatwierdzał usunięcie systemu lub komponentów systemu z obiektów organizacyjnych w celu konserwacji lub naprawy lub wymiany poza terenem obiektu;

d. Usuwanie poniższych informacji z powiązanych mediów przed przeniesieniem z pomieszczeń organizacyjnych w celu dokonania konserwacji, wymiany lub napraw poza siedzibą: [*Realizacja: informacje określone przez organizację*]*;*

e. Sprawdzenie wszystkich potencjalnych naruszeń środków bezpieczeństwa, celem określenia poprawności działania tych zabezpieczeń po przeprowadzonych czynnościach związanych z utrzymaniem, naprawą lub; oraz

f. Włączanie następujących informacji do dokumentacji technicznej organizacji: [*Realizacja: informacje określone przez organizację*].

Omówienie: Nadzór nad utrzymaniem systemu dotyczy aspektów bezpieczeństwa informacji objętych programem konserwacji systemu i odnosi się do wszystkich rodzajów konserwacji komponentów systemu przeprowadzanych lokalnie lub zdalnie. Utrzymanie i wsparcie obejmuje urządzenia peryferyjne, takie jak skanery, kopiarki i drukarki. Informacje niezbędne do utworzenia skutecznej dokumentacji utrzymaniowej obejmują datę i godzinę przeprowadzenia konserwacji, opis

przeprowadzonej konserwacji, nazwiska osób lub grup przeprowadzających konserwację, nazwisko osoby towarzyszącej oraz komponenty lub urządzenia systemu, które zostały usunięte lub wymienione. Organizacje biorą pod uwagę zagrożenia związane z łańcuchem dostaw związane z wymianą części składowych systemów.

Zabezpieczenia powiązane: CM-2, CM-3, CM-4, CM-5, CM-8, MA-4, MP-6, PE-16, SI-2, SR-3, SR-4, SR-11.

Zabezpieczenia rozszerzone:

(1) NADZÓR NAD UTRZYMANIEM| ZAWARTOŚĆ REKORDU

[Wycofane: Włączone do MA-2].

(2) NADZÓR NAD UTRZYMANIEM | AUTOMATYCZNE DZIAŁANIA KONSERWACYJNE

(a) Planowanie, przeprowadzanie i dokumentowanie czynności związanych z utrzymaniem, naprawą i wymianą systemu za pomocą [***Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację***]**; oraz**

(b) Tworzenie aktualnych, szczegółowych i kompletnych rejestrów wszystkich wymaganych, zaplanowanych, realizowanych i zakończonych czynności związanych z utrzymaniem, naprawą i wymianą.

Omówienie: Wykorzystanie zautomatyzowanych mechanizmów do zarządzania i zabezpieczania programów i działań związanych z utrzymaniem systemu pomaga zapewnić terminowe, dokładne, kompletne i spójne tworzenie dokumentacji utrzymaniowej.

Zabezpieczenia powiązane: MA-3.

Referencje: [OMB A-130], [IR 8023].

MA-3 NARZĘDZIA UTRZYMANIOWE

Zabezpieczenie podstawowe:

a. Zatwierdzanie, kontrolowanie i monitorowanie użycie narzędzi do utrzymania systemu; oraz

b. Przeglądanie uprzednio zatwierdzonych narzędzi obsługi technicznej systemu [*Realizacja: częstotliwość określona przez organizację*].

Omówienie: Zatwierdzanie, kontrolowanie, monitorowanie i przegląd narzędzi serwisowych dotyczy kwestii bezpieczeństwa związanych z narzędziami serwisowymi używanymi poza granicami autoryzacji systemu i są wykorzystywane w szczególności do działań diagnostycznych i naprawczych w systemach organizacyjnych. Organizacje mają możliwość elastycznego określania ról w zakresie zatwierdzania narzędzi obsługi technicznej oraz sposobu dokumentowania tego zatwierdzenia. Okresowy przegląd narzędzi obsługi technicznej ułatwia wycofanie zatwierdzenia dla narzędzi przestarzałych, nieobsługiwanych, nieistotnych lub nieużywanych przez dłuższy czas. Narzędzia obsługi technicznej mogą obejmować sprzęt, aplikacje i oprogramowanie układowe oraz mogą być wstępnie zainstalowane, dostarczone przez personel obsługi technicznej na nośniku, przechowywane w chmurze lub pobrane ze strony internetowej. Narzędzia takie mogą służyć do przenoszenia złośliwego kodu, w sposób zamierzony lub niezamierzony, do obiektu, a następnie do systemów. Narzędzia utrzymaniowe mogą obejmować sprzęt i oprogramowanie do testowania diagnostycznego oraz sniffery pakietów. Narzędzia utrzymaniowe nie obejmują komponentów sprzętowych i programowych, które wspierają konserwację i są częścią systemu (w tym oprogramowania wdrażającego narzędzia takie jak "ping", "ls", "ipconfig" czy też sprzętu i oprogramowania wdrażającego monitorowanie portu przełącznika Ethernet).

Zabezpieczenia powiązane: MA-2, PE-16.

Zabezpieczenia rozszerzone:

(1) NARZĘDZIA UTRZYMANIOWE | SPRAWDZANIE NARZĘDZI

Sprawdzanie, czy narzędzia używane przez personel utrzymaniowy nie uległy niewłaściwym lub nieautoryzowanym modyfikacjom.

Omówienie: Narzędzia serwisowe mogą być bezpośrednio wprowadzane do obiektu przez personel serwisowy lub pobierane ze strony internetowej sprzedawcy. Jeżeli po sprawdzeniu narzędzi do obsługi technicznej organizacje stwierdzą, że narzędzia te zostały zmodyfikowane w niewłaściwy sposób lub zawierają złośliwy kod, incydent ten jest obsługiwany zgodnie z zasadami i procedurami organizacji dotyczącymi obsługi incydentów.

Zabezpieczenia powiązane: SI-7.

(2) NARZĘDZIA UTRZYMANIOWE | SPRAWDZANIE NOŚNIKÓW DANYCH

Sprawdzanie nośników zawierających programy diagnostyczne i testowe pod kątem występowania złośliwego kodu, zanim zostaną one użyte w systemie.

Omówienie: Jeżeli po kontroli mediów zawierających programy utrzymaniowe, diagnostyczne i testowe organizacje stwierdzą, że zawierają one złośliwy kod, incydent jest obsługiwany zgodnie z zasadami i procedurami obsługi incydentów organizacyjnych.

Zabezpieczenia powiązane: SI-3.

(3) NARZĘDZIA UTRZYMANIOWE | ZAPOBIEGANIE NIEAUTORYZOWANEMU USUWANIU

Zapobieganie nieautoryzowanemu usuwaniu sprzętu utrzymaniowego zawierającego informacje organizacyjne poprzez:

(a) Sprawdzenie, czy nie są w nim przechowywane żadne informacje organizacyjne;

(b) Sanityzację lub zniszczenie sprzętu;

(c) Pozostawienie sprzętu na terenie obiektu; lub

(d) Uzyskanie zwolnienia wydanego przez [***Realizacja: personel lub role określone przez organizację***] **upoważniającego do usunięcia sprzętu z obiektu.**

Omówienie: Informacje organizacyjne obejmują wszystkie informacje będące własnością organizacji oraz wszelkie informacje przekazane organizacjom i którymi organizacje władają.

Zabezpieczenia powiązane: MP-6.

(4) NARZĘDZIA UTRZYMANIOWE | OGRANICZANIE UŻYWANIA NARZĘDZI

Korzystanie z narzędzi serwisowych tylko przez upoważnione osoby.

Omówienie: Ograniczenie korzystania z narzędzi utrzymaniowych wyłącznie do autoryzowanego personelu dotyczy systemów, które są wykorzystywane do wykonywania funkcji utrzymaniowych.

Zabezpieczenia powiązane: AC-3, AC-5, AC-6.

(5) NARZĘDZIA UTRZYMANIOWE | WYKORZYSTYWANIE PODWYŻSZONYCH UPRAWNIEŃ

Monitorowanie korzystania z narzędzi serwisowych uruchamianych z dodatkowymi uprawnieniami systemowymi.

Omówienie: Uruchamianie narzędzi do obsługi techniczne ze zwiększonymi uprawnieniami systemowymi może skutkować nieautoryzowanym dostępem do informacji organizacyjnych i zasobów, które w przeciwnym razie byłyby niedostępne.

Zabezpieczenia powiązane: AC-3, AC-6.

(6) NARZĘDZIA UTRZYMANIOWE | AKTUALIZACJE I POPRAWKI OPROGRAMOWANIA

Sprawdzanie narzędzi utrzymaniowych pod kątem zainstalowania najnowszych aktualizacji i poprawek oprogramowania.

Omówienie: Narzędzia utrzymaniowe wykorzystujące nieaktualne i/lub „niezałatane" oprogramowanie mogą być wektorem zagrożeń do wykorzystania przez adwersarzy i skutkować znaczącą podatnością organizacji na ataki.

Zabezpieczenia powiązane: AC-3, AC-6.

Referencje: [EO 13556], [NIST SP 800-88].

MA-4 UTRZYMANIE ZDALNE

Zabezpieczenie podstawowe:

a. Zatwierdzanie i monitorowanie zdalnych czynności utrzymaniowych i diagnostycznych;

b. Zezwolenie na korzystanie ze zdalnych narzędzi utrzymaniowych i diagnostycznych tylko w sposób zgodny z polityką organizacyjną i udokumentowaniu w planie bezpieczeństwa systemu;

c. Stosowanie silnego uwierzytelniania przy tworzeniu zdalnych sesji utrzymaniowych i diagnostycznych;

d. Prowadzenie dokumentacji dotyczącej zdalnych czynności utrzymaniowych i diagnostycznych; oraz

e. Zamykanie sesji i połączeń sieciowych po zakończeniu czynności zdalnego utrzymania.

Omówienie: Zdalne czynności utrzymaniowe i diagnostyczne są prowadzone przez personel komunikujący się poprzez zewnętrzną lub wewnętrzną sieć. Lokalne czynności utrzymaniowe i diagnostyczne są wykonywane przez osoby obecne w miejscu lokalizacji systemu i niekomunikujące się za pośrednictwem połączenia sieciowego. Techniki uwierzytelniania stosowane w celu ustanowienia zdalnych sesji utrzymaniowych i diagnostycznych odzwierciedlają wymogi dotyczące dostępu do sieci określone w zabezpieczeniu IA-2. Silne uwierzytelnianie wymaga urządzeń uwierzytelniających, które są odporne na ataki metodą powtórzeń (ataki typu "replay") i wykorzystuje uwierzytelnianie wieloskładnikowe. Do silnych mechanizmów uwierzytelniających należy PKI, gdzie certyfikaty są przechowywane na tokenie chronionym hasłem, frazą kodującą lub biometrycznie. Wymagania stawiane przez zabezpieczenie MA-4 są realizowane częściowo poprzez inne zabezpieczenia. Publikacja [NIST SP 800-63B] zawiera dodatkowe wytyczne dotyczące silnego uwierzytelniania i jednostek uwierzytelniających.

Zabezpieczenia powiązane: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, PL-2, SC-7, SC-10.

Zabezpieczenia rozszerzone:

(1) UTRZYMANIE ZDALNE | AUDYT I PRZEGLĄD

a) Prowadzenie audytu [*Realizacja: zdarzenia kontrolne zdefiniowane przez organizację*] zdalnych sesji utrzymania i diagnostyki; oraz

b) Dokonywanie przeglądów zapisów z audytów sesji utrzymaniowych i diagnostycznych w celu wykrycia anomalii.

Omówienie: Prowadzenie audytów zdalnej obsługi technicznej jest egzekwowane przez zabezpieczenie AU-2. Zdarzenia związane z audytem są określone w zabezpieczeniu AU-2a.

Zabezpieczenia powiązane: AU-6, AU-12.

(2) UTRZYMANIE ZDALNE | DOKUMENTY ZDALNEGO UTRZYMANIA

[Wycofane: Włączone do MA-1, MA-4].

(3) UTRZYMANIE ZDALNE | PORÓWNYWALNE POZIOMY BEZPIECZEŃSTWA / SANITYZACJA

(a) Wymaganie, aby zdalne usługi utrzymaniowe i diagnostyczne były wykonywane z systemu, który realizuje funkcje bezpieczeństwa porównywalną z funkcją wdrożoną w obsługiwanym systemie; lub

(b) Usuwanie serwisowanych komponentów z systemu przed przeprowadzeniem czynności zdalnego utrzymania lub diagnostyki; dokonywanie sanityzacji komponentu (w odniesieniu do informacji organizacyjnych); a po wykonaniu usługi, sprawdzenie i sanityzacja komponentu (w odniesieniu do potencjalnego złośliwego oprogramowania) przed ponownym podłączeniem komponentu do systemu.

Omówienie: Porównywalne możliwości w zakresie bezpieczeństwa systemów, narzędzi diagnostycznych i sprzętu do przeprowadzania usług utrzymaniowych oznaczają, że wdrożone środki bezpieczeństwa tych systemów, narzędzi i sprzętu są co najmniej tak samo kompleksowe, jak zabezpieczenia serwisowanego systemu.

Zabezpieczenia powiązane: MP-6, SI-3, SI-7.

(4) UTRZYMANIE ZDALNE | UWIERZYTELNIANIE / SEPARACJA SESJI UTRZYMANIOWYCH

Chronienie zdalnych sesji utrzymaniowych poprzez:

(a) Stosowanie [***Realizacja: zdefiniowanego przez organizację uwierzytelniania, które jest odporne na odtwarzanie***]**; oraz**

(b) Oddzielanie sesji utrzymaniowych od innych połączeń sieciowych z systemem poprzez:

(1) Fizycznie odseparowane ścieżki komunikacyjne; lub

(2) Logicznie rozdzielone ścieżki komunikacyjne.

Omówienie: Ścieżki komunikacyjne mogą być logicznie oddzielone za pomocą szyfrowania.

Zabezpieczenia powiązane: Brak.

(5) UTRZYMANIE ZDALNE | ZGODY I POWIADOMIENIA

(a) Wymaganie zatwierdzania każdej zdalnej sesji utrzymaniowej przez [***Realizacja: personel lub role określone przez organizację***]**; oraz**

(b) Powiadamianie: [*Realizacja: personel lub role określone przez organizację*] o dacie i godzinie planowanej zdalnej obsługi technicznej.

Omówienie: Zgłoszenie może być dokonane przez personel obsługi technicznej. Zatwierdzenie zdalnej obsługi technicznej jest dokonywane przez personel posiadający wystarczającą wiedzę na temat bezpieczeństwa informacji i systemu,

aby określić zasadność proponowanych do przeprowadzenia czynności utrzymaniowych.

Zabezpieczenia powiązane: Brak.

(6) UTRZYMANIE ZDALNE | OCHRONA KRYPTOGRAFICZNA

Wdrożenie następujących mechanizmów kryptograficznych w celu ochrony integralności i poufności transmisji zdalnego utrzymania i diagnostyki: [***Realizacja: zdefiniowane organizacyjnie mechanizmy kryptograficzne***].

Omówienie: Brak ochrony zdalnej komunikacji serwisowej i diagnostycznej może spowodować, że osoby nieupoważnione uzyskają dostęp do informacji organizacyjnych. Nieautoryzowany dostęp podczas sesji zdalnego utrzymania może skutkować różnymi wrogimi działaniami, w tym złośliwym wstawianiem kodu, nieautoryzowanymi zmianami parametrów systemu oraz eksfiltracją informacji organizacyjnych. Takie działania mogą prowadzić do utraty lub degradacji misji lub możliwości biznesowych.

Zabezpieczenia powiązane: SC-8, SC-12, SC-13.

(7) UTRZYMANIE ZDALNE | ZDALNA WERYFIKACJA ZAKOŃCZENIA SESJI

Weryfikacja zakończenia sesji i połączenia sieciowego po zakończeniu zdalnych sesji utrzymaniowych i diagnostycznych.

Omówienie: Weryfikacja zakończenia połączenia po zakończeniu konserwacji zapewnia, że połączenia nawiązane podczas zdalnych sesji utrzymaniowych i diagnostycznych zostały zakończone i nie są już dostępne do użytku.

Zabezpieczenia powiązane: AC-12.

Referencje: [FIPS 140-3], [FIPS 197], [FIPS 201-2], [NIST SP 800-63-3], [NIST SP 800-88].

MA-5 PERSONEL UTRZYMANIOWY

Zabezpieczenie podstawowe:

a. Ustanowienie procesu autoryzacji personelu utrzymaniowego i prowadzenie wykazu autoryzowanych organizacji obsługi technicznej lub personelu;

b. Zapewnianie, aby personel, wykonujący bez nadzoru prace utrzymaniowe w systemie, posiadał wymagane uprawnienia dostępu; oraz

c. Wyznaczenie personelu organizacyjnego, posiadającego wymagane uprawnienia dostępu i kompetencje techniczne, do nadzorowania czynności nieposiadających wymaganych uprawnień osób wykonujących prace utrzymaniowe.

Omówienie: Personel utrzymania odnosi się do osób, które wykonują prace utrzymaniowe sprzętu lub oprogramowania w systemach organizacyjnych, podczas gdy zabezpieczenie PE-2 dotyczy dostępu fizycznego osób, których obowiązki utrzymaniowe pozwalają im przebywać w granicach ochrony fizycznej systemów. Osoby, które nie zostały wcześniej zidentyfikowane, jako autoryzowany personel utrzymania - takie jak producenci technologii informatycznych, sprzedawcy, integratorzy systemów i konsultanci - mogą potrzebować uprzywilejowanego dostępu do systemów organizacyjnych, np. gdy są zobowiązane do przeprowadzenia działań konserwacyjnych z planowanych lub nieplanowanych. Na podstawie organizacyjnej oceny ryzyka, organizacje mogą wydawać tym osobom tymczasowe poświadczenia. Tymczasowe poświadczenia mogą być przeznaczone do jednorazowego użytku lub na bardzo ograniczony okres czasu.

Zabezpieczenia powiązane: AC-2, AC-3, AC-5, AC-6, IA-2, IA-8, MA-4, MP-2, PE-2, PE-3, PS-7, RA-3.

Zabezpieczenia rozszerzone:

(1) PERSONEL UTRZYMANIOWY | OSOBY NIEPOSIADAJĄCE STOSOWNYCH PRAW DOSTĘPU

a) Wdrożenie procedur zatrudniania personelu obsługi technicznej, którzy nie posiadają odpowiedniego poświadczenia bezpieczeństwa lub nie są polskimi obywatelami, określających następujące wymogi:

(1) Personel obsługi technicznej, który nie posiada niezbędnych uprawnień dostępu, poświadczeń bezpieczeństwa lub formalnych zezwoleń dostępu, jest eskortowany i nadzorowany podczas wykonywania czynności serwisowych i diagnostycznych w systemie przez zatwierdzony personel organizacyjny, który posiada poświadczenia bezpieczeństwa, odpowiednie zezwolenia na dostęp i posiada odpowiednie kwalifikacje techniczne; oraz

(2) Przed rozpoczęciem czynności utrzymaniowych lub diagnostycznych przez personel, który nie posiada autoryzacji dostępu, poświadczeń bezpieczeństwa lub formalnych zezwoleń na dostęp, wszystkie nietrwałe elementy przechowujące informacje w systemie są czyszczone, a wszystkie nieulotne nośniki pamięci są usuwane lub fizycznie odłączane od systemu i zabezpieczane; oraz

b) Opracowanie i wdrożenie [***Realizacja: zdefiniowane przez organizację zabezpieczenia alternatywne***] **w przypadku, gdy nie można wyczyścić, usunąć lub odłączyć komponentu systemu.**

Omówienie: Procedury dla osób, które nie posiadają odpowiedniego poświadczenia bezpieczeństwa lub nie są obywatelami polskimi, mają na celu odmowę wizualnego i elektronicznego dostępu do informacji jawnych lub nadzorowanych informacji jawnych zawartych w systemach organizacyjnych. Procedury dotyczące korzystania z usług personelu obsługi technicznej mogą być udokumentowane w planach bezpieczeństwa systemów.

Zabezpieczenia powiązane: MP-6, PL-2.

(2) PERSONEL UTRZYMANIOWY | POŚWIADCZENIA BEZPIECZEŃSTWA / SYSTEMY NIEJAWNE

Sprawdzanie, czy personel wykonujący czynności serwisowe i diagnostyczne w systemie przetwarzającym, przechowującym lub przekazującym informacje niejawne posiada poświadczenia bezpieczeństwa i formalne zatwierdzenia dostępu, do co najmniej najwyższego poziomu klasyfikacji informacji przetwarzanej w tym systemie.

Omówienie: Personel wykonujący czynności serwisowe i diagnostyczne w systemie organizacyjnym może uzyskać dostęp do informacji niejawnych w trakcie wykonywania czynności utrzymaniowych. Aby ograniczyć ryzyko związane z taką ekspozycją, organizacje korzystają z usług personelu utrzymaniowego, którzy został sprawdzony (tzn. osoby posiadają poświadczenie bezpieczeństwa) do poziomu klauzuli informacji przechowywanych w systemie.

Zabezpieczenia powiązane: PS-3.

(3) PERSONEL UTRZYMANIOWY | OBYWATELSTWO / SYSTEMY NIEJAWNE[58]

Sprawdzanie, czy pracownicy wykonujący czynności utrzymaniowe i diagnostyczne w systemie przetwarzającym, przechowującym lub przekazującym informacje niejawne są polskimi obywatelami.

Omówienie: Personel prowadzący prace serwisowe w systemach organizacyjnych może być narażony na kontakt z informacjami niejawnymi w trakcie wykonywania czynności utrzymaniowych. Zastosowanie mają przepisy ustawy o ochronie informacji niejawnych.

Zabezpieczenia powiązane: PS-3.

[58] Zastosowanie mają przepisy ustawy o ochronie informacji niejawnych.

(4) PERSONEL UTRZYMANIOWY | CUDZOZIEMCY[59]

Do wydawania zezwoleń, zgód i szczegółowych warunków operacyjnych dotyczących wykorzystywania cudzoziemców do prowadzenia działalności w zakresie utrzymania i diagnostyki systemów niejawnych zastosowanie mają przepisy ustawy o ochronie informacji niejawnych.

Omówienie: Personel, który wykonuje czynności konserwacyjne i diagnostyczne w systemach organizacyjnych, może być narażony na kontakt z informacjami niejawnymi. Zastosowanie mają przepisy ustawy o ochronie informacji niejawnych.

Zabezpieczenia powiązane: PS-3.

(5) PERSONEL UTRZYMANIOWY | OBSŁUGA NIEZWIĄZANA Z UTRZYMANIEM SYSTEMU

Zapewnienie, aby personel nieeskortowany, wykonujący czynności serwisowe, niezwiązane bezpośrednio z systemem, ale w fizycznej bliskości systemu, posiadał wymagane uprawnienia dostępu.

Omówienie: Personel, który wykonuje czynności konserwacyjne w innym charakterze, niezwiązane bezpośrednio z systemem, to m.in. pracownicy obsługi biurowej i administracji.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

[59] Zastosowanie mają przepisy ustawy o ochronie informacji niejawnych.

MA-6 TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI

Zabezpieczenie podstawowe: Uzyskanie wsparcia serwisowego i/lub części zamiennych dla [*Realizacja: zdefiniowanych przez organizację komponentów systemu*] w ciągu [*Realizacja: zdefiniowany przez organizację okres czasu*] wystąpienia awarii.

Omówienie: Organizacje określają komponenty systemu, które powodują zwiększone ryzyko dla operacji i majątku organizacji, osób, innych organizacji lub Państw, gdy funkcjonalność dostarczana przez te komponenty jest niedostępna. Działania organizacyjne w celu uzyskania wsparcia serwisowego dotyczą posiadanie odpowiednich umów.

Zabezpieczenia powiązane: CM-8, CP-2, CP-7, RA-7, SA-15, SI-13, SR-2, SR-3, SR-4.

Zabezpieczenia rozszerzone:

(1) TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI | KONSERWACJA ZAPOBIEGAWCZA

Przeprowadzanie konserwacji zapobiegawczej [Realizacja: zdefiniowane przez organizację *komponenty systemu*] w [*Realizacja: zdefiniowane przez organizację przedziały czasowe*].

Omówienie: Utrzymanie i wsparcie profilaktyczne obejmuje proaktywną opiekę i serwisowanie komponentów systemu w celu utrzymania urządzeń i obiektów organizacyjnych w zadowalającym stanie eksploatacyjnym. Utrzymanie i wsparcie takie zapewniają systematyczne przeglądy, testy, pomiary, regulacje, wymiana części, wykrywanie i korygowanie pojawiających się uszkodzeń zanim przerodzą się one w poważne usterki. Podstawowym celem konserwacji zapobiegawczej jest unikanie lub łagodzenie skutków awarii urządzeń. Utrzymanie i wsparcie zapobiegawcze ma na celu zachowanie i przywrócenie niezawodności urządzeń poprzez wymianę zużytych elementów przed ich awarią. Metody określania polityki zarządzania awariami prewencyjnymi (lub innymi) obejmują zalecenia

producenta oryginalnego sprzętu, statystyczną dokumentację awarii, ekspertyzy, konserwację, która została już przeprowadzona na podobnym sprzęcie, wymogi kodów, przepisów prawnych lub regulacji w ramach danej jurysdykcji, lub zmierzone wartości i wskazania dotyczące wydajności.

Zabezpieczenia powiązane: Brak.

(2) TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI | KONSERWACJA PLANOWA

Wykonywanie konserwacji planowej [Realizacja: zdefiniowane przez organizację *składniki systemu*] w [Realizacja: *zdefiniowane przez organizację przedziały czasowe*].

Omówienie: Utrzymanie i wsparcie zapobiegawcze ocenia stan urządzeń poprzez okresowe lub ciągłe (online) monitorowanie stanu urządzeń. Celem konserwacji planowej jest przeprowadzanie zaplanowanych czynności w czasie, kiedy działania konserwacyjne są najbardziej opłacalne i zanim urządzenie straci wydajność w granicach ustalonego progu. Konserwacja planowa komponentu wynika z celu przewidywania przyszłego stanu urządzeń. Podejście do konserwacji planowej wykorzystuje zasady statystycznej kontroli procesu w celu określenia, w którym momencie przyszłe działania związane z utrzymaniem będą właściwe. Większość przeglądów planowych przeprowadza się w trakcie eksploatacji urządzeń, minimalizując w ten sposób zakłócenia normalnej pracy systemu. Utrzymanie i wsparcie planowe może prowadzić do znacznych oszczędności kosztów i większej niezawodności systemu.

Zabezpieczenia powiązane: Brak.

(3) TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI | AUTOMATYCZNE WSPARCIE W ZAKRESIE KONSERWACJI PROGNOZOWANEJ

Wykorzystywanie do przesyłania danych dotyczących prognozowanej konserwacji do komputerowego systemu zarządzania konserwacją za pomocą [***Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację***]**.**

Omówienie: Skomputeryzowany system zarządzania konserwacją utrzymuje bazę danych zawierającą informacje o działaniach konserwacyjnych organizacji i automatyzuje przetwarzanie danych o stanie sprzętu w celu uruchomienia planowania, realizacji i raportowania działań utrzymaniowych.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

MA-7 KONSERWACJA W TERENIE

Zabezpieczenie podstawowe: Ograniczanie lub zakazanie przeprowadzania obsługi technicznej w terenie w odniesieniu do [Realizacja: *systemy lub komponenty systemu określone przez organizację*] do [*Realizacja: zaufane obiekty obsługi technicznej określone przez organizację*].

Omówienie: Ograniczanie lub zakazywanie obsługi technicznej w terenie [Realizacja: zdefiniowane przez organizację systemy lub komponenty systemu] wyłącznie do [Realizacja: zdefiniowane przez organizację zaufane obiekty obsługi technicznej].

Omówienie: Konserwacja w terenie jest rodzajem obsługi technicznej przeprowadzanej na systemie lub komponencie systemu po tym, jak system lub komponent został wdrożony do określonej lokalizacji (tj. środowiska operacyjnego). W pewnych przypadkach konserwacja w terenie (tj. konserwacja lokalna w obiekcie) może nie być przeprowadzana z takim samym rygorem lub przy takiej samej kontroli jakości jak konserwacja w jednostce organizacyjnej. Dla systemów krytycznych określonych przez organizację, może być konieczne ograniczenie lub zakazanie konserwacji w terenie w miejscu lokalnym i wymaganie, aby taka konserwacja była przeprowadzana w zaufanych obiektach z dodatkowymi zabezpieczeniami.

Zabezpieczenia powiązane: MA-2, MA-4, MA-5.

Zabezpieczenia rozszerzone: Brak.

KATEGORIA MP – OCHRONA NOŚNIKÓW DANYCH

MP-1 POLITYKA I PROCEDURY

Zabezpieczenie podstawowe:

a. Opracowywanie, dokumentowanie i rozpowszechnianie wśród [Realizacja: *personel lub role określone przez organizację*]:

   1. [*Wybór (jeden lub więcej): poziom organizacji; poziom misji/procesu biznesowego; poziom systemu*] polityki ochrony nośników danych, która:

      (a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami; oraz

      (b) Jest zgodna z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi; oraz

   2. Procedur ułatwiających wdrożenie polityki ochrony nośników danych oraz powiązanych zabezpieczeń w zakresie ochrony nośników danych;

b. Wyznaczanie [Realizacja: *osoba wyznaczona przez organizację*] do zarządzania rozwojem, dokumentacją i rozpowszechnianiem polityki i procedur ochrony nośników danych; oraz

c. Przeglądanie i aktualizacja bieżącej:

   1. Polityki ochrony nośników danych z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*]; oraz

   2. Procedur ochrony nośników danych z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*].

Omówienie: Polityka i procedury w zakresie ochrony nośników danych dotyczą zabezpieczeń w kategorii *Ochrona nośników danych* (MP), które są wdrażane w ramach systemów i organizacji. Strategia zarządzania ryzykiem jest ważnym

czynnikiem przy tworzeniu takich polityk i procedur. Polityki i procedury przyczyniają się do zapewnienia bezpieczeństwa i ochrony prywatności. Dlatego ważne jest, aby programy bezpieczeństwa i ochrony prywatności były opracowywane wspólnie przy kształtowaniu polityki i procedur ochrony nośników danych. Polityki i procedury dotyczące programów bezpieczeństwa i ochrony prywatności na poziomie organizacji są ogólnie rzecz biorąc preferowane i mogą eliminować potrzeby tworzenia polityk i procedur specyficznych dla danej misji lub systemu. Polityka może być włączona, jako część ogólnej polityki bezpieczeństwa i ochrony prywatności lub reprezentowana przez wiele polityk odzwierciedlających złożony charakter organizacji. Procedury mogą być ustanowione dla programów bezpieczeństwa i ochrony prywatności, dla misji lub procesów biznesowych oraz dla systemów, jeśli to konieczne. Procedury opisują sposób wdrażania zasad lub zabezpieczeń i mogą być skierowane do osoby lub roli, która jest przedmiotem procedury. Procedury mogą być udokumentowane w planach bezpieczeństwa i ochrony prywatności systemu w jednym lub kilku oddzielnych dokumentach.

Zdarzenia, które mogą spowodować konieczność aktualizacji polityki i procedur ochrony nośników danych, obejmują wyniki oceny lub audytu, incydenty lub naruszenia bezpieczeństwa, lub zmiany w przepisach prawa, zarządzeniach, dyrektywach, rozporządzeniach, zasadach, standardach i wytycznych.

Oświadczenie o wprowadzeniu zabezpieczeń nie jest równoznaczne z ustanowieniem polityki lub procedury organizacyjnej.

Zabezpieczenia powiązane: PM-9, PS-8, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [NIST SP 800-12], [NIST SP 800-30], [NIST SP 800-39], [NIST SP 800-100].

MP-2 DOSTĘP DO NOŚNIKÓW DANYCH

Zabezpieczenie podstawowe: Ograniczanie dostępu do [Realizacja: zdefiniowane przez *organizację typy mediów cyfrowych i/lub niecyfrowych*] tylko przez [*Realizacja: zdefiniowani przez organizację pracownicy lub role*].

Omówienie: Media systemowe obejmują media cyfrowe i niecyfrowe. Nośniki cyfrowe obejmują dyski flash, dyskietki, taśmy magnetyczne, zewnętrzne lub wymienne dyski twarde (np. półprzewodnikowe, magnetyczne), dyski kompaktowe i uniwersalne dyski cyfrowe. Nośniki niecyfrowe obejmują papier i mikrofilm. Przykładem ograniczenia dostępu do niecyfrowych nośników jest odmowa dostępu do dokumentacji medycznej pacjenta w szpitalu, chyba, że osoby ubiegające się o dostęp do takiej dokumentacji są upoważnionymi placówkami służby zdrowia. Przykładem ograniczenia dostępu do nośników cyfrowych jest ograniczenie dostępu do specyfikacji projektowych przechowywanych na płytach kompaktowych w bibliotece nośników do osób z zespołu opracowującego system.

Zabezpieczenia powiązane: AC-19, AU-9, CP-2, CP-9, CP-10, MA-5, MP-4, MP-6, PE-2, PE-3, SC-12, SC-13, SC-34, SI-12.

Zabezpieczenia rozszerzone:

(1) DOSTĘP DO MEDIÓW | OGRANICZONY DOSTĘP AUTOMATYCZNY

[Wycofane: Włączone do MP-4(2)]

(2) DOSTĘP DO MEDIÓW | OCHRONA KRYPTOGRAFICZNA

[Wycofane: Włączone do SC-28(1)]

Referencje: [OMB A-130], [FIPS 199], [NIST SP 800-111].

MP-3 OZNAKOWANIE NOŚNIKÓW DANYCH

Zabezpieczenie podstawowe:

a. Oznaczanie nośników systemowych wskazując ograniczenia w rozpowszechnianiu informacji, zastrzeżenia dotyczące postępowania z informacjami oraz odpowiednie określanie poziomów bezpieczeństwa (jeśli takie istnieją); oraz

b. Wyłączanie [*Realizacja: określone przez organizację rodzaje nośników systemowych*] z obowiązku oznaczania, jeżeli nośniki pozostają w obrębie [*Realizacja: określone przez organizację obszary kontrolowane*].

Omówienie: Oznaczanie bezpieczeństwa odnosi się do zastosowania lub użycia atrybutów bezpieczeństwa czytelnych dla człowieka. Nośniki cyfrowe obejmują dyskietki, taśmy magnetyczne, zewnętrzne lub wymienne dyski twarde (np. półprzewodnikowe, magnetyczne), napędy flash, dyski kompaktowe i uniwersalne dyski cyfrowe. Nośniki inne niż cyfrowe obejmują papier i mikrofilmy. Oznaczania bezpieczeństwa nie jest generalnie wymagane w odniesieniu do nośników zawierających informacje określone przez organizacje, jako należące do kategorii publicznej lub możliwe do publicznego udostępnienia. Niektóre organizacje mogą wymagać oznaczeń dla informacji publicznych wskazując, że informacje te są publicznie dostępne. Oznakowanie mediów systemowych odzwierciedla obowiązujące prawo, zarządzenia, dyrektywy, zasady, regulacje, normy i wytyczne.

Zabezpieczenia powiązane: AC-16, CP-9, MP-5, PE-22, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [32 CFR 2002], [FIPS 199].

MP-4 PRZECHOWYWANIE NOŚNIKÓW DANYCH

Zabezpieczenie podstawowe:

a. Fizyczne kontrolowanie i bezpieczne przechowywanie [*Realizacja: określone przez organizację rodzaje nośników cyfrowych i/lub niecyfrowych*] w obrębie [*Realizacja: określone przez organizację strefy kontrolowane*]; oraz

b. Ochrona mediów systemowych określonych w zabezpieczeniu MP-4a dopóki nie zostaną one zniszczone lub poddane sanityzacji przy użyciu zatwierdzonego sprzętu, technik i procedur.

Omówienie: Media systemowe obejmują media cyfrowe i niecyfrowe. Nośniki cyfrowe obejmują dyski flash, dyskietki, taśmy magnetyczne, zewnętrzne lub wymienne dyski twarde (np. półprzewodnikowe, magnetyczne), dyski kompaktowe i uniwersalne dyski cyfrowe. Nośniki niecyfrowe obejmują papier i mikrofilm. Fizyczne kontrolowanie przechowywanych nośników obejmuje przeprowadzanie inwentaryzacji, zapewnianie procedur umożliwiających personelowi sprawdzanie i zwracanie nośników do magazynu oraz utrzymywanie rozliczalności za przechowywane nośniki.

Bezpieczne przechowywanie obejmuje zamkniętą szufladę, biurko lub szafkę albo kontrolowaną przechowalnię nośników. Rodzaj przechowywanego nośnika jest współmierny do kategorii bezpieczeństwa lub klasyfikacji i informacji na nośniku.

Strefy kontrolowane to miejsca, które zapewniają fizyczną i proceduralną kontrolę w celu spełnienia wymagań ustanowionych dla ochrony informacji i systemów. Ograniczenie zabezpieczeń może być konieczne w przypadku nośników zawierających informacje, które uznano za należące do domeny publicznej, które można publicznie udostępnić lub które mogą mieć ograniczony negatywny wpływ na organizacje, działania lub osoby, jeżeli dostęp do nich uzyskają osoby nieupoważnione. W takich sytuacjach fizyczna kontrola dostępu zapewnia odpowiednią ochronę.

Zabezpieczenia powiązane: AC-19, CP-2, CP-6, CP-9, CP-10, MP-2, MP-7, PE-3, PL-2, SC-12, SC-13, SC-28, SC-34, SI-12.

Zabezpieczenia rozszerzone:

(1) PRZECHOWYWANIE NOŚNIKÓW DANYCH | OCHRONA KRYPTOGRAFICZNA

[Wycofane: Włączone do SC-28(1)]

(2) PRZECHOWYWANIE NOŚNIKÓW DANYCH | OGRANICZONY DOSTĘP AUTOMATYCZNY

Ograniczanie dostępu do miejsc przechowywania nośników i kontrola prób dostępu oraz przyznanego dostępu za pomocą [***Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację***]**.**

Omówienie: Zautomatyzowane mechanizmy obejmują klawiatury, czytniki biometryczne lub czytniki kart na zewnętrznych wejściach do miejsc przechowywania nośników.

Zabezpieczenia powiązane: AC-3, AU-2, AU-6, AU-9, AU-12, PE-3.

Referencje: [FIPS 199], [NIST SP 800-56A], [NIST SP 800-56B], [NIST SP 800-56C], [NIST SP 800-57-1], [NIST SP 800-57-2], [NIST SP 800-57-3], [NIST SP 800-111].

MP-5 TRANSPORT NOŚNIKÓW DANYCH

Zabezpieczenie podstawowe:

a. Ochrona i kontrola [*Realizacja: zdefiniowane typy nośników systemowych*] podczas transportu poza strefy kontrolne organizacji za pomocą [*Realizacja: zdefiniowane zabezpieczenia*];

b. Utrzymanie odpowiedzialność za nośniki systemu podczas transportu poza strefy kontrolowane;

c. Dokumentowanie działalności związanej z transportem nośników systemowych; oraz

d. Zezwalanie na wykonywanie czynności związanych z transportem nośników systemowych tylko przez upoważniony personel.

Omówienie: Nośniki systemowe obejmują media cyfrowe i niecyfrowe. Nośniki cyfrowe obejmują dyski flash, dyskietki, taśmy magnetyczne, zewnętrzne lub wymienne dyski twarde (np. półprzewodnikowe i magnetyczne), dyski kompaktowe i uniwersalne dyski cyfrowe. Nośniki niecyfrowe obejmują mikrofilmy i papier.

Strefy kontrolowane to miejsca, w których organizacje zapewniają fizyczną lub proceduralną zabezpieczenie w celu spełnienia wymagań ustanowionych dla ochrony informacji i systemów.

Zabezpieczenia mające na celu ochronę nośników podczas transportu obejmują kryptografię i zamknięte pojemniki. Mechanizmy kryptograficzne mogą zapewnić ochronę poufności i integralności w zależności od wdrożonych mechanizmów.

Działania związane z transportem nośników obejmują wydawanie nośników do transportu zapewniające, że nośniki przechodzą przez odpowiednie procesy transportowe oraz realizowanie samego transportu. Upoważniony personel transportowy i kurierski może obejmować osoby spoza organizacji. Utrzymywanie odpowiedzialności za nośniki podczas transportu obejmuje ograniczenie czynności transportowych do upoważnionego personelu oraz śledzenie i/lub uzyskiwanie

zapisów czynności transportowych w miarę przemieszczania się nośników w systemie transportowym w celu zapobiegania i wykrywania utraty, zniszczenia lub ingerencji. Organizacje ustanawiają wymagania dotyczące dokumentacji działań związanych z transportem nośników systemowych zgodnie z organizacyjną oceną ryzyka. Organizacje zachowują elastyczność w definiowaniu metod prowadzenia zapisów dla różnych rodzajów transportu nośników w ramach systemu ewidencji przebiegu transportu.

Zabezpieczenia powiązane: AC-7, AC-19, CP-2, CP-9, MP-3, MP-4, PE-16, PL-2, SC-12, SC-13, SC-28, SC-34.

Zabezpieczenia rozszerzone:

(1) TRANSPORT NOŚNIKÓW DANYCH | OCHRONA POZA STREFAMI KONTROLNYMI

[Wycofane: Włączone do MP-5].

(2) TRANSPORT NOŚNIKÓW DANYCH | DOKUMENTACJA DZIAŁAŃ

[Wycofane: Włączone do MP-5].

(3) TRANSPORT NOŚNIKÓW DANYCH | KONWOJENCI

Zatrudnianie konwojentów /nadzorujących transport nośników danych systemu poza obszary kontrolowane.

Omówienie: Zidentyfikowani konwojenci zapewniają organizacjom określone punkty kontaktowe podczas procesu transportu mediów i ułatwiają indywidualną odpowiedzialność. Odpowiedzialność konwojentów może być przeniesiona z jednej osoby na drugą, jeśli zostanie zidentyfikowany jednoznaczny nadzorca transportu.

Zabezpieczenia powiązane: Brak.

(4) TRANSPORT NOŚNIKÓW DANYCH | OCHRONA KRYPTOGRAFICZNA

[Wycofane: Włączone do SC-28(1)]

Referencje: [FIPS 199], [NIST SP 800-60-1], [NIST SP 800-60-2].

MP-6 SANITYZACJA NOŚNIKÓW DANYCH

Zabezpieczenie podstawowe:

a. Sanityzacja [*Realizacja: określone przez organizację nośniki systemowe*] przed usunięciem, uwolnieniem spod kontroli organizacyjnej lub ponownym użyciem przez zastosowanie [*Realizacja: określone przez organizację techniki i procedury oczyszczania*]; oraz

b. Stosowanie mechanizmów usuwania danych o sile i integralności proporcjonalnej do kategorii bezpieczeństwa lub klasyfikacji przetwarzanej informacji.

Omówienie: Sanityzacja nośników dotyczy wszystkich cyfrowych i niecyfrowych nośników systemowych podlegających utylizacji lub ponownemu użyciu, niezależnie od tego, czy nośnik jest uważany za usuwalny, czy też nie. Przykłady obejmują nośniki cyfrowe w skanerach, kopiarkach, drukarkach, notebookach, stacjach roboczych, komponentach sieciowych, urządzeniach przenośnych i nośnikach niecyfrowych (np. papierze i mikrofilmach). Proces sanityzacji usuwa informacje z nośników systemowych w taki sposób, że nie można ich odzyskać lub zrekonstruować. Techniki sanityzacji - w tym oczyszczanie, wymazywanie, kryptograficzne usuwanie, odmowa identyfikacji danych osobowych oraz niszczenie - zapobiegają ujawnieniu informacji nieupoważnionym osobom, gdy takie nośniki są ponownie wykorzystywane lub udostępniane do utylizacji. Organizacje określają odpowiednie metody sanityzacji, uznając, że zniszczenie jest czasami konieczne, gdy inne metody nie mogą być zastosowane do nośników wymagających sanityzacji. Organizacje podejmują decyzję o zastosowaniu zatwierdzonych technik i procedur sanityzacyjnych w odniesieniu do nośników, które zawierają informacje uznane za będące własnością publiczną lub publicznie dostępne, lub informacje uznane za niemające negatywnego wpływu na organizacje lub osoby w przypadku ich ponownego wykorzystania lub usunięcia. Sanityzacja nośników niecyfrowych obejmuje zniszczenie, usunięcie niejawnego załącznika z dokumentu, który w pozostałej części jest jawny, lub przeredagowanie wybranych sekcji lub słów z dokumentu poprzez zamaskowanie przeredagowanych

sekcji lub słów w sposób, którego skuteczność jest równoważna z usunięciem ich z dokumentu. Standardy i polityki Krajowej Władzy Bezpieczeństwa kontrolują proces sanityzacji nośników zawierających informacje niejawne. Polityki np. NARA kontrolują proces sanityzacji w odniesieniu do nadzorowanych informacji jawnych.

Zabezpieczenia powiązane: AC-3, AC-7, AU-11, MA-2, MA-3, MA-4, MA-5, PM-22, SI-12, SI-18, SI-19, SR-11.

Zabezpieczenia rozszerzone:

(1) SANITYZACJA NOŚNIKÓW DANYCH | PRZEGLĄD / ZATWIERDZANIE / ŚLEDZENIE / DOKUMENTOWANIE / WERYFIKACJA

Przeglądanie, zatwierdzanie, śledzenie, dokumentowanie i weryfikowanie działań w zakresie sanityzacji i niszczenia nośników.

Omówienie: Organizacje dokonują przeglądu i zatwierdzają nośniki, które należy poddać sanityzacji w celu zapewnienia zgodności z zasadami przechowywania dokumentacji. Śledzenie i dokumentowanie działań obejmuje sporządzenie listy personelu dokonującego przeglądu i zatwierdzania działań związanych z sanityzacją i niszczeniem, rodzajów mediów poddawanych sanityzacji, danych przechowywanych na nośnikach, stosowanych metod sanityzacji, daty i godziny działań związanych z sanityzacją, personelu, który przeprowadził sanityzację, podjętych działań weryfikacyjnych oraz personelu, który przeprowadził weryfikację oraz podjętych działań usuwających. Organizacje weryfikują, czy przed utylizacją przeprowadzono sanityzację nośników.

Zabezpieczenia powiązane: Brak.

(2) SANITYZACJA NOŚNIKÓW DANYCH | TESTOWANIE SPRZĘTU

Testowanie urządzeń i procedur sanityzacyjnych [***Realizacja: częstotliwość określona przez organizację***] **w celu zapewnienia, że zamierzona sanityzacja jest osiągana.**

Omówienie: Testowanie urządzeń i procedur sanityzacyjnych może być przeprowadzane przez wykwalifikowane i autoryzowane podmioty zewnętrzne.

Zabezpieczenia powiązane: Brak.

(3) SANITYZACJA NOŚNIKÓW DANYCH | TECHNIKI NIEDESTRUKCYJNE

Stosowanie niedestrukcyjnych technik sanityzacji przenośnych urządzeń pamięci masowej przed podłączeniem takich urządzeń do systemu w następujących okolicznościach: [Realizacja: *uwarunkowania organizacyjne wymagające sanityzacji przenośnych urządzeń pamięci masowej*].

Omówienie: Przenośne urządzenia pamięci masowej obejmują zewnętrzne lub wymienne dyski twarde (np. półprzewodnikowe, magnetyczne), dyski optyczne, taśmy magnetyczne lub optyczne, urządzenia pamięci flash, karty pamięci flash i inne zewnętrzne lub wymienne dyski. Przenośne urządzenia pamięci masowej mogą być pozyskiwane z niezaufanych źródeł i zawierać złośliwy kod, który może zostać wprowadzony do systemów organizacyjnych lub przeniesiony do nich za pośrednictwem portów USB lub innych portali wejściowych. Podczas skanowania urządzeń pamięci masowej zalecana jest sanityzacja, która daje dodatkową pewność, że takie urządzenia są wolne od złośliwego kodu. Organizacje rozważają stosowanie niedestrukcyjnych technik sanityzacji przenośnych urządzeń pamięci masowej, gdy urządzenia są kupowane od producentów lub sprzedawców do pierwszego użycia lub gdy organizacje nie mogą utrzymać prawidłowego łańcucha nadzoru nad urządzeniami.

Zabezpieczenia powiązane: Brak.

(4) SANITYZACJA NOŚNIKÓW DANYCH | KONTROLOWANE INFORMACJE JAWNE

[Wycofane: Włączone do MP-6].

(5) SANITYZACJA NOŚNIKÓW DANYCH | INFORMACJE NIEJAWNE[60]

[Wycofane: Włączone do MP-6].

(6) SANITYZACJA NOŚNIKÓW DANYCH | NISZCZENIE NOŚNIKÓW DANYCH

[Wycofane: Włączone do MP-6].

(7) SANITYZACJA NOŚNIKÓW DANYCH | PODWÓJNA AUTORYZACJA

Egzekwowanie podwójnej autoryzacji celem przeprowadzenia sanityzacji [***Realizacja: media systemowe zdefiniowane przez organizację***]**.**

Omówienie: Organizacje stosują podwójną autoryzację, aby zapewnić, że sanityzacja nośników systemowych nie może mieć miejsca, dopóki dwie technicznie wykwalifikowane osoby nie wykonają wyznaczonego zadania. Osoby dokonujące sanityzacji nośników systemowych posiadają wystarczające umiejętności i wiedzę, aby określić, czy proponowana sanityzacja odzwierciedla obowiązujące standardy, polityki i procedury. Podwójna autoryzacja pomaga również zapewnić, że sanityzacja przebiega zgodnie z założeniami, chroniąc przed błędami i fałszywymi twierdzeniami o wykonaniu czynności sanityzacyjnych. Podwójna autoryzacja może być również znana jako kontrola dwuosobowa. Aby zredukować ryzyko zmowy, organizacje rozważają przekazanie obowiązków związanych z podwójną autoryzacją innym osobom.

Zabezpieczenia powiązane: AC-3, MP-2.

(8) SANITYZACJA NOŚNIKÓW DANYCH | ZDALNE KASOWANIE / WYMAZYWANIE INFORMACJI

Zapewnienie możliwości kasowania lub wymazywania informacji z [Realizacja: ***systemy lub komponenty systemu zdefiniowane przez organizację***] [***Wybór:***

[60] Zastosowanie mają przepisy ustawy o ochronie informacji niejawnych.

zdalnie; pod następującymi warunkami: [***Realizacja: warunki określone przez organizację***]].

Omówienie: Zdalne kasowanie lub wymazywanie informacji chroni informacje w systemach organizacyjnych i komponentach systemu, jeśli systemy lub komponenty zostaną przejęte przez osoby nieupoważnione. Polecenia zdalnego kasowania lub wymazywania wymagają silnego uwierzytelnienia, aby ograniczyć ryzyko, że nieupoważnione osoby będą mogły dokonać usunięcia lub wymazania systemu, komponentu lub urządzenia. Funkcja kasowania lub wymazywania może być realizowana na różne sposoby, w tym przez wielokrotne nadpisywanie danych lub informacji albo przez niszczenie klucza niezbędnego do odszyfrowania zaszyfrowanych danych.

Zabezpieczenia powiązane: Brak.

Referencje: [32 CFR 2002], [OMB A-130], [NARA CUI], [FIPS 199], [NIST SP 800-60-1], [NIST SP 800-60-2], [NIST SP 800-88], [NIST SP 800-124], [IR 8023], [NSA MEDIA].

MP-7 UŻYWANIE NOŚNIKÓW DANYCH

Zabezpieczenie podstawowe:

a. [*Wybór: Ograniczanie; Zakazanie*] używania [*Realizacja: zdefiniowane przez organizację typów nośników systemowych*] w [*Realizacja: zdefiniowane przez organizację systemy lub komponenty systemowe*] przy użyciu [*Realizacja: zdefiniowane przez organizację zabezpieczenia*]; oraz

b. Zakazanie korzystania z przenośnych urządzeń pamięci masowej w systemach organizacyjnych, jeśli urządzenia te nie mają określonego właściciela.

Omówienie: Nośniki systemowe obejmują zarówno media cyfrowe, jak i niecyfrowe. Nośniki cyfrowe obejmują dyskietki, taśmy magnetyczne, napędy flash, dyski kompaktowe, uniwersalne dyski cyfrowe i wymienne dyski twarde. Nośniki niecyfrowe obejmują papier i mikrofilm. Zabezpieczenia związane z użytkowaniem nośników dotyczą również urządzeń przenośnych z możliwością przechowywania informacji. W przeciwieństwie do zabezpieczenia MP-2, które ogranicza dostęp użytkownika do nośników, zabezpieczenie MP-7 ogranicza korzystanie z niektórych rodzajów nośników w systemach, na przykład ograniczając lub zakazując korzystania z dysków flash lub zewnętrznych dysków twardych. Organizacje stosują techniczne i nietechniczne środki zabezpieczeń w celu ograniczenia korzystania z nośników systemowych. Organizacje mogą ograniczyć korzystanie z przenośnych urządzeń pamięci masowej, na przykład stosując fizyczne obudowy na stacjach roboczych w celu uniemożliwienia dostępu do niektórych portów zewnętrznych lub wyłączając lub usuwając możliwość podłączania, czytania lub zapisywania na takich urządzeniach. Organizacje mogą również ograniczyć korzystanie z przenośnych urządzeń pamięci masowej wyłącznie do zatwierdzonych urządzeń, w tym urządzeń dostarczanych przez organizację, urządzeń dostarczanych przez inne zaufane organizacje oraz urządzeń, które nie są własnością osobistą. Ponadto organizacje mogą ograniczyć korzystanie z przenośnych urządzeń pamięci masowej ze względu na typ urządzenia, np. zakazując korzystania z przenośnych

urządzeń pamięci masowej nadających się do zapisu oraz wprowadzając to ograniczenie poprzez wyłączenie lub usunięcie możliwości zapisu na takich urządzeniach. Wymaganie identyfikacji właścicieli urządzeń pamięci masowej zmniejsza ryzyko korzystania z takich urządzeń, pozwalając organizacjom na przypisanie odpowiedzialności za usuwanie znanych luk w zabezpieczeniach urządzeń.

Zabezpieczenia powiązane: AC-19, AC-20, PL-4, PM-12, SC-34, SC-41.

Zabezpieczenia rozszerzone:

(1) UŻYWANIE NOŚNIKÓW DANYCH | ZABRONIONE WYKORZYSTANIE NIEZIDENTYFIKOWANEJ WŁASNOŚCI

[Wycofane: Włączone do MP-7].

(2) UŻYWANIE NOŚNIKÓW DANYCH | ZABRONIONE WYKORZYSTANIE MEDIÓW ODPORNYCH NA SANITYZACJĘ

Zabronienie stosowania w systemach organizacyjnych nośników odpornych na sanityzację.

Omówienie: Odporność sanityzacyjna odnosi się do odporności mediów na nieniszczące techniki sanityzacyjne w odniesieniu do zdolności do usuwania informacji z mediów. Niektóre typy nośników nie obsługują poleceń sanityzacji, a jeśli są obsługiwane, interfejsy nie są obsługiwane w sposób standardowy przez te urządzenia. Nośniki odporne na skutki sanityzacji obejmują kompaktową pamięć flash, wbudowaną pamięć flash na płytach i urządzeniach, dyski półprzewodnikowe i nośniki wymienne USB.

Zabezpieczenia powiązane: MP-6.

Referencje: [FIPS 199], [SP. 800-111].

MP-8 DEKLASYFIKACJA NOŚNIKÓW DANYCH

Zabezpieczenie podstawowe:

a. Ustanowienie [*Realizacja: zdefiniowany przez organizację proces obniżania klasyfikacji nośników systemowych (deklasyfikacja)*], który obejmuje stosowanie mechanizmów obniżania klasyfikacji o sile i integralności proporcjonalnej do kategorii bezpieczeństwa lub klasyfikacji informacji;

b. Sprawdzanie, czy proces obniżania kategorii nośników jest współmierny do kategorii bezpieczeństwa i/lub poziomu klauzuli informacji, które mają zostać usunięte, oraz posiadanych upoważnień użytkowników do dostępu do zdeklasyfikowanych informacji;

c. Zidentyfikowanie [*Realizacja: nośniki systemowe zdefiniowane przez organizację, wymagające deklasyfikacji*]*;* oraz

d. Deklasyfikowanie zidentyfikowanych nośników za pomocą ustanowionego procesu.

Omówienie: Obniżenie klasyfikacji nośników dotyczy mediów cyfrowych i niecyfrowych, które mogą być udostępniane poza organizacją, bez względu na to, czy są one uznawane za wymienne czy nie. W przypadku nośników systemowych, proces deklasyfikacji usuwa informacje z nośników, zwykle według kategorii bezpieczeństwa lub poziomu klauzuli, w taki sposób, że informacja nie może być odzyskana lub zrekonstruowana. Obniżenie kategorii nośnika obejmuje zredagowanie informacji w celu umożliwienia ich szerszego udostępnienia i dystrybucji. Obniżenie klasyfikacji zapewnia, że puste miejsce na nośniku jest pozbawione informacji.

Zabezpieczenia powiązane: Brak.

Zabezpieczenia rozszerzone:

(1) DEKLASYFIKACJA NOŚNIKÓW DANYCH | DOKUMENTACJA PROCESU

Dokumentowanie działań związanych z deklasyfikacją nośników danych.

Omówienie: Organizacje mogą dokumentować proces deklasyfikacji nośników poprzez podanie informacji, takich jak zastosowana technika obniżania klasyfikacji, numer identyfikacyjny deklasyfikowanego nośnika oraz tożsamość osoby, która upoważniła i/lub przeprowadziła deklasyfikację.

Zabezpieczenia powiązane: Brak.

(2) DEKLASYFIKACJA NOŚNIKÓW DANYCH | TESTOWANIE SPRZĘTU

Testowanie sprzętu i procedur deklasyfikacji [***Realizacja: częstotliwość określona przez organizację***] ***w*** **celu zapewnienia weryfikacji prawidłowości wykonania tego procesu.**

Omówienie: Brak.

Zabezpieczenia powiązane: Brak.

(3) DEKLASYFIKACJA NOŚNIKÓW DANYCH | KONTROLOWANE INFORMACJE JAWNE

Deklasyfikowanie nośników systemowych zawierających kontrolowane informacje jawne przed ich publicznym udostępnieniem.

Omówienie: Obniżenie klasyfikacji kontrolowanych informacji jawnych obejmuje zatwierdzone narzędzia, techniki i procedury sanityzacyjne.

Zabezpieczenia powiązane: Brak.

(4) DEKLASYFIKACJA NOŚNIKÓW DANYCH | INFORMACJE NIEJAWNE

Deklasyfikowanie nośników systemowych zawierających informacje niejawne przed ich udostępnieniem osobom nieposiadającym stosownych poświadczeń bezpieczeństwa.

Omówienie: Przy obniżaniu klasyfikacji informacji niejawnych wykorzystuje się zatwierdzone narzędzia, techniki i procedury sanityzacji w celu przekazywania informacji z systemów niejawnych na nieklasyfikowane nośniki, co do których potwierdzono, że nie są zaklasyfikowane jako niejawne.

Zabezpieczenia powiązane: Brak.

Referencje: [32 CFR 2002], [NSA MEDIA].

KATEGORIA PE – OCHRONA FIZYCZNA I ŚRODOWISKOWA

PE-1 POLITYKA I PROCEDURY

Zabezpieczenie podstawowe:

a. Opracowywanie, dokumentowanie i rozpowszechnianie wśród [Realizacja: *personel lub role określone przez organizację*]:

   1. [*Wybór (jeden lub więcej): poziom organizacji; poziom misji/procesu biznesowego; poziom systemu*] polityki ochrony fizycznej i środowiskowej, która:

      (a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami; oraz

      (b) Jest zgodna z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi; oraz

   2. Procedur ułatwiających wdrożenie polityki ochrony fizycznej i środowiskowej oraz powiązanych zabezpieczeń w zakresie ochrony fizycznej i środowiskowej;

b. Wyznaczanie [Realizacja: *osoba wyznaczona przez organizację*] do zarządzania rozwojem, dokumentacją i rozpowszechnianiem polityki i procedur ochrony fizycznej i środowiska; oraz

c. Przeglądanie i aktualizacja bieżącej:

   1. Polityki ochrony fizycznej i środowiskowej z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*]; oraz

   2. Procedur ochrony fizycznej i środowiskowej z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*].

Omówienie: Polityka i procedury w zakresie ochrony fizycznej i środowiskowej dotyczą zabezpieczeń w kategorii *Ochrona fizyczna i środowiskowa* (PE), które są wdrażane w ramach systemów i organizacji. Strategia zarządzania ryzykiem jest ważnym czynnikiem przy tworzeniu takich polityk i procedur. Polityki i procedury przyczyniają się do zapewnienia bezpieczeństwa i ochrony prywatności. Dlatego ważne jest, aby programy bezpieczeństwa i ochrony prywatności były opracowywane wspólnie przy kształtowaniu polityki i procedur ochrony fizycznej i środowiskowej. Polityki i procedury dotyczące programów bezpieczeństwa i ochrony prywatności na poziomie organizacji są ogólnie rzecz biorąc preferowane i mogą eliminować potrzeby tworzenia polityk i procedur specyficznych dla danej misji lub systemu. Polityka może być włączona, jako część ogólnej polityki bezpieczeństwa i ochrony prywatności lub reprezentowana przez wiele polityk odzwierciedlających złożony charakter organizacji. Procedury mogą być ustanowione dla programów bezpieczeństwa i ochrony prywatności, dla misji lub procesów biznesowych oraz dla systemów, jeśli to konieczne. Procedury opisują sposób wdrażania zasad lub zabezpieczeń i mogą być skierowane do osoby lub roli, która jest przedmiotem procedury. Procedury mogą być udokumentowane w planach bezpieczeństwa i ochrony prywatności systemu w jednym lub kilku oddzielnych dokumentach.

Zdarzenia, które mogą spowodować konieczność aktualizacji polityki i procedur ochrony fizycznej i środowiskowej, obejmują wyniki oceny lub audytu, incydenty lub naruszenia bezpieczeństwa, lub zmiany w przepisach prawa, zarządzeniach, dyrektywach, rozporządzeniach, zasadach, standardach i wytycznych.

Oświadczenie o wprowadzeniu zabezpieczeń nie jest równoznaczne z ustanowieniem polityki lub procedury organizacyjnej.

Zabezpieczenia powiązane: NA 3, PM-9, PS-8, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [NIST SP 800-12], [NIST SP 800-30], [NIST SP 800-39], [NIST SP 800-100].

PE-2 ZEZWOLENIA NA DOSTĘP FIZYCZNY

Zabezpieczenie podstawowe:

a. Opracowanie, zatwierdzenie i prowadzenie listy osób posiadających autoryzowany dostęp do obiektu, w którym znajduje się system;

b. Wydawanie poświadczeń autoryzacji (przepustki) dostępu do obiektu;

c. Przeglądanie listy dostępu zawierającej szczegółowe informacje na temat autoryzowanego dostępu do obiektu przez osoby fizyczne [*Realizacja: częstotliwość określona przez organizację*]; oraz

d. Aktualizowanie listy osób posiadających dostęp do obiektu.

Omówienie: Fizyczne uprawnienia dostępu dotyczą pracowników i gości. Osoby posiadające stałe uprawnienia dostępu fizycznego nie są uważane za gości. Poświadczenia autoryzacji obejmują identyfikatory (plakietki), karty identyfikacyjne i karty inteligentne. Organizacje określają siłę wymaganych poświadczeń autoryzacji zgodnie z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi. Fizyczne uprawnienia dostępu mogą nie być wymagane w celu uzyskania dostęp do niektórych obszarów w ramach obiektów, które są oznaczone, jako publicznie dostępne.

Zabezpieczenia powiązane: AT-3, AU-9, IA-4, MA-5, MP-2, PE-3, PE-4, PE-5, PE-8, PM-12, PS-3, PS-4, PS-5, PS-6.

Zabezpieczenia rozszerzone:

(1) ZEZWOLENIA NA DOSTĘP FIZYCZNY | DOSTĘP ZGODNIE Z POSIADANĄ POZYCJĄ / ROLĄ

Zezwolenie na fizyczny dostęp do obiektu, w którym znajduje się system, w zależności od posiadanego stanowiska lub roli.

Omówienie: Dostęp do obiektu na podstawie ról obejmuje dostęp upoważnionego personelu stałego i przeprowadzającego regularne przeglądy techniczne, pracowników dyżurnych oraz ratowników medycznych (w nagłych przypadkach).

Zabezpieczenia powiązane: AC-2, AC-3, AC-6.

(2) ZEZWOLENIA NA DOSTĘP FIZYCZNY | PODWÓJNA IDENTYFIKACJA

Wymaganie dwóch form identyfikacji spośród następujących form identyfikacji dostępu gości do obiektu, w którym znajduje się system: [*Przypis: zdefiniowana przez organizację lista akceptowalnych form identyfikacji*].

Omówienie: Akceptowalne formy identyfikacji obejmują dowody osobiste, paszporty, prawa jazdy, karty identyfikacyjne oraz legitymacje ze zdjęciem. W celu uzyskania dostępu do obiektów wykorzystujących mechanizmy automatycznego dostępu, organizacje mogą stosować karty identyfikacyjne, karty-klucze, PIN-y i biometrię.

Zabezpieczenia powiązane: IA-2, IA-4, IA-5.

(3) ZEZWOLENIA NA DOSTĘP FIZYCZNY | OGRANICZANIE DOSTĘPU BEZ ASYSTY

Ograniczenie dostępu bez asysty do obiektu, w którym znajduje się system, do personelu posiadającego [***Wybór (jedno lub więcej): poświadczenia bezpieczeństwa do wszystkich informacji przetwarzanych w systemie; formalne upoważnienia dostępu dla wszystkich informacji przetwarzanych w systemie; potrzebę dostępu do wszystkich informacji zawartych w systemie;*** [***Realizacja: fizyczne upoważnienia dostępu zdefiniowane przez organizację***]]**.**

Omówienie: Osobom nieposiadającym wymaganych poświadczeń bezpieczeństwa, zezwoleń na dostęp lub potrzeby dostępu (*ang. need-to-know*) do informacji są przydzielane asysty osób posiadających odpowiednie uprawnienia do dostępu fizycznego w celu zapewnienia, że informacje nie zostaną ujawnione lub w inny sposób narażone na ujawnienie.

Zabezpieczenia powiązane: PS-2, PS-6.

Referencje: [FIPS 201-2], [NIST SP 800-73-4], [NIST SP 800-76-2], [NIST SP 800-78-4].

PE-3 KONTROLA DOSTĘPU FIZYCZNEGO

Zabezpieczenie podstawowe:

a. Egzekwowanie fizycznych uprawnień dostępu w [*Realizacja: zdefiniowane przez organizację punkty wejścia / wyjścia do / z obiektu, w którym znajduje się system*] poprzez:

   1. Weryfikację indywidualnych zezwoleń na dostęp przed udzieleniem dostępu do obiektu; oraz

   2. Zabezpieczenie wejściem i wyjściem do obiektu za pomocą funkcji [*Wybór (jeden lub więcej)*]: [*Realizacja: zdefiniowane przez organizację systemy lub urządzenia fizycznej kontroli dostępu*]; *ochrona*];

b. Prowadzenie dziennika kontroli dostępu fizycznego w [*Realizacja: punkty wejścia / wyjścia zdefiniowane przez organizację*];

c. Zabezpieczenie dostępu do obszarów w obrębie obiektu wyznaczonych, jako publicznie dostępne, poprzez wdrożenie następujących zabezpieczeń: [*Realizacja: określone przez organizację fizyczne zabezpieczenia dostępu*];

d. Eskortowanie gości i kontrola ich aktywności [*Realizacja: okoliczności organizacyjne wymagające eskorty gości i kontroli aktywności gości*];

e. Zabezpieczanie kluczy, zestawów kontroli i innych fizycznych urządzeń dostępu;

f. Inwentaryzacja [*Realizacja: urządzenia dostępu fizycznego zdefiniowane przez organizację*] co [*Realizacja: częstotliwość zdefiniowana przez organizację*]; oraz

g. Zmiana kombinacji zamków szyfrowych i kluczy z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*] i/lub w przypadku utraty kluczy, kompromitacji kombinacji lub przeniesienia / zwolnienia osób posiadających klucze lub kombinacje.

Omówienie: Fizyczne zabezpieczenie dostępu dotyczy pracowników i gości. Osoby posiadające stałe upoważnienie do dostępu fizycznego nie są uznawane za odwiedzających. Fizyczne zabezpieczenie dostępu do obszarów publicznie dostępnych może obejmować dzienniki/rejestry fizycznej kontroli dostępu, służbę ochrony lub fizyczne urządzenia dostępu oraz bariery uniemożliwiające przemieszczanie się z obszarów publicznie dostępnych do obszarów niepublicznych. Organizacje ustalają wymagane typy ochrony, w tym profesjonalnych pracowników ochrony, użytkowników systemu lub pracowników administracyjnych. Urządzenia dostępu fizycznego obejmują klucze, zamki, zamki szyfrowe, czytniki biometryczne i czytniki kart. Systemy kontroli dostępu fizycznego są zgodne z obowiązującym prawem, rozporządzeniami wykonawczymi, dyrektywami, politykami, przepisami, standardami i wytycznymi. Organizacje mają swobodę w wyborze rodzaju stosowanych dzienników kontroli dostępu. Dzienniki kontroli mogą być proceduralne, zautomatyzowane lub stanowić ich kombinację. Fizyczne punkty dostępu mogą obejmować punkty dostępu do obiektu, wewnętrzne punkty dostępu do systemów, które wymagają dodatkowej kontroli dostępu, lub oba te elementy. Komponenty systemów mogą znajdować się w miejscach oznaczonych jako ogólnodostępne, przy czym organizacje kontrolują dostęp do tych komponentów.

Zabezpieczenia powiązane: AT-3, AU-2, AU-6, AU-9, AU-13, CP-10, IA-3, IA-8, MA-5, MP-2, MP-4, PE-2, PE- 4, PE-5, PE-8, PS-2, PS-3, PS-6, PS-7, RA-3, SC-28, SI-4, SR-3.

Zabezpieczenia rozszerzone:

(1) KONTROLA DOSTĘPU FIZYCZNEGO | DOSTĘP DO SYSTEMU

Wymuszanie uwierzytelniania fizycznych uprawnień dostępu do systemu oprócz fizycznych kontroli dostępu do obiektu w [***Realizacja: zdefiniowane przez organizację przestrzenie fizyczne zawierające jeden lub więcej komponentów systemu***]**.**

Omówienie: Zabezpieczenie fizycznego dostępu do systemu zapewnia dodatkowe bezpieczeństwo fizyczne tych obszarów w obiektach, w których występuje koncentracja komponentów systemu.

Zabezpieczenia powiązane: Brak.

(2) KONTROLA DOSTĘPU FIZYCZNEGO | OBIEKT / OBSZAR SYSTEMU

Przeprowadzanie kontroli bezpieczeństwa w zakresie dostępu do fizycznej strefy obiektu lub dostępu do systemu informatycznego w celu uniemożliwienia nieautoryzowanego upublicznienia informacji lub usunięcia komponentów systemu z [***Realizacja: częstotliwość określona przez organizację***]

Omówienie: Organizacje określają zakres, częstotliwość i/lub losowość kontroli bezpieczeństwa w celu odpowiedniego ograniczenia ryzyka związanego z eksfiltracją.

Zabezpieczenia powiązane: AC-4, SC-7.

(3) KONTROLA DOSTĘPU FIZYCZNEGO |CIĄGŁOŚĆ OCHRONY FIZYCZNEJ

Personel ochrony zatrudniony do monitorowania [***Realizacja: zdefiniowane przez organizację fizyczne punkty***] **dostępu do obiektu, w którym znajduje się system, przez 24 godziny na dobę / 7 dni w tygodniu / przez cały rok.**

Omówienie: Monitorowanie przez ochronę wybranych fizycznych punktach dostępu do obiektu zapewnia organizacjom szybszą reakcję na wszelkiego rodzaju wydarzenia. Personel ochrony zapewnia również możliwość nadzoru osób przebywających w obszarach obiektu nieobjętych nadzorem wideo.

Zabezpieczenia powiązane: CP-6, CP-7, PE-6.

(4) KONTROLA DOSTĘPU FIZYCZNEGO | ZAMYKANE OBUDOWY

Używanie zamykanych na klucz obudów fizycznych do ochrony przed nieautoryzowanym fizycznym dostępem do komponentów systemu [***Realizacja: zdefiniowane przez organizację komponenty systemu***]**.**

Omówienie: Największym ryzykiem związanym z używaniem urządzeń przenośnych - takich jak smartfony, tablety i notebooki - jest kradzież. Organizacje mogą stosować zamykane, fizyczne obudowy, aby zmniejszyć lub wyeliminować ryzyko kradzieży sprzętu. Obudowy takie są dostępne w różnych rozmiarach, od jednostek chroniących jeden notebook po wielkogabarytowe szafy, które mogą chronić wiele serwerów, komputerów i urządzeń peryferyjnych. Zamykane obudowy fizyczne mogą być stosowane w połączeniu z linkami zabezpieczającymi lub uchwytami (płytkami) blokującymi, utrudniającymi kradzież zamkniętej obudowy zawierającej sprzęt komputerowy.

Zabezpieczenia powiązane: Brak.

(5) KONTROLA DOSTĘPU FIZYCZNEGO | OCHRONA PRZED MANIPULACJĄ

Stosowanie [***Realizacja: zdefiniowane przez organizację technologie zabezpieczające przed manipulacją***] **do** [***Wybór (jeden lub więcej): wykrywanie; zapobieganie***] **fizycznej manipulacji lub zmiany** [***Realizacja: zdefiniowane przez organizację komponenty sprzętowe***] **w systemie.**

Omówienie: Organizacje mogą wdrożyć wykrywanie i zapobieganie manipulacjom w wybranych komponentach sprzętu lub wdrożyć wykrywanie manipulacji przy jednych elementach i zapobieganie manipulacjom przy innych. W ramach działań związanych z wykrywaniem i zapobieganiem można stosować wiele rodzajów technologii zabezpieczających przed manipulacjom, w tym plomby i powłoki zabezpieczające przed sabotażem. Programy ochrony przed manipulacją pomagają w wykrywaniu w sprzęcie zmian nieautoryzowanych przeróbek i innych zagrożeń związanych z łańcuchem dostaw.

Zabezpieczenia powiązane: SA-16, SR-9, SR-11.

(6) KONTROLA DOSTĘPU FIZYCZNEGO | TESTY PENETRACYJNE OBIEKTU

[Wycofane: Włączone do CA-8].

(7) KONTROLA DOSTĘPU FIZYCZNEGO | BARIERY FIZYCZNE

Ograniczanie dostępu fizycznego za pomocą barier fizycznych.

Omówienie: Bariery fizyczne obejmują pachołki, płyty betonowe, ścian z płyt dżersej i aktywne bariery hydrauliczne dla pojazdów.

Zabezpieczenia powiązane: Brak.

(8) KONTROLA DOSTĘPU FIZYCZNEGO | ŚLUZY W KONTROLI DOSTĘPU

Stosowanie przedsionków (śluz) w kontroli dostępu w [***Realizacja: zdefiniowane przez organizacje lokalizacje w obrębie obiektu***]**.**

Omówienie: Śluza w kontroli dostępu jest częścią fizycznego systemu kontroli dostępu, który zazwyczaj zapewnia przestrzeń pomiędzy dwoma zestawami zamykanych na klucz drzwi. Śluzy są tak zaprojektowane, aby uniemożliwić osobom nieupoważnionym podążanie za upoważnionymi osobami do obiektów z kontrolowanym dostępem. Czynność ta, znana również jako "piggybacking" lub "tailgating", skutkuje nieautoryzowanym dostępem do obiektu. Sterowniki drzwi blokujących mogą być używane do ograniczenia liczby osób, które wchodzą do kontrolowanych punktów dostępu i do zapewnienia obszarów izolacyjnych podczas weryfikacji upoważnienia do fizycznego dostępu. Sterowniki drzwi blokujących mogą być w pełni zautomatyzowane (tj. kontrolujące otwieranie i zamykanie drzwi) lub częściowo zautomatyzowane (tj. wykorzystujące pracowników ochrony do kontrolowania liczby osób wchodzących do obszaru zamkniętego).

Zabezpieczenia powiązane: Brak.

Referencje: [FIPS 201-2], [NIST SP 800-73-4], [NIST SP 800-76-2], [NIST SP 800-78-4], [NIST SP 800-116].

PE-4 KONTROLA DOSTĘPU DO MEDIUM TRANSMISYJNEGO

Zabezpieczenie podstawowe: Zabezpieczenie fizycznego dostępu do [*Realizacja: zdefiniowane przez organizację linie dystrybucji i transmisji*] w obrębie obiektów organizacyjnych za pomocą [*Realizacja: zdefiniowane przez organizację środki bezpieczeństwa*].

Omówienie: Zabezpieczenia linii dystrybucji i transmisji mają za zadanie zapobieganiu przypadkowym uszkodzeniom, zakłóceniom i fizycznym manipulacjom. Stosowanie środków bezpieczeństwa może być również konieczne w celu zapobieżenia podsłuchowi lub modyfikacji nieszyfrowanych transmisji. Środki bezpieczeństwa stosowane do kontroli fizycznego dostępu do linii dystrybucji i transmisyjnych systemu obejmują odłączane lub blokowane gniazda przyłączeniowe, zamykane szafy kablowe, ochronę okablowania za pomocą osłon lub korytek kablowych oraz czujników zakładanych na kable (osłony).

Zabezpieczenia powiązane: AT-3, IA-4, MP-2, MP-4, PE-2, PE-3, PE-5, PE-9, SC-7, SC-8.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

PE-5 KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA

Zabezpieczenie podstawowe: Kontrola fizycznego dostępu do urządzeń wejścia / *wyjścia* [*Realizacja: urządzenia wejścia / wyjścia zdefiniowane przez organizację*] w celu uniemożliwienia osobom nieupoważnionym uzyskania dostępu do wyników przetwarzania informacji.

Omówienie: Zabezpieczenie fizycznego dostępu do urządzeń wejścia / wyjścia obejmuje umieszczanie tych urządzeń w pomieszczeniach zamkniętych lub innych pomieszczeniach zabezpieczonych zamkiem szyfrowym lub czytnikiem kart dostępu; zezwalanie na dostęp do urządzeń wejścia / wyjścia tylko upoważnionemu personelowi; instalowanie urządzeń wejścia / wyjścia w miejscach, które mogą być monitorowane przez personel ochrony; instalowanie filtrów monitorowych lub ekranowych oraz używanie słuchawek. Przykładowe urządzenia wejścia / wyjścia to monitory, drukarki, skanery, urządzenia audio, faksy i kopiarki.

Zabezpieczenia powiązane: PE-2, PE-3, PE-4, PE-18.

Zabezpieczenia rozszerzone:

(1) KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA | DOSTĘP UPOWAŻNIONYCH OSÓB DO URZĄDZEŃ

[Wycofane: włączone do PE-5].

(2) KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA | DOSTĘP DO DANYCH NA PODSTAWIE INDYWIDUALNEJ TOŻSAMOŚCI

Powiązanie indywidualnej tożsamości z udzielaniem dostępu do danych wejściowych / wyjściowych urządzenia.

Omówienie: Metody łączenia indywidualnej tożsamości z udzielaniem dostępu do danych wejściowych / wyjściowych urządzenia obejmują instalację funkcji bezpieczeństwa na urządzeniach faksowych, kopiarkach i drukarkach. Taka funkcjonalność pozwala organizacjom na zaimplementowanie uwierzytelniania na

urządzeniach wejścia / wyjścia przed uzyskaniem dostępu do wyników przetwarzania informacji.

Zabezpieczenia powiązane: Brak.

(3) KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA | OZNACZANIE URZĄDZEŃ WEJŚCIA - WYJŚCIA

[Wycofane: Włączone do PE-22].

Referencje: [IR 8023].

PE-6 MONITOROWANIE DOSTĘPU FIZYCZNEGO

Zabezpieczenie podstawowe:

a. Monitorowanie fizycznego dostępu do obiektu, w którym znajduje się system, w celu wykrywania i reagowania na incydenty związane z bezpieczeństwem fizycznym;

b. Przeglądanie dzienników dostępu fizycznego z częstotliwością [*Realizacja: częstotliwość określona przez organizację*] i po wystąpieniu [*Realizacja: zdarzenia określone przez organizację lub potencjalne wskazania zdarzeń*]; oraz

c. Koordynacja wyników przeprowadzanych przeglądów i dochodzeń z możliwościami reagowania na incydenty organizacyjne.

Omówienie: Monitorowanie dostępu fizycznego obejmuje ogólnodostępne obszary w obrębie obiektów organizacyjnych. Przykłady monitorowania dostępu fizycznego obejmują personel ochrony, monitoring wizyjny (np. kamery) oraz różnego rodzaju czujniki. Przeglądanie dzienników dostępu fizycznego może pomóc w zidentyfikowaniu podejrzanych działań, anomalnych zdarzeń lub potencjalnych zagrożeń. Przeglądy mogą być wspomagane przez zabezpieczenia rejestrów audytowych, takie jak zabezpieczenie AU-2, jeżeli rejestry dostępu są częścią zautomatyzowanego systemu. Możliwości reagowania na incydenty organizacyjne obejmują badanie incydentów związanych z bezpieczeństwem fizycznym i reagowanie na nie. Incydenty obejmują naruszenia bezpieczeństwa lub podejrzane działania związane z fizycznym dostępem. Podejrzane działania związane z fizycznym dostępem obejmują dostęp poza normalnymi godzinami pracy, wielokrotny dostęp do obszarów, do których nie ma normalnego dostępu, dostęp na nietypowy okres czasu oraz dostęp poza kolejnością.

Zabezpieczenia powiązane: AU-2, AU-6, AU-9, AU-12, CA-7, CP-10, IR-4, IR-8.

Zabezpieczenia rozszerzone:

(1) MONITOROWANIE DOSTĘPU FIZYCZNEGO | ALARMY WŁAMANIOWE I URZĄDZENIA NADZORUJĄCE

Monitorowanie fizycznego dostępu do obiektu, w którym znajduje się system, za pomocą systemów antywłamaniowych i urządzeń nadzorujących.

Omówienie: Systemy antywłamaniowe mogą być wykorzystywane do ostrzegania pracowników ochrony w przypadku próby nieautoryzowanego dostępu do obiektu. Systemy antywłamaniowe działają w połączeniu z barierami fizycznymi, systemami kontroli fizycznego dostępu i personelem ochrony, wywołując reakcję w przypadku zagrożenia lub naruszenia tych form ochrony. Systemy antywłamaniowe mogą obejmować różnego rodzaju sensory, takie jak czujniki ruchu, dotykowe i stłuczonego szkła. Urządzenia do nadzoru obejmują kamery wideo zainstalowane w strategicznych miejscach w całym obiekcie.

Zabezpieczenia powiązane: Brak.

(2) MONITOROWANIE DOSTĘPU FIZYCZNEGO | AUTOMATYCZNE ROZPOZNAWANIE WŁAMANIA / INFORMOWANIE

Rozpoznawanie [Realizacja: *klasy lub rodzaje włamań zdefiniowane przez organizację*] i inicjowanie [Realizacja: *działania reagowania zdefiniowane przez organizację*] wykorzystując [*Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację*].

Omówienie: Działania reagowania mogą obejmować powiadamianie wybranych przedstawicieli organizacji lub pracowników organów ścigania. Zautomatyzowane mechanizmy zaimplementowane w celu zainicjowania akcji reagowania obejmują powiadomienia o alarmach systemu, wiadomości e-mail i tekstowe oraz aktywowanie mechanizmów blokady drzwi. Monitorowanie dostępu fizycznego może być skoordynowane z systemami wykrywania włamań i możliwościami

systemu monitorowania w celu zapewnienia zintegrowanej ochrony organizacji przed zagrożeniami.

Zabezpieczenia powiązane: SI-4.

(3) MONITOROWANIE DOSTĘPU FIZYCZNEGO | MONITORING WIZYJNY

(a) Zastosowanie nadzoru wideo [***Realizacja: obszary operacyjne zdefiniowane przez organizację***]***;***

(b) Przeglądanie nagrań wideo [***Realizacja: częstotliwość określona przez organizację***]**; oraz**

(c) Przechowywanie nagrań wideo [***Realizacja: okres czasu określony przez organizację***]**.**

Omówienie: Monitoring wizyjny pozwala na rejestrowanie aktywności w określonych obszarach w celu późniejszego przeglądu, jeśli wymagają tego okoliczności. Nagrania wideo są zazwyczaj przeglądane w celu wykrycia anomalii lub incydentów. Monitoring wizyjny nie jest wymagany, choć organizacje mogą zdecydować się na jego wprowadzenie. Przy wykonywaniu i przechowywaniu monitoringu wideo mogą zaistnieć względy prawne, zwłaszcza, jeśli taki monitoring odbywa się w miejscu publicznym.

Zabezpieczenia powiązane: Brak.

(4) MONITOROWANIE DOSTĘPU FIZYCZNEGO | MONITOROWANIE DOSTĘPU FIZYCZNEGO DO SYSTEMÓW

Monitorowanie dostępu fizycznego do systemu w uzupełnieniu monitorowania dostępu fizycznego do obiektu w [***Realizacja: zdefiniowane organizacyjnie przestrzenie fizyczne zawierające jeden lub więcej komponentów systemu***]**.**

Omówienie: Monitorowanie dostępu fizycznego do systemów zapewnia dodatkowy monitoring tych obszarów w obiektach, w których występuje koncentracja komponentów systemu, w tym serwerowni, nośników danych i centrów komunikacyjnych. Monitorowanie dostępu fizycznego może być

skoordynowane z systemami wykrywania włamań i możliwościami monitorowania systemu w celu zapewnienia kompleksowej i zintegrowanej ochrony przed zagrożeniami dla organizacji.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

PE-7 KONTROLA GOŚCI

[Wycofane: Włączone do PE-2 i PE-3].

PE-8 REJESTRACJA DOSTĘPU GOŚCI

Zabezpieczenie podstawowe:

a. Prowadzenie ewidencji dostępu gości do obiektu, w którym znajduje się system przez [*Realizacja: okres czasu określony przez organizację*];

b. Przeglądanie zapisów dotyczących dostępu gości [*Realizacja: częstotliwość określona przez organizację*]; oraz

c. Zgłaszanie anomalii w rejestrach ewidencji odwiedzających [*Realizacja: personel określony przez organizację*].

Omówienie: Rejestry ewidencji odwiedzających obejmują nazwiska i organizacje osób odwiedzających, podpisy odwiedzających, formy identyfikacji, daty dostępu, godziny wejścia i wyjścia, cel wizyty oraz nazwiska i organizacje odwiedzanych osób. Przeglądy zapisów dostępu określają, czy uprawnienia dostępu są aktualne i nadal są wymagane do wspierania misji organizacji i funkcji biznesowych. Rejestry dostępu nie są wymagane w przypadku obszarów ogólnodostępnych.

Zabezpieczenia powiązane: PE-2, PE-3, PE-6.

Zabezpieczenia rozszerzone:

(1) REJESTRACJA DOSTĘPU GOŚCI | AUTOMATYCZNA REJESTRACJA / PRZEGLĄD

Utrzymywanie i przeglądanie ewidencji dostępu gości za pomocą [***Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację***]**.**

Omówienie: Ewidencja dostępu gości może być przechowywana i obsługiwana w systemie zarządzania bazą danych dostępnym dla personelu organizacji. Zautomatyzowany dostęp do takich zapisów ułatwia regularne przeglądanie zapisów w celu ustalenia, czy uprawnienia dostępu są aktualne i nadal wymagane do wspierania misji organizacji i funkcji biznesowych.

Zabezpieczenia powiązane: Brak.

(2) REJESTRACJA DOSTĘPU GOŚCI | EWIDENCJA DOSTĘPU FIZYCZNEGO

[Wycofane: Włączone do PE-2].

(3) REJESTRACJA DOSTĘPU GOŚCI | OGRANICZANIE ELEMENTÓW DANYCH OSOBOWYCH UMOŻLIWIAJĄCYCH IDENTYFIKACJĘ

Ograniczenie informacji umożliwiających identyfikację osób zawartych w ewidencji dostępu gości do następujących elementów określonych w ocenie wystąpienia ryzyka dotyczącego prywatności: [***Realizacja: elementy zdefiniowane przez organizację***]**.**

Omówienie: Organizacje powinny określić wymagania dotyczące zawartości ewidencji dostępu gości. Ograniczenie informacji umożliwiających identyfikację osób w rejestrach odwiedzających, gdy takie informacje nie są potrzebne do celów operacyjnych, pomaga zmniejszyć poziom zagrożenia prywatności stwarzanego przez system.

Zabezpieczenia powiązane: RA-3, SA-8.

Referencje: Brak.

PE-9 WYPOSAŻENIE ENERGETYCZNE I OKABLOWANIE

Zabezpieczenie podstawowe: Zabezpieczenie urządzeń zasilających i okablowania energetycznego systemu przed uszkodzeniem i zniszczeniem.

Omówienie: Organizacje określają rodzaje ochrony wymaganej dla urządzeń zasilających i okablowania energetycznego stosowanych w różnych lokalizacjach, znajdujących się zarówno wewnątrz, jak i na zewnątrz obiektów i środowisk działania organizacji. Rodzaje urządzeń zasilających i okablowania energetycznego obejmują okablowanie wewnętrzne i bezprzerwowe źródła zasilania w biurach lub centrach danych, agregaty prądotwórcze i okablowanie zasilające na zewnątrz budynków oraz źródła zasilania dla samodzielnych komponentów, takich jak systemy satelitarne, pojazdy i inne systemy możliwe do wdrożenia.

Zabezpieczenia powiązane: PE-4.

Zabezpieczenia rozszerzone:

(1) WYPOSAŻENIE ENERGETYCZNE I OKABLOWANIE | REDUNDANCJA OKABLOWANIA

Stosowanie nadmiarowych torów okablowania zasilającego, fizycznie oddzielonych od torów głównych [***Realizacja: odległość zdefiniowana przez organizację***]**.**

Omówienie: Fizycznie odseparowane i nadmiarowe kable zasilające zapewniają ciągłość zasilania w przypadku przecięcia lub innego uszkodzenia jednego z kabli.

Zabezpieczenia powiązane: Brak.

(2) WYPOSAŻENIE ENERGETYCZNE I OKABLOWANIE | AUTOMATYCZNA KONTROLA JAKOŚCI NAPIĘCIA

Stosowanie automatycznej kontroli jakości napięcia w [***Realizacja: zdefiniowane przez organizację krytyczne komponenty systemu***]**.**

Omówienie: Automatyczna kontroli jakości napięcia pozwala na monitorowanie i kontrolę poziom i rodzaj napięcia. Zapewniana jest m. in. przez regulatory napięcia, przetwornice napięcia i stabilizatory napięcia.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

PE-10 WYŁĄCZENIE AWARYJNE

Zabezpieczenie podstawowe:

a. Zapewnienie możliwości odcięcia zasilania [*Realizacja: system zdefiniowany przez organizację lub poszczególne komponenty systemu*] w sytuacjach awaryjnych;

b. Umieszczenie wyłączników awaryjnych lub urządzeń wyłączania awaryjnego w [*Realizacja: lokalizacja zdefiniowana przez organizację, w której znajduje się system lub komponent systemu*] w sposób umożliwiający upoważnionemu personelowi bezpieczny i łatwy dostęp; oraz

c. Zabezpieczenie wyłączników/ urządzeń wyłączania awaryjnego przed nieuprawnioną aktywacją.

Omówienie: Awaryjne wyłączanie zasilania dotyczy przede wszystkim obiektów organizacyjnych, w których występują skupiska zasobów systemowych, np. centra danych, serwerownie, pracownie komputerów typu mainframe oraz strefy z urządzeniami kontrolowanymi przez komputery.

Zabezpieczenia powiązane: PE-15.

Zabezpieczenia rozszerzone:

(1) WYŁĄCZENIE AWARYJNE | PRZYPADKOWA I NIEAUTORYZOWANA AKTYWACJA

[Wycofane: Włączone do PE-10].

Referencje: Brak.

PE-11 ZASILANIE AWARYJNE

Zabezpieczenie podstawowe: Zapewnienie gwarantowanego zasilania w celu umożliwienia [*Wybór (jeden lub więcej): wyłączenie systemu; przejście systemu na długoterminowe źródło zapasowe*] w przypadku utraty podstawowego źródła zasilania.

Omówienie: Zasilacz bezprzerwowy (UPS) to system lub mechanizm elektryczny, który zapewnia zasilanie awaryjne w przypadku awarii głównego źródła zasilania. Zasilacz UPS jest zwykle używany do ochrony komputerów, centrów danych, sprzętu telekomunikacyjnego lub innego sprzętu elektrycznego, w przypadku którego niespodziewana przerwa w dostawie prądu może spowodować obrażenia ciała, śmierć, poważne zakłócenia w pracy lub w działalności biznesowej, albo utratę danych lub informacji. Zasilacz UPS różni się od awaryjnego systemu zasilania lub generatora zapasowego tym, że zapewnia niemal natychmiastową ochronę przed nieprzewidzianymi przerwami w zasilaniu z głównego źródła, dostarczając energię zgromadzoną w akumulatorach, superkondensatorach lub akumulatorach energii kinetycznej. Czas pracy baterii zasilacza UPS jest stosunkowo krótki, ale zapewnia wystarczająco dużo czasu na uruchomienie rezerwowego źródła zasilania, takiego jak rezerwowy agregat prądotwórczy, lub na prawidłowe wyłączenie systemu.

Zabezpieczenia powiązane: NA 3, CP-2, CP-7.

Zabezpieczenia rozszerzone:

(1) ZASILANIE AWARYJNE | ALTERNATYWNE ZASILANIE - MINIMALNA ZDOLNOŚĆ OPERACYJNA

Zapewnienie alternatywnego źródła zasilania systemu aktywowanego [***Wybór: ręcznie; automatycznie***] **i które może utrzymać minimalną zdolność operacyjną w przypadku długotrwałej niedostępności podstawowego źródła zasilania.**

Omówienie: Zapewnienie alternatywnego źródła zasilania przy zachowaniu minimalnej zdolności operacyjnej może być spełnione poprzez dostęp do dodatkowego dostawcy energii elektrycznej lub innego zewnętrznego źródła zasilania.

Zabezpieczenia powiązane: Brak.

(2) ZASILANIE AWARYJNE | ALTERNATYWNE SAMOOBSŁUGOWE ŹRÓDŁO ZASILANIA

Zapewnienie alternatywnego źródła zasilania systemu aktywowanego [***Wybór: ręcznie; automatycznie***] **i które jest:**

a) Samoobsługowe (autostart);

(b) Niezależne od zewnętrznego przyłącza energetycznego; oraz

(c) Zdolne do utrzymania [***Wybór: minimalna wymagana zdolność operacyjna; pełna zdolność operacyjna***] **w przypadku długotrwałej utraty dostępności podstawowego źródła zasilania.**

Omówienie: Zapewnienie długoterminowego, samoobsługowego zasilania może być zaspokojone poprzez zastosowanie jednego lub kilku agregatów prądotwórczych o mocy wystarczającej do zaspokojenia potrzeb organizacji.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

PE-12 OŚWIETLENIE AWARYJNE

Zabezpieczenie podstawowe: Zastosowanie i utrzymanie automatycznego oświetlenia awaryjnego, które aktywuje się w przypadku przerwy w dostawie energii elektrycznej lub zakłócenia jej dostawy i które obejmuje wyjścia awaryjne i drogi ewakuacyjne na terenie obiektu.

Omówienie: Zapewnienie oświetlenia awaryjnego dotyczy przede wszystkim obiektów organizacyjnych, w których występują koncentracje zasobów systemowych, np.: centra danych, serwerownie, pracownie komputerów typu mainframe. Zapisy dotyczące oświetlenia awaryjnego systemu są opisane w planie awaryjnym organizacji. Jeżeli oświetlenie awaryjne systemu ulegnie awarii lub nie będzie mogło być zapewnione, organizacje rozważają zastosowanie alternatywnych miejsc przetwarzania na wypadek sytuacji awaryjnych związanych z zasilaniem.

Zabezpieczenia powiązane: CP-2, CP-7.

Zabezpieczenia rozszerzone:

(1) OŚWIETLENIE AWARYJNE | ZASADNICZE DZIAŁANIA / FUNKCJE BIZNESOWE

Zapewnienie oświetlenia awaryjnego we wszystkich pomieszczeniach w obiekcie, wspomagających realizację podstawowych zadań i funkcji biznesowych.

Omówienie: Organizacje określają własne podstawowe misje i funkcje.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

PE-13 OCHRONA PRZECIWPOŻAROWA

Zabezpieczenie podstawowe: Stosowanie i utrzymywanie systemów wykrywania i gaszenia pożaru, które są zasilane przez niezależne źródło energii.

Omówienie: Dostarczanie systemów wykrywania i gaszenia pożarów dotyczy przede wszystkim obiektów organizacyjnych, w których występują koncentracje zasobów systemowych, np. centra danych, serwerownie, pracownie komputerów typu mainframe. Systemy wykrywania i gaszenia pożaru, które mogą wymagać niezależnego źródła energii, obejmują systemy tryskaczowe i czujki dymu. Niezależnym źródłem energii może być mikrosieć elektroenergetyczna, która jest odseparowana lub może być oddzielona od źródeł zasilania dostarczających energię do innych części obiektu.

Zabezpieczenia powiązane: AT-3.

Zabezpieczenia rozszerzone:

(1) OCHRONA PRZECIWPOŻAROWA | SYSTEMY DETEKCJI - AUTOMATYCZNA AKTYWACJA I POWIADAMIANIE

Stosowanie systemów wykrywania pożaru, które aktywują się automatycznie i powiadamiają [***Realizacja: zdefiniowany przez organizację personel lub role***] **oraz** [***Realizacja: osoby reagujące na sytuacje kryzysowe określone przez organizację***] **w przypadku pożaru.**

Omówienie: Organizacje mogą określić personel, role i osoby odpowiedzialne za reagowanie w sytuacjach awaryjnych, jeżeli osoby znajdujące się na liście powiadamiania muszą posiadać uprawnienia dostępu i/lub poświadczenia osobowe (np. w celu wejścia do obiektów, do których dostęp jest ograniczony ze względu na klauzulę niejawności lub poziom wpływu informacji przetwarzanych w obiekcie). Mechanizmy powiadamiania mogą wymagać niezależnych źródeł

energii, aby zapewnić, że pożar nie będzie miał negatywnego wpływu na zdolność powiadamiania.

Zabezpieczenia powiązane: Brak.

(2) OCHRONA PRZECIWPOŻAROWA | SYSTEMY GASZĄCE - AUTOMATYCZNA AKTYWACJA I POWIADOMIENIE

(a) Stosowanie systemów gaszenia pożaru, które aktywują się automatycznie i powiadamiają [***Realizacja: zdefiniowany przez organizację personel lub role***] **oraz** [***Realizacja: zdefiniowani przez organizację ratownicy***]**; oraz**

(b) Stosowanie automatycznych środków gaśniczych, gdy w obiekcie nie jest wykonywana praca zmianowa (ciągła).

Omówienie: Organizacje mogą określić personel, role i osoby odpowiedzialne za reagowanie w sytuacjach awaryjnych, jeżeli osoby znajdujące się na liście powiadamiania muszą posiadać uprawnienia dostępu i/lub poświadczenia osobowe (np. w celu wejścia do obiektów, do których dostęp jest ograniczony ze względu na klauzulę niejawności lub poziom wpływu informacji przetwarzanych w obiekcie). Mechanizmy powiadamiania mogą wymagać niezależnych źródeł energii, aby zapewnić, że pożar nie wpłynie negatywnie na zdolność powiadamiania.

Zabezpieczenia powiązane: Brak.

(3) OCHRONA PRZECIWPOŻAROWA | AUTOMATYCZNE GASZENIE POŻARU

[Wycofane: Włączone do PE-13(2)]

(4) OCHRONA PRZECIWPOŻAROWA | INSPEKCJE

Zapewnienie, że obiekt jest poddawany inspekcji ochrony przeciwpożarowej [Realizacja: ***częstotliwość określona przez organizację***] **przez upoważniony i wykwalifikowany personel, a stwierdzone niedociągnięcia są usuwane w ciągu** [***Realizacja: okres określony przez organizację***]**.**

Omówienie: Upoważniony i wykwalifikowany personel obejmuje inspektorów ppoż. lub specjalistów ppoż. Organizacje zapewniają asystę podczas inspekcji ppoż. prowadzonych w sytuacjach, gdy systemy znajdujące się na terenie obiektu przetwarzają informacje wrażliwe.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

PE-14 ZABEZPIECZENIA ŚRODOWISKOWE

Zabezpieczenie podstawowe:

a. Utrzymywanie w obiekcie, w którym znajduje się system [*Wybór (jeden lub więcej): temperatura; wilgotność; ciśnienie; promieniowanie;* [*Realizacja: zdefiniowane przez organizację zabezpieczenia środowiskowa*]], na poziomie [*Realizacja: zdefiniowane przez organizację dopuszczalne poziomy*]; oraz

b. Monitorowanie poziomów zabezpieczeń środowiskowych [*Realizacja: częstotliwość zdefiniowana przez organizację*].

Omówienie: Zapewnienie zabezpieczeń środowiskowych dotyczy przede wszystkim obiektów organizacyjnych, w których występują koncentracje zasobów systemowych, np. centra danych, serwerownie i pracownie komputerów typu mainframe. Niedostateczne zabezpieczenie środowiskowe, szczególnie w bardzo surowych warunkach, może mieć istotny negatywny wpływ na dostępność systemów i komponentów systemowych, które są niezbędne do wspierania misji organizacji i funkcji biznesowych.

Zabezpieczenia powiązane: AT-3, CP-2.

Zabezpieczenia rozszerzone:

(1) ZABEZPIECZENIA ŚRODOWISKOWE | STEROWANIE AUTOMATYCZNE

Stosowanie następujących automatycznych zabezpieczeń środowiskowych w obiekcie, aby zapobiec potencjalnie szkodliwym dla systemu fluktuacjom: [***Realizacja: zdefiniowane przez organizację automatyczne zabezpieczenie środowiskowa***]**.**

Omówienie: Wdrożenie automatycznych zabezpieczeń środowiskowych zapewnia natychmiastową reakcję na warunki środowiskowe, które mogą uszkodzić, pogorszyć lub zniszczyć systemy organizacyjne lub komponenty systemów.

Zabezpieczenia powiązane: Brak.

(2) ZABEZPIECZENIA ŚRODOWISKOWE | MONITOROWANIE, ALARMOWANIE / POWIADOMIENIA

Monitorowanie zabezpieczeń środowiskowych, zapewniając alarmowanie lub powiadamianie o zmianach potencjalnie szkodliwych dla personelu lub urządzeń [***Realizacja: zdefiniowany przez organizację personel lub role***]**.**

Omówienie: Alarmowanie lub powiadamianie może mieć postać alarmu dźwiękowego lub komunikatu wizualnego informującego w czasie rzeczywistym personel lub role określone przez organizację. Takie alarmy i powiadomienia mogą pomóc w zminimalizowaniu szkód w odniesieniu do osób i majątku organizacji poprzez podjęcie szybkiej reakcji na incydent.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

PE-15 OCHRONA PRZED ZALANIEM

Zabezpieczenie podstawowe: Zabezpieczanie systemu przed uszkodzeniami wynikającymi z wycieku wody, zapewniając główne zawory odcinające lub separujące, które są łatwo dostępne, działają prawidłowo, a ich rozmieszczenie znane jest kluczowemu personelowi.

Omówienie: Zapewnienie ochrony przed szkodami wynikającymi z wycieku wody dotyczy przede wszystkim obiektów organizacyjnych, w których występują koncentracje zasobów systemowych, np. centra danych, serwerownie, pracownie komputerów typu mainframe. Zawory izolacyjne mogą być stosowane dodatkowo lub zamiast głównych zaworów odcinających w celu odcięcia dostaw wody w ściśle określonych obszarach bez wpływu na całą organizację.

Zabezpieczenia powiązane: AT-3, PE-10.

Zabezpieczenia rozszerzone:

(1) OCHRONA PRZED ZALANIEM | AUTOMATYCZNE WYKRYWANIE

Wykrywanie obecności wody w pobliżu systemu i alarmowanie [Realizacja: *personel określony przez organizację lub role*] przy użyciu [*Realizacja: zautomatyzowane mechanizmy określone przez organizację*].

Omówienie: Zautomatyzowane mechanizmy obejmują systemy powiadamiania, czujniki wykrywania wody i alarmy.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

PE-16 DOSTAWA I USUWANIE

Zabezpieczenie podstawowe:

a. Autoryzacja i zabezpieczenie [*Realizacja: zdefiniowane przez organizację typy komponentów systemu*] dostarczane i usuwane z obiektu; oraz

b. Prowadzenie ewidencji komponentów systemu.

Omówienie: Egzekwowanie zezwoleń na dostawę i usuwanie komponentów systemu może wymagać ograniczania dostępu do obszarów dostaw oraz odizolowania tych obszarów od systemu i zasobów.

Zabezpieczenia powiązane: CM-3, CM-8, MA-2, MA-3, MP-5, PE-20, SR-2, SR-3, SR-4, SR-6.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

PE-17 ZAPASOWE MIEJSCE PRACY

Zabezpieczenie podstawowe:

a. Ustalenie i udokumentowanie [*Realizacja: zdefiniowane przez organizację zapasowe miejsca pracy*] wyznaczone do używania przez personel;

b. Wprowadzenie [*Realizacja: środki bezpieczeństwa zdefiniowane przez organizację*] w zapasowych miejscach pracy*;*

c. Ocenianie skuteczność zabezpieczeń stosowanych w zapasowych miejscach pracy; oraz

d. Zapewnienie pracownikom środków umożliwiających komunikację z personelem ds. bezpieczeństwa informacji i ochrony prywatności w przypadku wystąpienia incydentów lub problemów związanych z bezpieczeństwem.

Omówienie: Zapasowe miejsca pracy obejmują obiekty państwowe lub prywatne posesje pracowników. Chociaż różnią się one od zapasowych miejsc przetwarzania danych, mogą zapewnić łatwo dostępne alternatywne miejsca pracy podczas operacji awaryjnych. Organizacje mogą zdefiniować różne zestawy zabezpieczeń poszczególnych zapasowych miejsc pracy lub rodzajów miejsc pracy, w zależności od rodzaju pracy wykonywanej w tych miejscach. Wdrożenie i ocena skuteczności zabezpieczeń zdefiniowanych przez organizację oraz zapewnienie środków komunikacji w zapasowych miejscach pracy wspiera działania organizacji w zakresie planowania awaryjnego.

Zabezpieczenia powiązane: AC-17, AC-18, CP-7.

Zabezpieczenia rozszerzone: Brak.

Referencje: [NIST SP 800-46].

PE-18 LOKALIZACJA KOMPONENTÓW SYSTEMU

Zabezpieczenie podstawowe: Stosowne rozmieszczenie komponentów systemu w obiekcie w celu zminimalizowania potencjalnych szkód wynikających z [*Realizacja: zdefiniowane przez organizację zagrożenia fizyczne i środowiskowe*] oraz zminimalizowania możliwości dostępu osób nieupoważnionych.

Omówienie: Zagrożenia fizyczne i środowiskowe obejmują powodzie, pożary, trzęsienia ziemi, wichury, terroryzm, wandalizm, impuls elektromagnetyczny, zakłócenia elektromagnetyczne i inne formy docierającego promieniowania elektromagnetycznego. Organizacje biorą pod uwagę lokalizację obszarów wejściowych, umożliwiających dostęp do systemów osobom nieupoważnionym, które, mimo że nie mają do nich dostępu, mogą przebywać w ich bezpośredniej bliskości. Taka bliskość może zwiększyć ryzyko nieautoryzowanego dostępu do komunikacji organizacyjnej przy użyciu bezprzewodowych snifferów pakietów lub mikrofonów, bądź nieautoryzowanego ujawnienia informacji.

Powiązane kontrole:

Zabezpieczenia powiązane: CP-2, PE-5, PE-19, PE-20, RA-3.

(1) LOKALIZACJA KOMPONENTÓW SYSTEMU | LOKALIZACJA OBIEKTU

[Wycofany: przeniesiony na PE-23].

Referencje: Brak.

PE-19 ULOT INFORMACJI / ELEKTROMAGNETYCZNA EMISJA UJAWNIAJĄCA

Zabezpieczenie podstawowe: Zabezpieczanie systemu przed ulotem informacji spowodowanym promieniowaniem sygnałów elektromagnetycznych, tzw. elektromagnetyczną emisją ujawniającą.

Omówienie: Ulot informacji to celowe lub niezamierzone przekazywanie danych lub informacji do niezaufanego środowiska w wyniku elektromagnetycznej emisji ujawniającej. Kategorie bezpieczeństwa lub klasyfikacje systemów (w odniesieniu do klasyfikacji informacji), polityka bezpieczeństwa organizacji oraz tolerancja ryzyka stanowią wytyczne do wyboru środków bezpieczeństwa stosowanych w celu ochrony systemów przed ulotem informacji z powodu elektromagnetycznej emisji ujawniającej.

Zabezpieczenia powiązane: AC-18, PE-18, PE-20.

Zabezpieczenia rozszerzone:

(1) ULOT INFORMACJI / ELEKTROMAGNETYCZNA EMISJA UJAWNIAJĄCA | KRAJOWE POLITYKI I PROCEDURY DOTYCZĄCE EMISJI UJAWNIAJĄCEJ

Zabezpieczanie komponentów systemu, powiązanej transmisji danych i sieci zgodnie z krajowymi politykami i procedurami dotyczącymi emisji ujawniającej w oparciu o kategorię bezpieczeństwa lub klasyfikację informacji.

Omówienie: Polityki bezpieczeństwa emisji (*ang. Emissions Security - EMSEC*) obejmują dotychczasowe polityki TEMPEST.

Zabezpieczenia powiązane: Brak.

Referencje: [FIPS 199].

PE-20 MONITOROWANIE I ŚLEDZENIE ZASOBÓW

Zabezpieczenie podstawowe: Stosowanie [*Realizacja: technologie lokalizacji zasobów określone przez organizację*] do śledzenia i monitorowania lokalizacji i przemieszczania [Realizacja: *zasoby określone przez organizację*] w ramach [*Realizacja: obszary kontrolowane określone przez organizację*].

Omówienie: Technologie lokalizacji zasobów mogą przyczynić się do uzyskania pewności, że zasoby krytyczne - w tym środki transportu, sprzęt i komponenty systemu - pozostaną w autoryzowanych lokalizacjach. Organizacje konsultują się z inspektorem danych lub SAOP[61] w zakresie wdrażania i wykorzystywania technologii lokalizacji zasobów w celu rozwiązania potencjalnych problemów związanych z ochroną prywatności.

Zabezpieczenia powiązane: CM-8, PE-16, PM-8.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

[61] Patrz: NSC 800-37; NSC 7298.

PE-21 OCHRONA PRZED IMPULSEM ELEKTROMAGNETYCZNYM

Zabezpieczenie podstawowe: Stosowanie [Realizacja: zdefiniowane w *organizacji środki ochronnych*] zapobiegające uszkodzeniom spowodowanym impulsem elektromagnetycznym [*Realizacja: zdefiniowane przez organizację systemy i komponenty systemu*].

Omówienie: Impuls elektromagnetyczny (*ang. electromagnetic pulse - EMP*) to impuls energii elektromagnetycznej, o szerokim widmie stosunkowo niskich częstotliwościach, krótkim czasie trwania i bardzo dużym natężeniu. Takie wybuchy energii mogą być naturalne lub spowodowane przez człowieka. Zakłócenia EMP mogą być uciążliwe lub szkodliwe dla sprzętu elektronicznego. Środki ochronne stosowane w celu zmniejszenia ryzyka EMP obejmują ekranowanie, tłumiki przepięć, transformatory ferrorezonansowe oraz uziemienie. Ochrona EMP może mieć szczególne znaczenie w przypadku systemów i zastosowań, które stanowią część infrastruktury krytycznej.

Zabezpieczenia powiązane: PE-18, PE-19.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

PE-22 ZNAKOWANIE KOMPONENTÓW

Zabezpieczenie podstawowe: Znakowanie [*Realizacja: zdefiniowane przez organizację komponenty sprzętowe systemu*] wskazujące poziom wpływu lub klasyfikację informacji, które mogą być przetwarzane przez komponent sprzętowy.

Omówienie: Komponenty sprzętowe, które mogą wymagać znakowania, obejmują urządzenia wejścia i wyjścia. Urządzenia wejścia to komputery stacjonarne i notebooki, klawiatury, tablety i smartfony. Urządzenia wyjścia obejmują drukarki, monitory/wyświetlacze wideo, faksy, skanery, kopiarki i urządzenia audio. Kontrola dostępu do urządzeń wyjściowych jest omawiana w zabezpieczeniach AC-3 i AC-4. Komponenty są znakowane w celu wskazania poziomu wpływu lub klasyfikacji systemu, do którego podłączone są urządzenia, lub poziomu wpływu lub klasyfikacji informacji, które mogą być przetwarzane. Oznaczanie poziomów bezpieczeństwa odnosi się do stosowania atrybutów bezpieczeństwa umożliwiających ich odczytanie przez personel. Etykietowanie bezpieczeństwa dotyczy stosowania atrybutów bezpieczeństwa w odniesieniu do wewnętrznych struktur danych systemu. Oznaczanie poziomów bezpieczeństwa nie jest zazwyczaj wymagane w przypadku komponentów sprzętu, które przetwarzają informacje określone przez organizacje, jako będące własnością publiczną lub możliwe do publicznego udostępnienia. Organizacje mogą jednak wymagać znakowania komponentów sprzętowych przetwarzających informacje publiczne w celu wskazania, że takie informacje są publicznie dostępne. Znakowanie komponentów sprzętowych systemu odzwierciedla obowiązujące przepisy prawa, rozporządzenia, dyrektywy, zasady, regulacje i standardy.

Zabezpieczenia powiązane: AC-3, AC-4, AC-16, MP-3.

Zabezpieczenia rozszerzone: Brak.

Referencje: [IR 8023].

PE-23 LOKALIZACJA OBIEKTU

Zabezpieczenie podstawowe:

a. Planowanie lokalizacji lub miejsca posadowienia obiektu, w którym znajduje się system, uwzględniając zagrożenia fizyczne i środowiskowe; oraz

b. Uwzględnianie w strategii zarządzania ryzykiem organizacyjnym zagrożeń fizycznych i środowiskowych w odniesieniu do istniejących obiektów.

Omówienie: Zagrożenia fizyczne i środowiskowe obejmują powodzie, pożary, trzęsienia ziemi, wichury, terroryzm, wandalizm, impuls elektromagnetyczny, zakłócenia elektromagnetyczne i inne formy docierającego promieniowania elektromagnetycznego. Rozmieszczenie komponentów systemu na terenie obiektu jest omówione w zabezpieczeniu PE-18.

Zabezpieczenia powiązane: CP-2, PE-18, PE-19, PM-8, PM-9, RA-3.

KATEGORIA PL – PLANOWANIE

PL-1 POLITYKA I PROCEDURY

Zabezpieczenie podstawowe:

a. Opracowywanie, dokumentowanie i rozpowszechnianie wśród [Realizacja: *personel lub role określone przez organizację*]:

   1. [*Wybór (jeden lub więcej): poziom organizacji; poziom misji/procesu biznesowego; poziom systemu*] polityki planowania, która:

      (a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami; oraz

      (b) Jest zgodna z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi; oraz

   2. Procedur ułatwiających wdrożenie polityki planowania oraz powiązanych zabezpieczeń w zakresie planowania;

b. Wyznaczanie [Realizacja: *osoba wyznaczona przez organizację*] do zarządzania rozwojem, dokumentacją i rozpowszechnianiem polityki i procedur planowania; oraz

c. Przeglądanie i aktualizacja bieżącej:

   1. Polityki planowania z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*]; oraz

   2. Procedur planowania z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*].

Omówienie: Polityka i procedury w zakresie planowania dotyczą zabezpieczeń w kategorii *Planowanie* (PL), które są wdrażane w ramach systemów i organizacji. Strategia zarządzania ryzykiem jest ważnym czynnikiem przy tworzeniu takich polityk i procedur. Polityki i procedury przyczyniają się do zapewnienia bezpieczeństwa

i ochrony prywatności. Dlatego ważne jest, aby programy bezpieczeństwa i ochrony prywatności były opracowywane wspólnie przy kształtowaniu polityki i procedur planowania. Polityki i procedury dotyczące programów bezpieczeństwa i ochrony prywatności na poziomie organizacji są ogólnie rzecz biorąc preferowane i mogą eliminować potrzeby tworzenia polityk i procedur specyficznych dla danej misji lub systemu. Polityka może być włączona, jako część ogólnej polityki bezpieczeństwa i ochrony prywatności lub reprezentowana przez wiele polityk odzwierciedlających złożony charakter organizacji. Procedury mogą być ustanowione dla programów bezpieczeństwa i ochrony prywatności, dla misji lub procesów biznesowych oraz dla systemów, jeśli to konieczne. Procedury opisują sposób wdrażania zasad lub zabezpieczeń i mogą być skierowane do osoby lub roli, która jest przedmiotem procedury. Procedury mogą być udokumentowane w planach bezpieczeństwa i ochrony prywatności systemu w jednym lub kilku oddzielnych dokumentach.

Zdarzenia, które mogą spowodować konieczność aktualizacji polityki i procedur planowania, obejmują wyniki oceny lub audytu, incydenty lub naruszenia bezpieczeństwa, lub zmiany w przepisach prawa, zarządzeniach, dyrektywach, rozporządzeniach, zasadach, standardach i wytycznych.

Oświadczenie o wprowadzeniu zabezpieczeń nie jest równoznaczne z ustanowieniem polityki lub procedury organizacyjnej.

Zabezpieczenia powiązane: PM-9, PS-8, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [NIST SP 800-12], [NIST SP 800-18], [NIST SP 800-30], [NIST SP 800-39], [NIST SP 800-100].

PL-2 PLANY BEZPIECZEŃSTWA SYSTEMU I OCHRONY PRYWATNOŚCI

Zabezpieczenie podstawowe:

a. Opracowanie planów bezpieczeństwa i ochrony prywatności dla systemu, które:

1. Są zgodne z architekturą korporacyjną organizacji;
2. Jednoznacznie określają składowe komponentów systemu;
3. Opisują środowisko operacyjne systemu w kontekście misji i procesów biznesowych;
4. Identyfikują osoby pełniące role i obowiązki w systemie;
5. Identyfikują typy informacji przetwarzanych, przechowywanych i przesyłanych przez system;
6. Zapewniają kategoryzację bezpieczeństwa systemu, łącznie z uzasadnieniem;
7. Opisują wszelkie zagrożenia specyficzne dla systemu, które dotyczą organizacji;
8. Przedstawiają wyniki oceny ryzyka związanego z ochroną prywatności w systemach przetwarzających dane osobowe;
9. Opisują środowisko operacyjne systemu oraz wszelkie zależności lub połączenia z innymi systemami lub komponentami systemu;
10. Przedstawiają przegląd wymagań dotyczących bezpieczeństwa i ochrony prywatności systemu;
11. Określają wszelkie istotne zabezpieczenia bazowe lub nakładki, jeśli mają zastosowanie;
12. Opisują istniejące lub planowane zabezpieczenia mające na celu spełnienie wymogów bezpieczeństwa i ochrony prywatności, w tym uzasadnienie wszelkich decyzji dotyczących dostosowywania zabezpieczeń;

13. Uwzględnienie określenia ryzyka dla architektury i decyzji projektowych dotyczących bezpieczeństwa i prywatności;

14. Obejmują działania związane z bezpieczeństwem i ochroną prywatności mające wpływ na system, które wymagają planowania i koordynacji z [*Realizacja: osoby lub grupy określone przez organizację*]; oraz

15. Są weryfikowane i zatwierdzane przez osobę autoryzującą lub wyznaczonego przedstawiciela przed wprowadzeniem w życie planu.

b. Dystrybuowanie kopii planów i przekazywanie kolejnych zmian w planach personelowi [*Realizacja: personel lub role określone przez organizację*];

c. Przeglądanie planów [*Realizacja: częstotliwość określona przez organizację*];

d. Aktualizowanie planów w celu uwzględnienia zmian w systemie i środowisku działania lub problemów zidentyfikowanych podczas wdrażania planu lub przeprowadzanych ocen zabezpieczeń; oraz

e. Chronienie planów przed nieautoryzowanym ujawnieniem i modyfikacją.

Omówienie: Plany bezpieczeństwa i ochrony prywatności systemu są ograniczone do systemu i jego komponentów w ramach zdefiniowanych granic autoryzacyjnych i zawierają przegląd wymagań dotyczących bezpieczeństwa i ochrony prywatności systemu oraz zabezpieczeń wybranych w celu spełnienia tych wymagań. Plany opisują zamierzone zastosowanie każdego z wybranych zabezpieczeń w kontekście systemu z wystarczającym poziomem szczegółowości, aby prawidłowo zaimplementować zabezpieczenie i następnie ocenić jego skuteczność. Dokumentacja zabezpieczeń opisuje sposób realizacji zabezpieczeń specyficznych dla systemu i zabezpieczeń hybrydowych oraz plany i oczekiwania dotyczące funkcjonalności systemu. Plany bezpieczeństwa i ochrony prywatności systemu mogą być również wykorzystywane przy projektowaniu i rozwoju cyklu życia systemów wspierających procesy inżynierii bezpieczeństwa i ochrony prywatności. Plany bezpieczeństwa i ochrony prywatności systemu są stale aktualizowane i dostosowywane podczas

całego cyklu życia systemu (np. podczas określania zdolności, analizy alternatyw, zapytań ofertowych i przeglądów projektu). W rozdziale 2.1 opisano różne rodzaje wymagań, które są istotne dla organizacji w trakcie cyklu życia systemu oraz relacje między wymaganiami, a zabezpieczeniami.

Organizacje mogą opracować jeden, zintegrowany plan bezpieczeństwa i ochrony prywatności lub utrzymywać oddzielne plany. Plany bezpieczeństwa i ochrony prywatności wiążą wymogi bezpieczeństwa i ochrony prywatności z zestawem środków bezpieczeństwa i zabezpieczeń rozszerzonych. Plany te opisują, w jaki sposób zabezpieczenia podstawowe i zabezpieczenia rozszerzone spełniają wymagania dotyczące bezpieczeństwa i ochrony prywatności, ale nie zawierają szczegółowych, technicznych opisów projektu lub wdrożenia zabezpieczeń podstawowych i zabezpieczeń rozszerzonych. Plany bezpieczeństwa i ochrony prywatności zawierają wystarczające informacje (w tym specyfikacje wartości parametrów zabezpieczeń dla operacji wyboru i przypisania, przez bezpośrednie przyporządkowanie lub przez odniesienie), aby umożliwić rozwój i wdrożenie, które jest jednoznacznie zgodne z intencjami planów i późniejszymi ustaleniami dotyczącymi ryzyka dla operacji organizacyjnych i aktywów, osób, innych organizacji i Państwa.

Plany bezpieczeństwa i ochrony prywatności nie muszą być pojedynczymi dokumentami. Plany mogą być zbiorem różnych dokumentów, w tym dokumentów już istniejących. Skuteczne plany bezpieczeństwa i ochrony prywatności w szerokim zakresie wykorzystują odniesienia do polityk, procedur i dodatkowych dokumentów, w tym specyfikacje projektowe i wykonawcze, w których można uzyskać bardziej szczegółowe informacje. Stosowanie odniesień pomaga zmniejszyć ilość dokumentacji związanej z programami bezpieczeństwa i ochrony prywatności oraz utrzymuje informacje związane z bezpieczeństwem i ochroną prywatności w innych ustalonych obszarach zarządzania i funkcjonowania, w tym w architekturze korporacyjnej, cyklu życia systemu, inżynierii systemów i procesie nabywania. Plany bezpieczeństwa i ochrony prywatności nie muszą zawierać szczegółowych informacji

o planach awaryjnych lub planach reagowania na incydenty, mogą natomiast dostarczać - w sposób wyraźny lub poprzez odniesienia - wystarczających informacji do określenia, co należy osiągnąć za pomocą tych planów.

Działania związane z bezpieczeństwem i ochroną prywatności, które mogą wymagać koordynacji i planowania z innymi osobami lub grupami w organizacji, obejmują oceny, audyty, inspekcje, konserwację sprzętu i oprogramowania, zarządzanie ryzykiem związanym z zakupami i łańcuchem dostaw, zarządzanie poprawkami oraz testowanie planów awaryjnych. Planowanie i koordynacja obejmują sytuacje awaryjne i inne niż awaryjne (tj. zaplanowane lub nieplanowane w trybie pilnym). Zdefiniowany przez organizacje proces planowania i koordynacji działań związanych z bezpieczeństwem i ochroną prywatności może być również uwzględniony w innych dokumentach, w zależności od potrzeb.

Zabezpieczenia powiązane: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CM-13, CP-2, CP-4, IR-4, IR-8, MA-4, MA-5, MP-4, MP-5, PL-7, PL-8, PL-10, PL-11, PM-1, PM-7, PM-8, PM-9, PM-10, PM-11, RA-3, RA-8, RA-9, SA-17, SA-22, SI-12, SR-2, SR-4.

Zabezpieczenia rozszerzone:

(1) PLANY BEZPIECZEŃSTWA SYSTEMU I OCHRONY PRYWATNOŚCI | KONCEPCJA DZIAŁANIA

[Wycofane: Włączone do PL-7].

(2) PLANY BEZPIECZEŃSTWA SYSTEMU I OCHRONY PRYWATNOŚCI | ARCHITEKTURA FUNKCJONALNA

[Wycofane: Włączone do PL-8].

(3) PLANY BEZPIECZEŃSTWA SYSTEMU I OCHRONY PRYWATNOŚCI | PLANOWANIE / KOORDYNACJA Z INNYMI PODMIOTAMI ORGANIZACYJNYMI

[Wycofane: Włączone do PL-2].

Referencje: [OMB A-130], [NIST SP 800-18], [NIST SP 800-37], [NIST SP 800-160-1], [NIST SP 800-160-2].

PL-3 AKTUALIZACJA PLANU BEZPIECZEŃSTWA SYSTEMU

[Wycofane: Włączone do PL-2].

PL-4 ZASADY POSTĘPOWANIA

Zabezpieczenie podstawowe:

a. Ustanowienie i zapewnienie osobom wymagającym dostępu do systemu zasad, które opisują ich obowiązki i oczekiwane zachowanie w zakresie korzystania z informacji i systemu, bezpieczeństwa i ochrony prywatności;

b. Przed wydaniem zezwolenia na dostęp do informacji i systemu należy uzyskać od tych osób udokumentowane potwierdzenie, że przeczytały, zrozumiały i zgadzają się przestrzegać ustanowione zasady postępowania;

c. Przeglądanie i aktualizowanie zasad zachowania [*Realizacja: częstotliwość określona przez organizację*]; oraz

d. Wymaganie od osób, które zapoznały się z poprzednią wersją zasad zachowania, ponownego przeczytania i podpisania tych reguł [*Wybór (jeden lub więcej)*]: [*Realizacja: częstotliwość określona przez organizację*]; *gdy zasady są zmieniane lub aktualizowane*].

Omówienie: Zasady zachowania stanowią rodzaj umowy dostępu dla użytkowników organizacyjnych. Inne rodzaje umów o dostępie obejmują umowy o nieujawnianiu informacji, umowy o konflikcie interesów oraz umowy o dopuszczalnym użytkowaniu (patrz zabezpieczenie PS-6). Organizacje biorą pod uwagę reguły zachowania oparte na indywidualnych rolach i obowiązkach użytkowników oraz rozróżniają reguły, które odnoszą się do użytkowników uprzywilejowanych i reguły, które odnoszą się do użytkowników ogólnych. Ustanowienie reguł zachowania dla nie których typów użytkowników nieorganizacyjnych, w tym osób otrzymujących informacje z systemów państwowych, jest często niewykonalne ze względu na dużą liczbę takich użytkowników i ograniczony charakter ich interakcji z systemami. Reguły zachowania dla użytkowników organizacyjnych i nieorganizacyjnych można również ustanowić w zabezpieczeniu AC-8. Powiązana sekcja zabezpieczeń zawiera listę zabezpieczeń, które są istotne dla organizacyjnych zasad zachowania. Zabezpieczenie PL-4b, dokumentujące potwierdzenie zapoznania się z zabezpieczeniami, może być

usatysfakcjonowane szkoleniami w zakresie uświadamiania bezpieczeństwa oraz programami szkoleniowymi opartymi na świadomości i roli prowadzonymi przez organizacje, jeśli takie szkolenia zawierają zasady zachowania. Udokumentowane potwierdzenia reguł zachowania obejmują podpisy elektroniczne lub fizyczne oraz elektroniczne checkboxy lub elektroniczne zaznaczenia zgody.

Zabezpieczenia powiązane: AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5, SI-12.

Zabezpieczenia rozszerzone:

(1) ZASADY POSTĘPOWANIA | MEDIA SPOŁECZNOŚCIOWE I OGRANICZENIA KORZYSTANIA ZE STRON / APLIKACJI ZEWNĘTRZNYCH

Włączenie do zasad zachowania, ograniczenia:

(a) Korzystania z mediów społecznościowych, portali społecznościowych i zewnętrznych stron/aplikacji;

(b) Umieszczania informacji organizacyjnych na publicznych stronach internetowych; oraz

(c) Wykorzystywania identyfikatorów dostarczonych przez organizację (np. adresów e-mail) i sekretów uwierzytelniania (np. haseł) do tworzenia kont na zewnętrznych stronach/aplikacjach.

Omówienie: Ograniczenia w korzystaniu z mediów społecznościowych, sieci społecznościowych i zewnętrznych witryn/aplikacji dotyczą zasad zachowania związanych z korzystaniem z mediów społecznościowych, sieci społecznościowych i zewnętrznych witryn, które są używane przez personel organizacyjny do wykonywania obowiązków służbowych lub prowadzenia oficjalnej działalności; gdy informacje organizacyjne są wykorzystywane do transakcji w mediach społecznościowych i sieciach społecznościowych; oraz gdy personel uzyskuje dostęp do mediów społecznościowych i sieci społecznościowych z systemów organizacyjnych. Organizacje zwracają również uwagę na szczególne zasady, które

uniemożliwiają nieuprawnionym podmiotom uzyskiwanie niepublicznych informacji organizacyjnych z serwisów społecznościowych i portali społecznościowych bezpośrednio lub przez inferencje. Informacje niepubliczne obejmują dane osobowe oraz informacje o kontach systemowych.

Zabezpieczenia powiązane: AC-22, AU-13.

Referencje: [OMB A-130], [NIST SP 800-18].

PL-5 OCENA WPŁYWU NA PRYWATNOŚĆ

[Wycofane: Włączone do RA-8].

[Zgodnie z Ogólnym Rozporządzeniem o Ochronie Danych Osobowych 2016/679 (RODO)].

PL-6 PLANOWANIE DZIAŁALNOŚCI ZWIĄZANEJ Z BEZPIECZEŃSTWEM

[Wycofane: Włączone do PL-2].

PL-7 KONCEPCJA BEZPIECZEŃSTWA DZIAŁAŃ OPERACYJNYCH

Zabezpieczenie podstawowe:

a. Opracowanie koncepcji działań operacyjnych (*ang. concept of operations - CONOPS*) opisującej sposób, w jaki organizacja zamierza obsługiwać system z punktu widzenia bezpieczeństwa informacji i ochrony prywatności; oraz

b. Przeglądanie i aktualizacja CONOPS [*Realizacja: częstotliwość określona przez organizację*].

Omówienie: CONOPS może być zawarty w planach bezpieczeństwa lub ochrony prywatności dla systemu lub w innych dokumentach dotyczących cyklu życia systemu. CONOPS jest dokumentem wymagającym aktualizacji w całym cyklu życia systemu. Na przykład, podczas przeglądów projektu systemu, sprawdzana jest koncepcja działania w celu zapewnienia, że pozostaje ona zgodna z projektem zabezpieczeń, architekturą systemu i procedurami operacyjnymi. Zmiany w CONOPS są odzwierciedlane w bieżących aktualizacjach planów bezpieczeństwa i ochrony prywatności, architektur bezpieczeństwa i ochrony prywatności oraz innych dokumentach organizacyjnych, takich jak specyfikacje zamówień, dokumenty dotyczące cyklu życia systemu oraz dokumenty inżynieryjne systemu.

Zabezpieczenia powiązane: PL-2, SA-2, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130].

PL-8 ARCHITEKTURY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Zabezpieczenie podstawowe:

a. Opracowanie architektury bezpieczeństwa i ochrony prywatności dla systemu, która opisuje:

   1. Wymagania i podejście, jakie należy zastosować w celu ochrony poufności, integralności i dostępności informacji organizacyjnych;

   2. Wymagania i podejście, jakie należy przyjąć w odniesieniu do przetwarzania danych osobowych, aby zminimalizować zagrożenie dla prywatności osób;

   3. Sposób, w jaki architektury te są zintegrowane z architekturą korporacyjną i wspierają ją; oraz

   4. Wszelkie założenia dotyczące zewnętrznych systemów i usług oraz ich zależności;

b. Przeglądanie i aktualizacja architektury bezpieczeństwa i ochrony prywatności [*Realizacja: częstotliwość zdefiniowana przez organizację*] *w* celu odzwierciedlenia zmian w architekturze korporacyjnej; oraz

c. Odzwierciedlanie planowanych zmian w architekturze planów bezpieczeństwa i ochrony prywatności, koncepcji bezpieczeństwa operacji (CONOPS), analizach krytyczności, procedurach organizacyjnych oraz zamówieniach / zakupach organizacyjnych.

Omówienie: Architektury bezpieczeństwa i prywatności na poziomie systemu są spójne z ogólnoorganizacyjnymi architekturami bezpieczeństwa i prywatności opisanymi w zabezpieczeniu PM-7, które są integralną częścią architektury korporacyjnej i są rozwijane jako jej część. Architektury te obejmują opis architektoniczny, przydział funkcji bezpieczeństwa i ochrony prywatności (w tym zabezpieczeń), informacje związane z bezpieczeństwem i prywatnością odnoszące się do zewnętrznych interfejsów, informacje wymieniane pomiędzy interfejsami oraz mechanizmy ochrony związane z każdym interfejsem. Architektura może również

obejmować inne informacje, takie jak role użytkowników i przywileje dostępu przypisane do każdej roli; wymogi dotyczące bezpieczeństwa i ochrony prywatności; rodzaje informacji przetwarzanych, przechowywanych i przekazywanych przez system; wymogi dotyczące zarządzania ryzykiem w łańcuchu dostaw; priorytety przywracania informacji i usług systemowych; oraz inne potrzeby w zakresie ochrony.

Publikacja [NIST SP 800-160-1] zawiera wytyczne dotyczące wykorzystania architektur bezpieczeństwa w ramach procesu rozwoju w cyklu życia systemu. Publikacja [OMB M-19-03] wymaga zastosowania koncepcji inżynierii bezpieczeństwa systemów opisanych w [NIST SP 800-160-1] dla aktywów o wysokiej wartości. Architektury bezpieczeństwa i ochrony prywatności są przeglądane i aktualizowane przez cały cykl życia systemu, począwszy od analizy rozwiązań alternatywnych, poprzez przegląd proponowanej architektury w planach zapytań ofertowych (*ang. Request For Proposal – RFP*), aż po przeglądy projektów przed i w trakcie realizacji (np. podczas wstępnych przeglądów projektów i krytycznych przeglądów projektów).

W dzisiejszych nowoczesnych architekturach obliczeniowych coraz rzadziej zdarza się, że organizacje kontrolują wszystkie zasoby informacyjne. Mogą istnieć kluczowe zależności od zewnętrznych usług i dostawców usług informatycznych. Opisanie takich zależności w architekturach bezpieczeństwa i ochrony prywatności jest niezbędne do opracowania kompleksowej misji i strategii ochrony biznesu. Ustanowienie, opracowanie, udokumentowanie i utrzymanie podstawowej kontroli konfiguracji bazowej systemów organizacyjnych ma kluczowe znaczenie dla wdrożenia i utrzymania efektywnych architektur. Opracowanie architektur jest koordynowane z SAISO i SAOP[62] w celu zapewnienia, że zabezpieczenia niezbędne do spełnienia wymogów bezpieczeństwa i ochrony prywatności są zidentyfikowane i skutecznie wdrożone. W wielu okolicznościach może nie istnieć rozróżnienie między architekturą bezpieczeństwa i ochrony prywatności systemu. W innych

[62] Patrz: NSC 800-37; NSC 7298.

okolicznościach cele w zakresie bezpieczeństwa mogą być odpowiednio spełnione, ale cele w zakresie prywatności mogą być jedynie częściowo spełnione przez wymogi bezpieczeństwa. W takich przypadkach uwzględnienie wymogów dotyczących prywatności niezbędnych do osiągnięcia satysfakcji doprowadzi do stworzenia odrębnej architektury prywatności. Dokumentacja może jednakże odzwierciedlać połączoną architekturę.

Zabezpieczenie PL-8 jest ukierunkowane przede wszystkim na organizację, aby zapewnić, że architektury są opracowywane dla danego systemu, a ponadto, że architektury te są zintegrowane z architekturą korporacyjną lub ściśle z nią powiązane. Natomiast zabezpieczenie SA-17 skierowane jest przede wszystkim do zewnętrznych deweloperów i integratorów produktów i systemów informatycznych. Zabezpieczenie SA-17, które jest uzupełnieniem zabezpieczenia PL-8, jest wybierane w przypadku, gdy organizacje zlecają rozwój systemów lub komponentów podmiotom zewnętrznym oraz gdy istnieje potrzeba wykazania spójności z architekturą korporacyjną organizacji oraz architekturą bezpieczeństwa i prywatności.

Zabezpieczenia powiązane: CM-2, CM-6, PL-2, PL-7, PL-9, PM-5, PM-7, RA-9, SA-3, SA-5, SA-8, SA-17, SC-7.

Zabezpieczenia rozszerzone:

(1) ARCHITEKTURA BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | ZABEZPIECZENIE WIELOSTOPNIOWE (OCHRONA WARSTWOWA)

Zaprojektowanie architektury bezpieczeństwa i ochrony prywatności dla systemu, stosując dogłębne podejście ochronne, które:

(a) Przydziela [Realizacja: *zabezpieczenie zdefiniowane przez organizację*] do [*Realizacja: zdefiniowane przez organizację lokalizacje i warstwy architektoniczne*]; oraz

(b) Zapewnia, że przydzielone zabezpieczenia działają w sposób skoordynowany i wzajemnie się uzupełniają.

Omówienie: Organizacje strategicznie przydzielają środki bezpieczeństwa i ochrony prywatności w architekturze bezpieczeństwa i ochrony prywatności tak, aby przeciwnicy musieli pokonać wiele zabezpieczeń ażeby osiągnąć swój cel. Wymaganie od przeciwników pokonania wielu zabezpieczeń utrudnia atak na zasoby informacyjne poprzez zwiększenie czynnika pracy przeciwnika; zwiększa również prawdopodobieństwo ich wykrycia. Koordynacja przydzielonych zabezpieczeń ma zasadnicze znaczenie dla zapewnienia, że atak obejmujący jedno zabezpieczenie nie spowoduje negatywnych, niezamierzonych skutków poprzez zakłócenie innych zabezpieczeń. Niezamierzone konsekwencje mogą obejmować blokadę systemu i kaskadowe alarmy. Umieszczanie zabezpieczeń w systemach i organizacjach jest ważną czynnością, która wymaga przemyślanej analizy. Wartość aktywów organizacyjnych jest ważnym czynnikiem w zapewnieniu dodatkowego warstwowania. Głębokie podejście architektoniczne do ochrony obejmuje modułowość i warstwowość (patrz zabezpieczenie SA-8(3)), rozdzielenie funkcjonalności systemu i użytkownika (patrz zabezpieczenie SC-2) oraz izolację funkcji bezpieczeństwa (patrz zabezpieczenie SC-3).

Zabezpieczenia powiązane: SC-2, SC-3, SC-29, SC-36.

(2) ARCHITEKTURA BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | DYWERSYFIKACJA DOSTAWCY

Wymaganie, aby [Realizacja: określone przez organizację *zabezpieczenia*] przydzielone do [*Realizacja: określone przez organizację lokalizacje i warstwy architektoniczne*] były nabywane od różnych dostawców.

Omówienie: Produkty informatyczne mają różne mocne i słabe strony. Szerokie spektrum produktów stanowi uzupełnienie poszczególnych ofert. Na przykład, dostawcy oferujący ochronę przed złośliwym kodem zazwyczaj aktualizują swoje produkty w różnym czasie, często opracowując rozwiązania dla znanych wirusów,

trojanów lub robaków w oparciu o swoje priorytety i harmonogramy rozwoju. Wdrażając różne produkty w różnych miejscach, istnieje zwiększone prawdopodobieństwo, że przynajmniej jeden z nich wykryje złośliwy kod. Jeśli chodzi o ochronę prywatności, sprzedawcy mogą oferować produkty, które śledzą dane osobowe w systemach. Produkty mogą wykorzystywać różne metody śledzenia. Korzystanie z wielu produktów może dawać większą pewność, że dane osobowe są zinwentaryzowane.

Zabezpieczenia powiązane: SC-29, SR-3.

Referencje: [OMB A-130], [NIST SP 800-160-1], [NIST SP 800-160-2].

PL-9 ZARZĄDZANIE CENTRALNE

Zabezpieczenie podstawowe: Zarządzanie centralne zabezpieczeniami [Realizacja: *zabezpieczenia zdefiniowane przez organizację i powiązane procesy*].

Omówienie: Zarządzanie centralne odnosi się do zarządzania w całej organizacji oraz wdrażania wybranych zabezpieczeń i procesów. Obejmuje to planowanie, wdrażanie, ocenę, autoryzowanie i monitorowanie zdefiniowanych w organizacji centralnie zarządzanych zabezpieczeń i procesów. Ponieważ centralne zarządzanie zabezpieczeniami jest generalnie związane z koncepcją zabezpieczeń wspólnych (dziedziczonych), takie zarządzanie promuje i ułatwia standaryzację wdrażania i zarządzania zabezpieczeniami oraz rozsądne wykorzystanie zasobów organizacyjnych. Centralnie zarządzane zabezpieczeniami i procesami może również spełniać wymogi niezależności w zakresie oceny na poparcie wstępnych i bieżących upoważnień do działania oraz jako część ciągłego monitorowania organizacji.

Zautomatyzowane narzędzia (np. narzędzia do zarządzania informacjami dotyczącymi bezpieczeństwa i zdarzeniami lub narzędzia do monitorowania bezpieczeństwa przedsiębiorstwa i zarządzania nim) mogą poprawić dokładność, spójność i dostępność informacji związanych z centralnie zarządzanymi zabezpieczeniami i procesami. Automatyzacja może również zapewnić możliwość agregacji i korelacji danych, mechanizmy ostrzegania oraz pulpity menedżerskie wspierające podejmowanie decyzji opartych na analizie ryzyka w obrębie organizacji.

W ramach procesów selekcji zabezpieczeń, organizacje określają w oparciu o zasoby i możliwości zabezpieczenia, które mogą być odpowiednie do centralnego zarządzania. Nie zawsze możliwe jest centralne zarządzanie każdym aspektem zabezpieczenia. W takich przypadkach zabezpieczenie może być traktowana, jako zabezpieczenie hybrydowe, zarządzane i wdrażane centralnie lub na poziomie systemu. Zabezpieczenia podstawowe i zabezpieczenia rozszerzone, które kwalifikują się do pełnego lub częściowego zarządzania centralnego, obejmują między innymi zabezpieczenia: AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-4 (wszystkie), AC-17(1),

AC 17(2), AC-17(3), AC- 17(9), AC-18(1), AC-18(3), AC-18(4), AC-18(5), AC-19(4), AC-22, AC-23, AT-2(1), AT-2(2), AT-3(1), AT-3(2), AT-3(3), AT-4, AU-3, AU-6(1), AU 6(3), AU-6(5), AU-6(6), AU-6(9), AU-7(1), AU-7(2), AU- 11, AU-13, AU-16, CA-2(1), CA-2(2), CA-2(3), CA-3(1), CA-3(2), CA-3(3), CA-7(1), CA-9, CM-2(2), CM-3(1), CM-3(4), CM-4, CM-6, CM-6(1), CM-7(2), CM-7(4), CM-7(5), CM-8 (wszystkie), CM-9(1), CM-10, CM-11, CP-7 (wszystkie), CP-8 (wszystkie), SC-43, SI-2, SI-3, SI-4 (wszystkie), SI-7, SI-8.

Zabezpieczenia powiązane: PL-8, PM-9.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [NSC 800-37].

PL-10 WYBÓR ZABEZPIECZEŃ BAZOWYCH

Zabezpieczenie podstawowe: Wyselekcjonowanie zabezpieczeń bazowych systemu.

Omówienie: Zabezpieczenia bazowe to wstępnie zdefiniowane zestawy zabezpieczeń, które zostały specjalnie zebrane w celu zaspokojenia potrzeb ochrony grupy, organizacji lub wspólnoty interesów. Zabezpieczenie jest wybierana jako bazowe, aby albo spełnić wymagania narzucone przez prawa, rozporządzenia, dyrektywy, regulacje, polityki, standardy i wytyczne, albo przeciwdziałać zagrożeniom wspólnym dla wszystkich użytkowników zabezpieczeń bazowych zgodnie z założeniami specyficznymi dla poziomów bazowych. Poziomy bazowe stanowią punkt wyjścia dla ochrony prywatności osób, informacji i systemów informatycznych, a następnie są dostosowywane w celu zarządzania ryzykiem zgodnie z misją, biznesem lub innymi ograniczeniami (patrz zabezpieczenie PL-11). Katalog zabezpieczeń bazowych jest podany w standardzie [NSC 800-53B]. Wybór zabezpieczeń bazowych jest uzależniony od potrzeb interesariuszy. Potrzeby interesariuszy uwzględniają wymogi misyjne i biznesowe, jak również mandaty nałożone przez obowiązujące prawo, zarządzenia, dyrektywy, zasady, regulacje, standardy i wytyczne. Na przykład, zabezpieczenia bazowe określone w [NSC 800-53B] oparte są na publikacji [NIST SP 800-53B][63]. Wymagania te, wraz z normami i wytycznymi NSC implementującymi te przepisy, zalecają organizacjom wybór jednego z zabezpieczeń bazowych po dokonaniu przeglądu rodzajów informacji oraz informacji przetwarzanych, przechowywanych i przesyłanych w systemie; przeanalizowaniu potencjalnego negatywnego wpływu utraty lub narażenia na szwank bezpieczeństwa informacji lub systemu, aktywów organizacji, osób, innych organizacji lub Państwa; oraz rozważeniu wyników oceny ryzyka systemowego i organizacyjnego. Publikacja [CNSSI 1253] zawiera wytyczne dotyczące zabezpieczeń bazowych dla krajowego systemu cyberbezpieczeństwa.

Zabezpieczenia powiązane: PL-2, PL-11, RA-2, RA-3, SA-8.

Zabezpieczenia rozszerzone: Brak.

Referencje: [FIPS 199], [FIPS 200], [NIST SP 800-30], [NIST SP 800-37], [NIST SP 800-39], [NIST SP 800-53B], [NIST SP 800- 60-1], [NIST SP 800-60-2], [NIST SP 800-160-1], [CNSSI 1253].

[63] [NIST SP- 800-53B] bazuje na wymaganiach [FISMA] i [PRIVACT].

PL-11 DOSTOSOWYWANIE ZABEZPIECZEŃ BAZOWYCH

Zabezpieczenie podstawowe: Dostosowywanie wybranych zabezpieczeń bazowych poprzez zastosowanie określonych czynności dopasowywania.

Omówienie: Koncepcja dostosowywania pozwala organizacjom na wyspecyfikowanie lub spersonalizowanie zestawu zabezpieczeń bazowych poprzez zastosowanie zdefiniowanego zestawu czynności dopasowywania. Czynności dopasowywania ułatwiają wyspecyfikowanie lub spersonalizowanie zabezpieczeń bazowych, pozwalając organizacjom na opracowanie planów bezpieczeństwa i ochrony prywatności, które odzwierciedlają ich specyficzną misję i funkcje biznesowe, środowiska, w których działają ich systemy, zagrożenia i podatności, które mogą mieć wpływ na ich systemy oraz wszelkie inne warunki i sytuacje, które mogą mieć wpływ na ich misję lub sukces biznesowy. Wskazówki dotyczące dostosowywania są zawarte w dokumencie [NSC 800-53B]. Dostosowywanie zabezpieczeń bazowych jest realizowane poprzez identyfikację i wyznaczenie wspólnych zabezpieczeń, zastosowanie rozważań dotyczących zakresu, wybór zabezpieczeń kompensacyjnych, przypisanie wartości do parametrów zabezpieczeń, uzupełnienie zabezpieczenia bazowego o dodatkowe zabezpieczenia w razie potrzeby oraz dostarczenie informacji do wdrożenia zabezpieczeń. Ogólne działania dostosowawcze zawarte w standardzie [NSC 800-53B] mogą być uzupełnione o dodatkowe działania w oparciu o potrzeby organizacji. Działania dostosowawcze mogą być stosowane do zabezpieczeń bazowych zawartych w [NIST SP 800-53B] zgodnie z wymogami bezpieczeństwa i ochrony prywatności publikacji [FISMA], [PRIVACT] i [OMB A-130]. Alternatywnie, inne społeczności przyjmujące różne zabezpieczenia bazowe mogą zastosować działania dostosowawcze zawarte w [NSC 800-53B], aby wyspecjalizować lub dostosować zabezpieczenia, które reprezentują specyficzne potrzeby i problemy tych podmiotów.

Zabezpieczenia powiązane: PL-10, RA-2, RA-3, RA-9, SA-8.

Zabezpieczenia rozszerzone: Brak.

Referencje: [FIPS 199], [FIPS 200], [NIST SP 800-30], [NIST SP 800-37], [NIST SP 800-39], [NIST SP 800-53B], [NIST SP 800- 60-1], [NIST SP 800-60-2], [NIST SP 800-160-1], [CNSSI 1253].

KATEGORIA PM – PROGRAMY ZARZĄDZANIA

PROGRAM ZARZĄDZANIA ZABEZPIECZENIAMI

FISMA], [PRIVACT] i [OMB A-130] wymagają od organizacji opracowania, wdrożenia i zapewnienia nadzoru nad programami bezpieczeństwa informacji i ochrony prywatności w całej organizacji, aby pomóc w zapewnieniu poufności, integralności i dostępności informacji przetwarzanych, przechowywanych i przesyłanych przez systemy informatyczne oraz w celu ochrony prywatności osób. Program zarządzania zabezpieczeniami (*ang. program management - PM*) opisany w tej sekcji jest wdrażany na poziomie organizacji i nie jest ukierunkowany na poszczególne systemy informatyczne. PM został zaprojektowany w celu ułatwienia osiągnięcia zgodności organizacji z obowiązującymi przepisami, rozporządzeniami, dyrektywami, politykami, regulacjami i standardami. Zabezpieczenia te są niezależne od minimalnych wymagań bezpieczeństwa informacji i systemów informatycznych w zależności od zakresu poziomów ryzyka [patrz NSC 200] i dlatego nie są powiązane z zabezpieczeniami bazowymi opisanymi w [NSC 800-53B].

Organizacje opracowują program zarządzania zabezpieczeniami w planach programów bezpieczeństwa informacji i ochrony prywatności. Ogólnoorganizacyjny plan programu bezpieczeństwa informacji (patrz zabezpieczenie PM-1) i plan programu ochrony prywatności (patrz zabezpieczenie PM-18) uzupełniają plany bezpieczeństwa systemu i ochrony prywatności (patrz zabezpieczenie PL-2) opracowane dla organizacyjnych systemów informatycznych. Wspólnie, plany bezpieczeństwa systemu i ochrony prywatności dla poszczególnych systemów informatycznych oraz plany programów bezpieczeństwa informacji i ochrony prywatności obejmują całość środków bezpieczeństwa i ochrony prywatności stosowanych w organizacji.

PM-1 PLAN PROGRAMU BEZPIECZEŃSTWA INFORMACJI

Zabezpieczenie podstawowe:

a. Opracowywanie i rozpowszechnienie w całej organizacji planu programu bezpieczeństwa informacji, który:

   1. Zawiera przegląd wymogów dotyczących programu bezpieczeństwa oraz opis programu zarządzania zabezpieczeniami i zabezpieczeń wspólnych obowiązujących lub planowanych w celu spełnienia tych wymogów;

   2. Obejmuje identyfikację i przydział ról, obowiązków, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi oraz zgodność z przepisami;

   3. Odzwierciedla koordynację pomiędzy jednostkami organizacyjnymi odpowiedzialnymi za bezpieczeństwo informacji; oraz

   4. Jest zatwierdzony przez osobę odpowiedzialną za zarządzanie ryzykiem[64] związanym z działalnością organizacji (w tym za misję, funkcje, wizerunek i reputację), zasobami organizacyjnymi, osobami, innymi organizacjami i Państwem;

b. Przeglądanie i aktualizacja planu programu bezpieczeństwa informacji w całej organizacji z [*Realizacja: częstotliwość określona przez organizację*] i następujących [*Realizacja: zdarzenia określone przez organizację*]; oraz

c. Zabezpieczenie planu bezpieczeństwa informacji przed nieautoryzowanym ujawnieniem i modyfikacją.

Omówienie: Plan programu bezpieczeństwa informacji jest formalnym dokumentem zawierającym przegląd wymagań bezpieczeństwa dotyczących programu bezpieczeństwa informacji w całej organizacji oraz opisującym program zarządzania

[64] Patrz: NSC 800-37.

zabezpieczeniami i zabezpieczeniami wspólnymi istniejącymi lub planowanymi do wdrożenia w celu spełnienia tych wymagań. Plan programu bezpieczeństwa informacji może być przedstawiony w formie pojedynczego dokumentu lub kompilacji dokumentów. Plany programów ochrony prywatności i plany zarządzania ryzykiem w łańcuchu dostaw są omówione oddzielnie odpowiednio w zabezpieczeniach PM-18 i SR-2.

Plan programu bezpieczeństwa informacji dokumentuje szczegóły dotyczące programu zarządzania zabezpieczeniami i zabezpieczeń wspólnych. Plan zawiera wystarczające informacje na temat zabezpieczeń (w tym specyfikację parametrów operacji przydzielania i wyboru w sposób wyraźny lub przez odniesienie), aby umożliwić realizację działań, które są jednoznacznie zgodne z intencją planu oraz określenie ryzyka, które ma zostać poniesione w przypadku realizacji planu zgodnie z założeniami. Aktualizacje planów programów bezpieczeństwa informacji obejmują zmiany organizacyjne i problemy zidentyfikowane podczas wdrażania planu lub oceny zabezpieczeń.

Program zarządzania zabezpieczeniami może być wdrożony na poziomie organizacji lub na poziomie misji lub procesu biznesowego i jest niezbędny do zarządzania programem bezpieczeństwa informacji w organizacji. Program zarządzania zabezpieczeniami jest odrębny od programu zabezpieczeń wspólnych, specyficznych dla danego systemu i hybrydowych, ponieważ program zarządzania zabezpieczeniami jest niezależny od konkretnego systemu. Razem, indywidualne plany bezpieczeństwa systemu i plan programu bezpieczeństwa informacji w całej organizacji zapewniają pełny zakres środków bezpieczeństwa stosowanych w organizacji.

Zabezpieczenia wspólne dostępne podczas dziedziczenia przez systemy organizacyjne są udokumentowane w załączniku do planu programu bezpieczeństwa informacji organizacji, chyba że zabezpieczenia są zawarte w oddzielnym planie bezpieczeństwa systemu. Plan programu ochrony informacji obejmujący całą organizację wskazuje, które oddzielne plany bezpieczeństwa zawierają opisy zabezpieczeń wspólnych.

Zdarzenia, które mogą spowodować konieczność aktualizacji planu programu bezpieczeństwa informacji, obejmują między innymi ocenę lub wyniki audytu w całej organizacji, incydenty lub naruszenia bezpieczeństwa, lub zmiany w przepisach prawa, rozporządzeniach, dyrektywach, przepisach, zasadach, standardach i wytycznych.

Zabezpieczenia powiązane: PL-2, PM-18, PM-30, RA-9, SI-12, SR-2.

Zabezpieczenia rozszerzone: Brak.

Referencje: [FISMA], [OMB A-130], [NIST SP 800-37], [NIST SP 800-39].

PM-2 ROLE KIEROWNICZE PROGRAMU BEZPIECZEŃSTWA INFORMACJI

Zabezpieczenie podstawowe: Wyznaczenie SAISO[65], którego zadaniem i uprawnieniami są koordynacja, opracowanie, wdrożenie i utrzymanie programu bezpieczeństwa informacji w całej organizacji.

Omówienie: SAISO jest pracownikiem organizacji. Organizacje mogą również określać SAISO, jako SISO lub CISO.[66]

Zabezpieczenia powiązane: Brak.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB M-17-25], [NIST SP 800-37], [NIST SP 800-39], [NIST SP 800-181].

[65] Patrz: NSC 800-37; NSC 7298.

[66] jw.

PM-3 ZASOBY W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI I OCHRONY PRYWATNOŚCI

Zabezpieczenie podstawowe:

a. Włączenie zasobów niezbędnych do wdrożenia programów bezpieczeństwa informacji i ochrony prywatności do planowania inwestycyjnego i wniosków inwestycyjnych oraz udokumentowanie wszystkich wyjątków od tego wymogu;

b. Przygotowanie dokumentacji niezbędnej do realizacji programów bezpieczeństwa informacji i ochrony prywatności w planowaniu inwestycyjnym i przy składaniu wniosków inwestycyjnych zgodnie z obowiązującym prawem, rozporządzeniami, dyrektywami, zasadami, przepisami, standardami; oraz

c. Udostępnianie do wykorzystania planowanych zasobów w zakresie bezpieczeństwa informacji i prywatności.

Omówienie: Organizacje, w zależności od potrzeb, rozważają ustanowienie ekspertów w dziedzinie bezpieczeństwa informacji i ochrony prywatność oraz w ramach zapewnienia niezbędnych zasobów, udzielania specjalistycznej pomocy i wsparcia. Organizacje mogą wyznaczyć i upoważnić radę ds. przeglądu inwestycji lub podobną grupę do zarządzania i zapewnienia nadzoru nad aspektami bezpieczeństwa informacji i ochrony prywatności w procesie planowania inwestycyjnego i kontroli inwestycji.

Zabezpieczenia powiązane: PM-4, SA-2.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130].

PM-4 PLAN DZIAŁANIA I ETAPY WPROWADZANIA ZABEZPIECZEŃ

Zabezpieczenie podstawowe:

a. Wdrożenie procesu mającego na celu zapewnienie, że plany działania i etapy wprowadzania zabezpieczeń informacji, ochrony prywatności i programów zarządzania ryzykiem w łańcuchu dostaw oraz powiązanych systemów organizacyjnych:

   1. Są rozwijane i utrzymywane;

   2. Dokumentują działania naprawcze w zakresie bezpieczeństwa informacji, ochrony prywatności i zarządzania ryzykiem w łańcuchu dostaw w celu właściwego reagowania na ryzyko związane z działalnością organizacji i jej aktywami, osobami fizycznymi, innymi organizacjami i Państwem; oraz

   3. Są zgłaszane zgodnie z ustalonymi wymogami sprawozdawczymi.

b. Przeglądanie planów działania i etapów wprowadzania zabezpieczeń pod kątem spójności ze strategią zarządzania ryzykiem organizacyjnym oraz priorytetów działań w zakresie reagowania na ryzyko w całej organizacji.

Omówienie: Plan działania i etapy wprowadzania zabezpieczeń są kluczowym dokumentem organizacyjnym i podlegają wymogom sprawozdawczości ustanowionym przez organizację. Organizacje opracowują plany działania i etapy wprowadzania zabezpieczeń z perspektywy całej organizacji, nadając priorytet działaniom związanym z reagowaniem na ryzyko i zapewniając spójność z celami i zadaniami organizacji. Aktualizacje planów działania i etapów wprowadzania zabezpieczeń są oparte na ustaleniach z oceny zabezpieczeń i realizacji ciągłego monitorowania. Może istnieć potrzeba opracowania wielu planów działania i wprowadzania zabezpieczeń odpowiadających poziomowi klasyfikacji systemu informatycznego, poziomowi misji/procesu biznesowego oraz poziomowi organizacyjnemu/zarządczemu. Chociaż plany działania i wprowadzania zabezpieczeń są wymagane dla organizacji publicznych, inne rodzaje organizacji mogą zmniejszyć

ryzyko poprzez dokumentowanie i śledzenie planowanych środków zaradczych. Szczegółowe wytyczne dotyczące planów działania i wprowadzania zabezpieczeń na poziomie systemu znajdują się w zabezpieczeniu CA-5.

Zabezpieczenia powiązane: CA-5, CA-7, PM-3, RA-7, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [PRIVACT], [OMB A-130], [NSC 800-37].

PM-5 INWENTARYZACJA SYSTEMU

Zabezpieczenie podstawowe: Opracowanie i aktualizacja [*Realizacja: częstotliwość określona przez organizację*] inwentaryzacji systemów organizacyjnych.

Omówienie: [OMB A-130][67] zawiera wytyczne dotyczące opracowywania wykazów systemów i związanych z nimi wymogów sprawozdawczych. Inwentaryzacja systemów odnosi się do ogólnozakładowego spisu systemów, a nie komponentów systemu opisanych w zabezpieczeniu CM-8.

Zabezpieczenia powiązane: Brak.

Zabezpieczenia rozszerzone:

(1) INWENTARYZACJA SYSTEMU | SPIS DANYCH OSOBOWYCH

Tworzenie, utrzymywanie i aktualizacja [***Realizacja: częstotliwość określona przez organizację***] **wykazu wszystkich systemów, aplikacji i inwestycji, które przetwarzają dane osobowe.**

Omówienie: Spis systemów, aplikacji i inwestycji, które przetwarzają dane osobowe, wspiera mapowanie działań związanych z danymi, dostarczanie osobom informacji o ochronie prywatności, utrzymywanie dokładnych danych osobowych i ograniczanie przetwarzania danych osobowych, gdy takie informacje nie są potrzebne do celów operacyjnych. Organizacje mogą korzystać z tego spisu w celu zapewnienia, że systemy przetwarzają dane osobowe wyłącznie w autoryzowanych celach i że przetwarzanie to jest nadal istotne i niezbędne do celów w nim określonych.

Zabezpieczenia powiązane: AC-3, CM-8, CM-12, CM-13, PL-8, PM-22, PT-3, PT-5, SI-12, SI-18.

Referencje: [IR 8062], [OMB A-130].

[67] Dotyczy rynku USA.

PM-6 MIARY SKUTECZNOŚCI

Zabezpieczenie podstawowe: Opracowywanie, monitorowanie i przedstawianie sprawozdań na temat wyników działań związanych z bezpieczeństwem informacji i ochroną prywatności.

Omówienie: Miarą wydajności są wskaźniki oparte na wynikach, wykorzystywane przez organizację do pomiaru skuteczności lub wydajności programów bezpieczeństwa informacji i ochrony prywatności oraz zabezpieczeń stosowanych w celu wsparcia programu. Aby ułatwić zarządzanie ryzykiem związanym z bezpieczeństwem i prywatnością, organizacje rozważają dostosowanie miar wydajności do poziomu tolerancji ryzyka organizacji, określonego w strategii zarządzania ryzykiem.

Zabezpieczenia powiązane: CA-7, PM-9.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [NIST SP 800-37], [NIST SP 800-39], [NIST SP 800-55], [NIST SP 800-137].

PM-7 STRUKTURA ORGANIZACYJNA

Zabezpieczenie podstawowe: Opracowanie i utrzymanie architektury organizacyjnej z uwzględnieniem bezpieczeństwa informacji, prywatności i wynikającego z tego ryzyka dla operacji organizacyjnych i aktywów, osób, innych organizacji i Państwa.

Omówienie: Integracja wymagań i środków bezpieczeństwa i ochrony prywatności w architekturze korporacyjnej pomaga zapewnić, że kwestie bezpieczeństwa i ochrony prywatności są uwzględniane w całym cyklu życia systemu i są jednoznacznie związane z misją organizacji i jej procesami biznesowymi. Proces integracji wymagań dotyczących bezpieczeństwa i ochrony prywatności jest również wpisany w architekturę korporacyjną oraz architekturę bezpieczeństwa i ochrony prywatności organizacji zgodną ze strategią zarządzania ryzykiem organizacyjnym. W zabezpieczeniu PM-7 architektury bezpieczeństwa i ochrony prywatności tworzone są na poziomie zbioru systemów (*ang. system-of-systems – SoS*), reprezentujących wszystkie systemy organizacyjne. W zabezpieczeniu PL-8 architektury bezpieczeństwa i ochrony prywatności tworzone są na poziomie reprezentującym pojedynczy system. Model architektury na poziomie systemu jest spójny z architekturą bezpieczeństwa i ochrony prywatności zdefiniowaną dla organizacji. Wymagania w zakresie bezpieczeństwa i ochrony prywatności oraz integracja zabezpieczeń są najskuteczniej realizowane poprzez rygorystyczne stosowanie Ram Zarządzania Ryzykiem [patrz NSC 800-37] oraz wspieranie standardów i wytycznych bezpieczeństwa.

Zabezpieczenia powiązane: AU-6, PL-2, PL-8, PM-11, RA-2, SA-3, SA-17.

Zabezpieczenia rozszerzone:

(1) ARCHITEKTURA PRZEDSIĘBIORSTWA | ODCIĄŻENIA

Odciążanie [***Realizacja: zdefiniowane przez organizację niekrytyczne funkcje lub usługi***] **poprzez przenoszenie ich do innych systemów, komponentów systemu lub zewnętrznego dostawcy.**

Omówienie: Nie każda funkcja lub usługa świadczona przez system jest niezbędna do realizacji misji organizacyjnej lub funkcji biznesowych. Drukowanie lub kopiowanie jest przykładem usługi niekrytycznej, ale wspierającej dla organizacji. Tam, gdzie jest to możliwe, takie wspierające, ale niekrytyczne funkcje lub usługi nie są kolokowane z funkcjami lub usługami, które wspierają zasadniczą misję lub funkcje biznesowe. Utrzymywanie takich funkcji w tym samym systemie lub komponencie systemu zwiększa powierzchnię ataku misji (podstawowych funkcji lub) organizacji. Przeniesienie wspomagających, ale niekrytycznych funkcji do systemu, komponentu systemu lub dostawcy zewnętrznego, które nie są krytyczne, może również zwiększyć wydajność poprzez oddanie tych funkcji lub usług pod kontrolę osób lub dostawców, którzy są ekspertami w zakresie tych funkcji lub usług.

Zabezpieczenia powiązane: SA-8.

Referencje: [OMB A-130], [NIST SP 800-37], [NIST SP 800-39], [NIST SP 800-160-1], [NIST SP 800-160-2].

PM-8 PLAN INFRASTRUKTURY KRYTYCZNEJ

Zabezpieczenie podstawowe: Uwzględnienie kwestii bezpieczeństwa informacji i ochrony prywatności przy opracowywaniu, dokumentowaniu i aktualizowaniu planu ochrony infrastruktury krytycznej i kluczowych zasobów.

Omówienie: Strategie ochrony opierają się na priorytetowym traktowaniu krytycznych aktywów i zasobów. Wymagania i wytyczne dotyczące definiowania infrastruktury krytycznej i kluczowych zasobów oraz przygotowywania związanych z nią planów ochrony infrastruktury krytycznej znajdują się w obowiązujących przepisach prawa, rozporządzeniach, dyrektywach, polityce, regulacjach, standardach i wytycznych.[68]

Zabezpieczenia powiązane: CP-2, CP-4, PE-18, PL-2, PM-9, PM-11, PM-18, RA-3, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [HSPD 7], [DHS NIPP], [EO 13636].

[68] Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym (Dz.U. 2007 Nr 89 poz. 590) i Narodowy Program Ochrony Infrastruktury Krytycznej.

PM-9 STRATEGIA ZARZĄDZANIA RYZYKIEM

Zabezpieczenie podstawowe:

a. Opracowanie kompleksowej strategii zarządzania:

   1. Ryzykiem bezpieczeństwa operacji organizacyjnych i majątku, osób, innych organizacji i Państwa związanych z funkcjonowaniem i korzystaniem z systemów organizacyjnych; oraz

   2. Zagrożeniami prywatności osób wynikającymi z autoryzowanego przetwarzania danych osobowych;

b. Wdrażanie strategii zarządzania ryzykiem w sposób spójny w całej organizacji; oraz

c. Przeglądanie i aktualizacja strategii zarządzania ryzykiem [*Realizacja: częstotliwość określona przez organizację*] lub w razie potrzeby w celu uwzględnienia zmian organizacyjnych.

Omówienie: Strategia zarządzania ryzykiem w skali całej organizacji obejmuje określenie tolerancji ryzyka związanego z bezpieczeństwem i prywatnością w organizacji, strategie ograniczania ryzyka związanego z bezpieczeństwem i prywatnością, metodologię oceny akceptowalnego ryzyka, proces oceny ryzyka związanego z bezpieczeństwem i prywatnością w całej organizacji w odniesieniu do tolerancji ryzyka w organizacji oraz koncepcje monitorowania ryzyka w czasie. SAORM[69] (kierownik jednostki organizacyjnej lub wyznaczona osoba) dostosowuje procesy zarządzania bezpieczeństwem informacji do procesów planowania strategicznego, operacyjnego i budżetowego. Funkcja RE[70], sprawowana przez SAORM, może ułatwić spójne stosowanie strategii zarządzania ryzykiem w całej organizacji. Strategia zarządzania ryzykiem może opierać się na informacjach

[69] Patrz: NSC 800-37; NSC 7298.

[70] jw.

dotyczących bezpieczeństwa i ochrony prywatności pochodzących z innych źródeł, zarówno wewnętrznych, jak i zewnętrznych w stosunku do organizacji, w celu zapewnienia, że strategia ta ma szeroki zakres i jest kompleksowa. Strategia zarządzania ryzykiem w łańcuchu dostaw opisana w zabezpieczeniu PM-30 może również stanowić użyteczny wkład w strategię zarządzania ryzykiem w skali całej organizacji.

Zabezpieczenia powiązane: AC-1, AU-1, AT-1, CA-1, CA-2, CA-5, CA-6, CA-7, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-2, PM-2, PM-8, PM-18, PM-28, PM-30, PS-1, PT-2, PT-3, RA-1, RA-3, RA-9, SA-1, SA-4, SC-1, SC-38, SI-1, SI-12, SR-1, SR-2.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [NIST SP 800-30], [NIST SP 800-37], [NIST SP 800-39], [NIST SP 800-161], [IR 8023].

PM-10 PROCES AUTORYZACJI

Zabezpieczenie podstawowe:

a. Zarządzanie stanem bezpieczeństwa i ochrony prywatności systemów organizacyjnych oraz środowisk, w których systemy te działają, poprzez procesy autoryzacji;

b. Wyznaczanie osób do pełnienia określonych ról i obowiązków w ramach procesu zarządzania ryzykiem organizacyjnym; oraz

c. Integrowanie procesów autoryzacji z programem zarządzania ryzykiem w całej organizacji.

Omówienie: Szczególna rola w procesach zarządzania ryzykiem obejmuje osobę odpowiedzialną za zarządzanie ryzykiem (RM funkcja)[71] oraz wyznaczone osoby autoryzujące (AO)[72] dla każdego systemu organizacyjnego i dostawcy zabezpieczeń wspólnych. Procesy autoryzacji organizacji są zintegrowane z procesami ciągłego monitorowania w celu ułatwienia bieżącego zrozumienia i akceptacji ryzyka związanego z bezpieczeństwem i prywatnością dla operacji organizacyjnych, aktywów organizacyjnych, osób, innych organizacji i Państwa.

Zabezpieczenia powiązane: CA-6, CA-7, PL-2.

Zabezpieczenia rozszerzone: Brak.

Referencje: [NIST SP 800-37], [NIST SP 800-39], [NIST SP 800-181].

[71] Patrz: NSC 800-37; NSC 7298.

[72] jw.

PM-11 DEFINICJA MISJI I PROCESU BIZNESOWEGO

Zabezpieczenie podstawowe:

a. Zdefiniowanie misji organizacji i procesów biznesowych z uwzględnieniem bezpieczeństwa informacji i ochrony prywatności oraz wynikającego z tego ryzyka dla operacji organizacyjnych, zasobów organizacyjnych, osób, innych organizacji i Państwa; oraz

b. Określanie potrzeb w zakresie ochrony informacji i przetwarzania danych osobowych wynikających z określonej misji i procesów biznesowych; oraz

c. Przeglądanie i rewizja misji i procesów biznesowych [*Realizacja: częstotliwość określona przez organizację*].

Omówienie: Potrzeby w zakresie ochrony to niezależne od technologii możliwości, które są wymagane do przeciwdziałania zagrożeniom organizacji, osób, systemów i Narodu na skutek narażenia na ryzyko informacji (tj. utraty poufności, integralności, dostępności lub prywatności) przez nich przetwarzanych. Ochrona informacji i potrzeby przetwarzania danych osobowych wynikają z misji i potrzeb biznesowych określonych przez interesariuszy organizacji, misji i procesów biznesowych zaprojektowanych w celu zaspokojenia tych potrzeb oraz strategii zarządzania ryzykiem organizacyjnym. Potrzeby w zakresie ochrony informacji i przetwarzania danych osobowych określają wymagane środki bezpieczeństwa organizacji i systemów. Nieodłącznym elementem definiowania potrzeb w zakresie ochrony informacji i przetwarzania danych osobowych jest zrozumienie negatywnych skutków, jakie mogą wyniknąć w przypadku narażenia na kompromitację lub naruszenia informacji. Proces kategoryzacji jest wykorzystywany do określenia takiego potencjalnego wpływu zagrożenia. Zagrożenia dla prywatności osób fizycznych mogą wynikać z narażenia na szwank danych osobowych, ale mogą również powstać, jako niezamierzone konsekwencje lub produkt uboczny przetwarzania danych osobowych w dowolnym etapie cyklu życia informacji. Ocena ryzyka związana z ochroną prywatności jest wykorzystywana do ustalania

priorytetów w zakresie ryzyka, jakie stwarza dla osób fizycznych systemowe przetwarzanie danych osobowych. Te oceny ryzyka pozwalają na wybór wymaganych zabezpieczeń prywatności dla organizacji i systemów. Definicje misji i procesów biznesowych oraz związane z nimi wymogi ochrony są dokumentowane zgodnie z zasadami i procedurami organizacji.

Zabezpieczenia powiązane: CP-2, PL-2, PM-7, PM-8, RA-2, RA-3, RA-9, SA-2.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [FIPS 199], [NIST SP 800-39], [NIST SP 800-60-1], [NIST SP 800-60-2], [NIST SP 800-160-1].

PM-12 ZAGROŻENIA WEWNĘTRZNE

Zabezpieczenie podstawowe: Wdrożenie programu przeciwdziałania zagrożeniom wewnętrznym, który obejmuje interdyscyplinarny zespół zajmujący się incydentami związanymi z zagrożeniami wewnętrznymi.

Omówienie: Standardy i wytyczne, które odnoszą się do programów przeciwdziałania zagrożeniom odnoszącym się do informacji niejawnych, mogą być skutecznie stosowane w celu poprawy bezpieczeństwa kontrolowanych informacji jawnych w systemach organizacji. Programy przeciwdziałania zagrożeniom wewnętrznym obejmują zabezpieczenia mające na celu wykrywanie i przeciwdziałanie złośliwym działaniom osób poprzez scentralizowaną integrację i analizę informacji technicznych i nietechnicznych w celu identyfikacji potencjalnych zagrożeń wewnętrznych Kierownik jednostki organizacyjnej wyznacza osobę odpowiedzialną za wdrożenie programu i zapewnienie nadzoru nad nim. Poza scentralizowaną integracją i analizą, programy przeciwdziałania zagrożeniom wewnętrznym wymagają od organizacji przygotowania polityki przeciwdziałania zagrożeniom wewnętrznym i planów wdrożeniowych, prowadzenia monitorowania działań poszczególnych pracowników na stanowiskach pracy, przeprowadzania szkoleń pracowników w zakresie rozpoznawania zagrożeń wewnętrznych, uzyskiwania dostępu do informacji umożliwiających analizę zagrożeń wewnętrznych oraz przeprowadzania samooceny stanu zagrożenia wewnętrznego w organizacji.

Programy dotyczące zagrożeń wewnętrznych mogą bazować na działających już w organizacjach zespołach zajmujących się obsługą incydentów, takich jak zespoły reagowania na incydenty związane z bezpieczeństwem komputerowym. Rejestry zasobów ludzkich są szczególnie ważne w tych działaniach, ponieważ istnieją przekonujące dowody na to, że niektóre rodzaje przestępstw wewnętrznych są często poprzedzone pozatechnicznymi zachowaniami w miejscu pracy, w tym ciągłymi wzorcami niezadowolonych zachowań i konfliktów ze współpracownikami i innymi kolegami. Te prekursory mogą ukierunkować organy organizacyjne na

bardziej skoncentrowane i ukierunkowane działania monitorujące. Wykorzystanie rejestrów zasobów ludzkich może jednak budzić poważne obawy dotyczące prywatności. Udział zespołu prawnego, w tym konsultacje z SAOP[73], pozwala uniknąć sytuacji, w której działania monitorujące nie są prowadzone zgodnie z obowiązującym prawem, zarządzeniami, dyrektywami, rozporządzeniami, politykami, standardami i wytycznymi.

Zabezpieczenia powiązane: AC-6, AT-2, AU-6, AU-7, AU-10, AU-12, AU-13, CA-7, IA-4, IR-4, MP-7, PE-2, PM- 16, PS-3, PS-4, PS-5, PS-7, PS-8, SC-7, SC-38, SI-4, PM-14.

Zabezpieczenia rozszerzone: Brak.

Referencje: [EO 13587], [NITP12], [ODNI NITP].

[73] Patrz: NSC 800-37; NSC 7298.

PM-13 PERSONEL BEZPIECZEŃSTWA I OCHRONY I PRYWATNOŚCI

Zabezpieczenie podstawowe: Stworzenie programu rozwoju i doskonalenia pracowników zajmujących się bezpieczeństwem i prywatnością.

Omówienie: Programy rozwoju i doskonalenia pracowników zajmujących się bezpieczeństwem i prywatnością obejmują określenie wiedzy, umiejętności i zdolności potrzebnych do wykonywania obowiązków i zadań związanych z bezpieczeństwem i prywatnością; opracowanie programów szkoleniowych opartych na podziale ról dla osób, którym przydzielono role i obowiązki w zakresie bezpieczeństwa i ochrony prywatności; oraz zapewnienie standardów i wytycznych w zakresie oceny i rozwijania indywidualnych kwalifikacji osób zajmujących i ubiegających się o stanowiska związane z bezpieczeństwem i ochroną prywatności. Takie programy rozwoju i doskonalenia pracowników mogą również obejmować ścieżki kariery w zakresie bezpieczeństwa i ochrony prywatności, aby zachęcić specjalistów ds. bezpieczeństwa i ochrony prywatności do awansu w tej dziedzinie i obsadzenia stanowisk o większej rozliczalności. Programy te zachęcają organizacje do zatrudniania wykwalifikowanego personelu na stanowiskach związanych z bezpieczeństwem i ochroną prywatności. Programy rozwoju i doskonalenia pracowników zajmujących się bezpieczeństwem i prywatnością są uzupełnieniem organizacyjnych programów świadomości i szkolenia w zakresie bezpieczeństwa i koncentrują się na rozwijaniu i instytucjonalizacji podstawowych zdolności personelu w zakresie bezpieczeństwa i prywatności, potrzebnych do ochrony operacji organizacyjnych, aktywów i osób.

Zabezpieczenia powiązane: AT-2, AT-3.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [NIST SP 800-181].

PM-14 TESTOWANIE, SZKOLENIA I MONITOROWANIE

Zabezpieczenie podstawowe:

a. Wdrożenie procesu zapewniającego, że plany organizacyjne dotyczące przeprowadzania testów bezpieczeństwa i ochrony prywatności, szkoleń oraz działań monitorujących związanych z systemami organizacyjnymi:

   1. Są rozwijane i utrzymywane; oraz

   2. Zapewniają ciągłość ich realizacji; oraz

b. Przeglądanie planów testowania, szkolenia i monitorowania pod kątem spójności ze strategią zarządzania ryzykiem organizacyjnym oraz ogólnoorganizacyjnymi priorytetami działań w odpowiedzi na ryzyko.

Omówienie: Proces testowania, szkolenia i monitorowania bezpieczeństwa i ochrony prywatności w całej organizacji pomaga zapewnić nadzór nad działaniami związanymi z testowaniem, szkoleniem i monitorowaniem oraz koordynację tych działań.

Wraz z rosnącym znaczeniem programów ciągłego monitorowania, wdrażaniem bezpieczeństwa informacji i ochrony prywatności na trzech poziomach hierarchii zarządzania ryzykiem oraz powszechnym stosowaniem wspólnych zabezpieczeń, organizacje koordynują i konsolidują działania związane z testowaniem i monitorowaniem, które są rutynowo prowadzone w ramach bieżących ocen wspierających różne rodzaje zabezpieczeń.

Działania szkoleniowe w zakresie bezpieczeństwa i ochrony prywatności, koncentrujące się na poszczególnych systemach i konkretnych rolach, wymagają koordynacji wszystkich elementów organizacyjnych. Plany i działania związane z testowaniem, szkoleniem i monitorowaniem są oparte na bieżących ocenach zagrożeń i podatności.

Zabezpieczenia powiązane: AT-2, AT-3, CA-7, CP-4, IR-3, PM-12, SI-4.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [NIST SP 800-37], [NIST SP 800-39], [NIST SP 800-53A], [NIST SP 800-115], [NIST SP 800-137].

PM-15 GRUPY I STOWARZYSZENIA ZAJMUJĄCE SIĘ BEZPIECZEŃSTWEM I OCHRONĄ PRYWATNOŚCI

Zabezpieczenie podstawowe: Nawiązywanie i instytucjonalizacja kontaktów z wybranymi grupami i stowarzyszeniami w ramach wspólnot bezpieczeństwa i ochrony prywatności w celu:

a. Ułatwianie bieżącej edukacji i szkoleń personelu organizacji w zakresie bezpieczeństwa i ochrony prywatności;

b. Utrzymywanie aktualizacji zalecanych praktyk, technik i technologii w zakresie bezpieczeństwa i ochrony prywatności; oraz

c. Udostępnianie aktualnych informacji dotyczących bezpieczeństwa i ochrony prywatności, w tym zagrożeń, podatności i incydentów.

Omówienie: Stały kontakt z grupami i stowarzyszeniami zajmującymi się bezpieczeństwem i ochroną prywatności jest ważny w środowisku szybko zmieniających się technologii i zagrożeń. Grupy i stowarzyszenia obejmują specjalne grupy interesów, stowarzyszenia zawodowe, fora, grupy dyskusyjne, grupy użytkowników i grupy koleżeńskie specjalistów ds. bezpieczeństwa i ochrony prywatności w analogicznych organizacjach. Organizacje wybierają grupy i stowarzyszenia zajmujące się bezpieczeństwem i ochroną prywatności w oparciu o misję i funkcje biznesowe. Organizacje dzielą się informacjami na temat zagrożeń, podatności na zagrożenia i incydentów, jak również informacjami dotyczącymi kontekstu, technik zapewnienia zgodności i problemów związanych z ochroną prywatności zgodnie z obowiązującymi przepisami, rozporządzeniami, dyrektywami, zasadami, standardami i wytycznymi.

Zabezpieczenia powiązane: SA-11, SI-5.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130].

PM-16 OSTRZEGANIE O ZAGROŻENIACH

Zabezpieczenie podstawowe: Wdrożenie programu uświadamiania zagrożeń, który obejmuje międzyorganizacyjną wymianę informacji - zdolność do wymiany informacji na temat zagrożeń.

Omówienie: Ze względu na stale zmieniającą się i rosnącą złożoność przeciwników, zwłaszcza zaawansowanego stałego zagrożenia typu APT, staje się bardziej prawdopodobne, że przeciwnicy mogą z powodzeniem naruszyć lub skompromitować systemy organizacyjne. Jedną z najlepszych technik rozwiązania tego problemu jest dzielenie się przez organizacje informacjami o zagrożeniach, w tym o zdarzeniach (tj. taktyce, technikach i procedurach), których organizacje doświadczyły, środkach zaradczych, które organizacje uznały za skuteczne w walce z określonymi rodzajami zagrożeń, oraz rozpoznanych zagrożeniach (tj. wskazówkach i ostrzeżeniach o zagrożeniach). Wymiana informacji o zagrożeniach może mieć charakter dwustronny lub wielostronny. Dwustronna wymiana informacji o zagrożeniach obejmuje kooperacje państwowo - komercyjne i państwowo - państwowe. Wielostronna wymiana informacji o zagrożeniach obejmuje organizacje biorące udział w konsorcjach wymiany informacji o zagrożeniach. Informacje o zagrożeniach mogą wymagać specjalnych porozumień i ochrony lub mogą być swobodnie udostępniane.

Zabezpieczenia powiązane: IR-4, PM-12.

Zabezpieczenia rozszerzone:

(1) OSTRZEGANIE O ZAGROŻENIACH | ZAUTOMATYZOWANE ŚRODKI WYMIANY INFORMACJI O ZAGROŻENIACH

Stosowanie zautomatyzowanych mechanizmów maksymalizujących skuteczność wymiany rozpoznanych informacji o zagrożeniach.

Omówienie: W celu zmaksymalizowania skuteczności monitoringu ważne jest, by określić, jakich obserwowalnych zagrożeń i wskaźników powinny szukać

zastosowane sensory. Dzięki wykorzystaniu dobrze ugruntowanych standardów, usług i zautomatyzowanych narzędzi, organizacje zwiększają swoją zdolność do szybkiego udostępniania i wprowadzania do narzędzi monitorujących odpowiednich sygnatur wykrywania zagrożeń.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

PM-17 OCHRONA NADZOROWANYCH INFORMACJI JAWNYCH PRZETWARZANYCH W SYSTEMACH ZEWNĘTRZNYCH

Zabezpieczenie podstawowe:

a. Ustanowienie polityki i procedur w celu zapewnienia, że wymogi dotyczące ochrony nadzorowanych informacji jawnych, które są przetwarzane, przechowywane lub przekazywane w systemach zewnętrznych, są realizowane zgodnie z obowiązującymi przepisami, rozporządzeniami, dyrektywami, politykami, wytycznymi i standardami; oraz

b. Przeglądanie i aktualizacja polityki i procedur [*Realizacja: częstotliwość określona przez organizację*].

Omówienie: Nadzorowane informacje jawne są określane przez organizację wraz z wymaganiami dotyczącymi ochrony i rozpowszechniania takich informacji. Powinny szczegółowo określać zastosowanie i warunki, które mają być realizowane zgodnie z procedurami organizacyjnymi, w tym poprzez procesy zawierania umów.

Zabezpieczenia powiązane: CA-6, PM-10.

Zabezpieczenia rozszerzone: Brak.

Referencje: [32 CFR 2002], [NIST SP 800-171], [NIST SP 800-172], [NARA CUI].

PM-18 PLAN PROGRAMU OCHRONY PRYWATNOŚCI

Zabezpieczenie podstawowe:

a. Opracowanie i rozpowszechnienie w całej organizacji planu programu ochrony prywatności, który zapewnia przegląd programu ochrony prywatności organizacji, oraz:

   1. Zawiera opis struktury programu ochrony prywatności oraz zasobów przeznaczonych na program ochrony prywatności;

   2. Przedstawia przegląd wymagań dotyczących programu ochrony prywatności oraz opis zabezpieczeń zarządzania programem ochrony prywatności i istniejących lub planowanych zabezpieczeń wspólnych spełniających te wymagania;

   3. Uwzględnia rolę SAOP[74] oraz określa i przydziela role i obowiązki innym urzędnikom i pracownikom odpowiedzialnym za ochronę prywatności;

   4. Opisuje zaangażowanie kierownictwa, zgodność z przepisami oraz strategiczne cele i zadania programu ochrony prywatności;

   5. Odzwierciedla koordynację pomiędzy jednostkami organizacyjnymi odpowiedzialnymi za różne aspekty prywatności; oraz

   6. Jest zatwierdzony przez wyższego rangą urzędnika/pracownika, który ponosi odpowiedzialność za ryzyko związane z ochroną prywatności w odniesieniu do działań organizacyjnych (w tym misji, funkcji, wizerunku i reputacji), aktywów organizacyjnych, osób, innych organizacji i Państwa; oraz

b. Aktualizowanie planu [Realizacja: częstotliwość określona przez organizację] oraz uwzględnianie zmian w przepisach i polityce ochrony prywatności oraz zmian organizacyjnych..

[74] Patrz: NSC 800-37; NSC 7298.

Omówienie: Plan programu ochrony prywatności jest formalnym dokumentem, który zawiera przegląd programu ochrony prywatności organizacji, w tym opis struktury programu ochrony prywatności, zasoby przeznaczone na program ochrony prywatności, rolę SAOP oraz innych urzędników i pracowników zajmujących się ochroną prywatności, strategiczne cele i zadania programu ochrony prywatności, a także zabezpieczenia zarządzania programem i zabezpieczenia wspólne, które zostały wprowadzone lub są planowane w celu spełnienia obowiązujących wymogów dotyczących ochrony prywatności i zarządzania zagrożeniami prywatności. Plany programu ochrony prywatności mogą być przedstawione w pojedynczych dokumentach lub kompilacjach dokumentów.

SAOP jest odpowiedzialny za określanie, które zabezpieczenia prywatności organizacja będzie traktować, jako programy bezpieczeństwa informacji, zabezpieczenia wspólne, specyficzne dla danego systemu i hybrydowe. Plany programów ochrony prywatności dostarczają wystarczających informacji na temat zarządzania programami ochrony prywatności i zabezpieczeń wspólnych (w tym specyfikacji parametrów oraz operacji przydzielania i selekcji w sposób wyraźny lub przez odniesienie), aby umożliwić wdrożenie zabezpieczeń, które są całkowicie zgodne z intencjami planów oraz szacowanie ryzyka ponoszonego w przypadku wdrożenia planów zgodnie z założeniami.

Program zarządzania zabezpieczeniami jest na ogół wdrażany na poziomie organizacji i jest niezbędny do zarządzania programem ochrony prywatności w organizacji. Program zarządzania zabezpieczeniami różni się od zwykłych, specyficznych dla danego systemu i hybrydowych zabezpieczeń, ponieważ program zarządzania zabezpieczeniami jest niezwiązany z żadnym konkretnym systemem informatycznym. Razem, plany ochrony prywatności dla poszczególnych systemów i plan programu ochrony prywatności dla całej organizacji zapewniają pełne pokrycie zabezpieczeń prywatności stosowanych w organizacji.

Zabezpieczenia wspólne są udokumentowane w załączniku do planu programu ochrony prywatności organizacji, chyba że są one zawarte w oddzielnym planie ochrony prywatności systemu. Plan programu ochrony prywatności dla całej organizacji wskazuje, które oddzielne plany ochrony prywatności zawierają opisy zabezpieczeń w zakresie ochrony prywatności.

Zabezpieczenia powiązane: PM-8, PM-9, PM-19.

Zabezpieczenia rozszerzone: Brak.

Referencje: [PRIVACT], [0MB A-130].

PM-19 ROLE KIEROWNICZE PROGRAMU OCHRONY PRYWATNOŚCI

Zabezpieczenie podstawowe: Wyznaczenie SAOP[75], który posiada uprawnienia, obowiązki, odpowiedzialność i zasoby do koordynowania, opracowywania i wdrażania obowiązujących wymogów w zakresie ochrony prywatności i zarządzania ryzykiem związanym z ochroną prywatności poprzez ogólnoorganizacyjny program ochrony prywatności.

Omówienie: Urzędnik ds. prywatności/ jest pracownikiem organizacyjnym. W przypadku instytucji państwowych jest on wyznaczony jako SAOP. Organizacje mogą również określać tego urzędnika mianem CPO[76] (inspektor ochrony danych). SAOP pełni również funkcje w komisji ds. zarządzania danymi (patrz PM-23) i komisji ds. integralności danych (patrz PM-24).

Zabezpieczenia powiązane: PM-18, PM-20, PM-23, PM-24, PM-27.

Zabezpieczenia rozszerzone: Brak.

Referencje: [0MB A-130].

[75] Patrz: NSC 800-37; NSC 7298.

[76] jw.

PM-20 ROZPOWSZECHNIANIE INFORMACJI O PROGRAMIE OCHRONY PRYWATNOŚCI

Zabezpieczenie podstawowe: Prowadzenie strony internetowej z centralnymi zasobami na głównej publicznej stronie internetowej organizacji, która służy jako główne źródło informacji o programie ochrony prywatności organizacji i która:

a. Zapewnia, że społeczeństwo ma dostęp do informacji na temat działań organizacji w zakresie ochrony prywatności i może komunikować się z SAOP;

b. Zapewnia, że praktyki i raporty dotyczące ochrony prywatności organizacji są publicznie dostępne; oraz

c. Stosuje publicznie dostępne adresy e-mail i/lub linie telefoniczne, aby umożliwić społeczeństwu przekazanie informacji zwrotnych i/lub skierowanie pytań do biur ochrony prywatności dotyczących praktyk w zakresie ochrony prywatności.

Omówienie: Organizacje zamieszczają publiczne oceny wpływu na prywatność, zawiadomienia o systemie rejestrów, zawiadomienia i umowy o zgodności, przepisy dotyczące wyłączenia i wdrożenia rozporządzenia ochronie danych osobowych, sprawozdania dotyczące prywatności, polityki prywatności, instrukcje dla osób składających wnioski o dostęp lub poprawki, adresy poczty elektronicznej do zgłaszania pytań/skarg, blogi i okresowe publikacje.

Zabezpieczenia powiązane: AC-3, PM-19, PT-5, PT-6, PT-7, RA-8.

Zabezpieczenia rozszerzone:

(1) ROZPOWSZECHNIANIE INFORMACJI O PROGRAMIE OCHRONY PRYWATNOŚCI | POLITYKI PRYWATNOŚCI PREZENTOWANE NA STRONACH INTERNETOWYCH, W APLIKACJACH I USŁUGACH CYFROWYCH

Opracowywanie i zamieszczanie polityki prywatności na wszystkich zewnętrznych stronach internetowych, aplikacjach mobilnych i innych usługach cyfrowych, która:

(a) Jest napisana prostym językiem i zorganizowane w sposób, który jest łatwy do zrozumienia i nawigacji;

(b) Dostarcza informacji potrzebnych społeczeństwu do podjęcia świadomej decyzji o tym, czy i jak współpracować z organizacją; oraz

(c) Jest aktualizowana za każdym razem, gdy organizacja dokonuje istotnych zmian w opisywanych przez siebie praktykach i zawiera znacznik czasu/ daty informujący opinię publiczną o dacie ostatnich zmian.

Omówienie: Organizacje publikują politykę prywatności na wszystkich zewnętrznych stronach internetowych, aplikacjach mobilnych i innych usługach cyfrowych. Organizacje umieszczają link do odpowiedniej polityki prywatności na wszystkich znanych, głównych punktach wejścia na stronę, aplikację lub usługę cyfrową. Ponadto, organizacje zamieszczają link do polityki prywatności na każdej stronie internetowej, która gromadzi dane osobowe. Organizacje podlegają obowiązującym przepisom, zarządzeniom wykonawczym, dyrektywom, rozporządzeniom lub zasadom, które wymagają podania określonych informacji do wiadomości publicznej. Personel organizacji konsultuje się SAOP i radcą prawnym w sprawie takich wymogów.

Zabezpieczenia powiązane: Brak.

Referencje: [PRIVACT], [OMB A-130], [0MB M-17-06].

PM-21 REJESTROWANIE UJAWNIEŃ

Zabezpieczenie podstawowe:

a. Opracowywanie i utrzymywanie dokładnej ewidencji ujawnień informacji umożliwiających identyfikację osób, zawierającej co najmniej:

   1. Datę, charakter i cel każdego ujawnienia; oraz

   2. Nazwę i adres lub inne informacje kontaktowe osoby lub organizacji, której ujawniono informacje;

b. Przechowywanie ujawnionych informacji przez okres retencji danych osobowych lub pięć lat po ich ujawnieniu, w zależności od tego, który z tych okresów jest dłuższy; oraz

c. Udostępnianie na wniosek osoby, do której odnoszą się dane osobowe, informacji o ujawnieniu danych.

Omówienie: Celem ewidencji ujawnień jest umożliwienie osobom fizycznym uzyskania informacji, komu ujawniono ich dane osobowe, uzyskanie podstawy do późniejszego poinformowania odbiorców o wszelkich poprawionych lub zakwestionowanych danych osobowych oraz zapewnienie ścieżki audytu dla późniejszych przeglądów zgodności organizacji z warunkami ujawnień. Prowadzenie rejestru ujawnień jest wymagane przez stosowne przepisy; organizacje powinny konsultować się w sprawie tego wymogu z SAOP i z radcą prawnym oraz być świadome wyjątków ustawowych i wytycznych dotyczących tego przepisu.

Organizacje mogą korzystać z dowolnego systemu przechowywania zapisu ujawnień, jeśli są w stanie wygenerować z takiego systemu dokument zawierający wykaz wszystkich ujawnień wraz z wymaganymi informacjami. Organizacje mogą korzystać ze zautomatyzowanych mechanizmów w celu ustalenia, kiedy informacje umożliwiające identyfikację osoby zostały ujawnione, w tym z komercyjnych usług zapewniających powiadomienia i alerty. Ewidencja ujawnień może być również wykorzystywana do pomocy organizacjom w sprawdzeniu zgodności

z obowiązującymi ustawami i politykami dotyczącymi prywatności regulującymi ujawnianie lub rozpowszechnianie informacji oraz ograniczenia dotyczące rozpowszechniania.

Zabezpieczenia powiązane: AC-3, AU-2, PKT-2.

Zabezpieczenia rozszerzone: Brak.

Referencje: [PRIVACT], [OMB A-130].

PM-22 ZARZĄDZANIE JAKOŚCIĄ DANYCH OSOBOWYCH

Zabezpieczenie podstawowe: Opracowanie i udokumentowanie w całej organizacji zasad i procedur:

a. Sprawdzania dokładności, istotności, aktualności i kompletności danych osobowych w całym cyklu życia informacji;

b. Poprawiania lub usuwania nieprawidłowych lub nieaktualnych danych osobowych;

c. Rozpowszechniania informacji o skorygowanych lub usuniętych danych osobowych wśród osób fizycznych lub innych odpowiednich podmiotów; oraz

d. Odwoływania się od niekorzystnych decyzji w sprawie wniosków o poprawienie lub usunięcie danych.

Omówienie: Zarządzanie jakością informacji umożliwiających identyfikację osób obejmuje kroki, które organizacje podejmują w celu potwierdzenia dokładności i przydatności informacji umożliwiających identyfikację osób w całym cyklu życia informacji. Cykl życia informacji obejmuje tworzenie, zbieranie, wykorzystywanie, przetwarzanie, przechowywanie, obsługę, rozpowszechnianie, ujawnianie i dysponowanie informacjami umożliwiającymi identyfikację osób. Polityka organizacyjna i procedury zarządzania jakością informacji umożliwiających identyfikację osób są ważne, ponieważ niedokładne lub nieaktualne informacje umożliwiające identyfikację osób przechowywane przez organizacje mogą powodować problemy dotyczące poszczególnych osób fizycznych. Organizacje biorą pod uwagę jakość informacji umożliwiających identyfikację osób zaangażowanych w funkcje biznesowe, gdzie niedokładne informacje mogą skutkować niekorzystnymi decyzjami lub odmową świadczeń i usług, lub też ujawnienie tych informacji może spowodować stygmatyzację. Prawidłowe informacje, w pewnych okolicznościach, mogą powodować problemy dla osób fizycznych, które przewyższają korzyści organizacji przechowujących te informacje. Organizacje rozważają stworzenie zasad i procedur dotyczących usuwania takich informacji.

SAOP zapewnia, że istnieją praktyczne środki i mechanizmy, które są dostępne dla osób fizycznych lub ich upoważnionych przedstawicieli w celu uzyskania korekty lub usunięcia danych osobowych. Procesy poprawiania lub usuwania danych są jasno określone i publicznie dostępne. Organizacje decydują o usunięciu lub poprawieniu danych w oparciu o zakres wniosków, żądane zmiany i wpływ zmian. Ponadto procesy obejmują udzielanie osobom fizycznym odpowiedzi na decyzje o odrzuceniu wniosków o poprawienie lub usunięcie danych.

Organizacje powiadamiają osoby fizyczne lub wyznaczonych przez nie przedstawicieli, gdy ich dane osobowe zostaną poprawione lub usunięte w celu zapewnienia przejrzystości i potwierdzenia wykonanych działań. Ze względu na złożoność przepływów i przechowywania danych, może zaistnieć potrzeba poinformowania innych podmiotów o poprawieniu lub usunięciu danych. Powiadomienie wspiera spójne poprawianie i usuwanie informacji umożliwiających identyfikację osób w całym ekosystemie danych.

Zabezpieczenia powiązane: PM-23, SI-18.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [OMB M-19-15], [NIST SP 800-188].

PM-23 ORGAN ZARZĄDZANIA DANYMI

Zabezpieczenie podstawowe: Ustanowienie organu zarządzającego danymi składającego się z [Realizacja: *role określone przez organizację*] z [*Realizacja: obowiązki określone przez organizację*].

Omówienie: Organ ds. zarządzania danymi może pomóc w zapewnieniu, że organizacja posiada spójne polityki i zdolność do równoważenia użyteczności danych z wymogami bezpieczeństwa i ochrony prywatności. Organ ds. zarządzania danymi ustanawia polityki, procedury i standardy, które ułatwiają zarządzanie danymi, tak aby dane, w tym dane osobowe, były skutecznie zarządzane i utrzymywane zgodnie z obowiązującymi przepisami, rozporządzeniami, dyrektywami, politykami, standardami i wytycznymi. Obowiązki mogą obejmować opracowanie i wdrożenie wytycznych, które wspierają modelowanie danych, jakość, integralność i potrzeby w zakresie określania informacji umożliwiających identyfikację osób w całym cyklu życia informacji, a także przeglądanie i zatwierdzanie wniosków o udostępnienie danych poza organizacją, archiwizację wniosków i udostępnionych danych oraz prowadzenie monitoringu po ich udostępnieniu w celu zapewnienia, że założenia przyjęte w ramach udostępniania danych są nadal aktualne. Członkami organu ds. zarządzania danymi są CIO, SAISO, oraz SAOP.[77]

Zabezpieczenia powiązane: AT-2, AT-3, PM-19, PM-22, PM-24, PT-7, SI-4, SI-19.

Zabezpieczenia rozszerzone: Brak.

Referencje: [EVIDACT], [OMB A-130], [OMB M-19-23], [NIST SP 800-188].

[77] Patrz: NSC 800-37; NSC 7298.

PM-24 RADA DS. INTEGRALNOŚCI DANYCH

Zabezpieczenie podstawowe: Ustanowienie rady ds. integralności danych w celu:

a. Przeglądania propozycji przeprowadzenia lub uczestnictwa w programie dopasowującym; oraz

b. Przeprowadzenie corocznego przeglądu wszystkich dopasowujących programów, w których brała udział organizacja.

Omówienie: Rada ds. integralności danych to rada wyższych urzędników / pracowników wyznaczonych przez kierownika jednostki organizacyjnej, która jest odpowiedzialna m.in. za przegląd propozycji organizacji dotyczących przeprowadzenia lub uczestnictwa w programie dopasowywania oraz przeprowadzanie corocznego przeglądu wszystkich programów dopasowujących, w których organizacja uczestniczyła. Ogólnie rzecz biorąc, program dopasowujący to dokonywane komputerowo porównanie zapisów z dwóch lub więcej zautomatyzowanych systemów zapisów podmiotów publicznych lub zautomatyzowanego systemu zapisów podmiotu publicznego i zapisów prowadzonych przez organizacją (lub jej przedstawiciela). Program dopasowujący odnosi się do programów świadczeń publicznych lub rejestrów osobowych lub płacowych. W skład rady ds. integralności danych wchodzi co najmniej inspektor ochrony danych oraz SAOP.

Zabezpieczenia powiązane: AC-4, PM-19, PM-23, PT-2, PT-8.

Zabezpieczenia rozszerzone: Brak.

Referencje: [PRIVACT], [0MB A-130], [OMB A-108].

PM-25 MINIMALIZACJA DANYCH OSOBOWYCH WYKORZYSTYWANYCH W TESTACH, SZKOLENIACH I BADANIACH

Zabezpieczenie podstawowe:

a. Opracowywanie, dokumentowanie i wdrażanie polityk i procedur, które dotyczą wykorzystania informacji umożliwiających identyfikację osób do celów wewnętrznych testów, szkoleń i badań;

b. Ograniczenie lub zminimalizowanie ilości danych osobowych wykorzystywanych do celów wewnętrznych testów, szkoleń i badań;

c. Zezwolenie na wykorzystanie informacji umożliwiających identyfikację osób, gdy informacje takie są wymagane do celów wewnętrznych testów, szkoleń i badań; oraz

d. Przegląd i aktualizacja zasad i procedur [*Realizacja: częstotliwość określona przez organizację*].

Omówienie: Wykorzystanie danych osobowych w testach, badaniach i szkoleniach zwiększa ryzyko nieuprawnionego ujawnienia lub niewłaściwego wykorzystania takich informacji. Organizacje konsultują się SAOP[78] i/lub radcą prawnym w celu zapewnienia, że wykorzystanie danych osobowych w testach, szkoleniach i badaniach jest zgodne z pierwotnym celem, dla którego zostały one zebrane. Jeżeli jest to możliwe, organizacje używają danych zastępczych, aby uniknąć ujawnienia informacji umożliwiających identyfikację osób podczas przeprowadzania testów, szkoleń i badań.

Zabezpieczenia powiązane: PM-23, PT-3, SA-3, SA-8, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [0MB A-130].

[78] Patrz: NSC 800-37; NSC 7298.

PM-26 ZARZĄDZANIE SKARGAMI

Zabezpieczenie podstawowe: Wdrożenie procesu przyjmowania i odpowiadania na skargi, wątpliwości lub pytania osób fizycznych dotyczące bezpieczeństwa organizacyjnego i praktyk ochrony prywatności, który obejmuje:

a. Mechanizmy, które są łatwe w użyciu i łatwo dostępne dla społeczeństwa;

b. Wszystkie informacje niezbędne do skutecznego złożenia reklamacji;

c. Mechanizmy śledzenia w celu zapewnienia, że wszystkie otrzymane skargi są przeglądane i rozpatrywane w ciągu [*Realizacja: okres czasu określony przez organizację*]*;*

d. Potwierdzanie otrzymania skarg, zastrzeżeń lub pytań od osób fizycznych w ciągu [*Realizacja: okres czasu określony przez organizację*]*;* oraz

e. Reagowanie na skargi, wątpliwości lub pytania osób fizycznych w ramach [*Realizacja: okres czasu określony przez organizację*].

Omówienie: Skargi, pytania i wnioski osób fizycznych mogą służyć jako cenne źródło informacji dla organizacji i ostatecznie przyczynić się do poprawy modeli operacyjnych, wykorzystania technologii, praktyk w zakresie gromadzenia danych i zabezpieczeń. Mechanizmy, które mogą być wykorzystywane przez społeczeństwo, obejmują gorącą linię telefoniczną (telefoniczny punkt kontaktowy), pocztę elektroniczną lub formularze internetowe. Informacje niezbędne do skutecznego składania skarg obejmują dane kontaktowe SAOP lub innego pracownika wyznaczonego do przyjmowania skarg. Skargi dotyczące prywatności mogą również dotyczyć danych osobowych, które są przetwarzane zgodnie z odpowiednimi zasadami i procesami.

Zabezpieczenia powiązane: IR-7, IR-9, PM-22, SI-18.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130].

PM-27 SPRAWOZDAWCZOŚĆ W ZAKRESIE OCHRONY PRYWATNOŚCI

Zabezpieczenie podstawowe:

a. Opracowanie [*Realizacja: raporty dotyczące ochrony prywatności zdefiniowane przez organizację*] i rozpowszechnienie ich wśród:

   1. [*Realizacja: organy nadzorcze określone przez organizację*] *w* celu wykazania rozliczalności w ramach mandatów ustawowych, wykonawczych i dotyczących ochrony prywatności; oraz

   2. [*Realizacja: osoby wyznaczone przez organizację*] i inny personel odpowiedzialny za monitorowanie zgodności z programem ochrony prywatności; oraz

b. Przeglądanie i aktualizacja raportów dotyczących prywatności [*Realizacja: częstotliwość określona przez organizację*].

Omówienie: Poprzez wewnętrzną i zewnętrzną sprawozdawczość organizacje promują odpowiedzialność i przejrzystość w działaniach związanych z ochroną prywatności. Raportowanie może również pomóc organizacjom w określaniu postępów w spełnianiu wymogów zgodności z polityką prywatności i zabezpieczeniami prywatności, w porównaniu osiąganych wyników, wykrywaniu podatności, identyfikowaniu luk w polityce i jej wdrażaniu oraz określaniu modeli sukcesu.

Raporty o ochronie prywatności obejmują roczne raporty o ochronie prywatności wymagane przez przepisy wykonawcze oraz inne publiczne raporty wymagane przez prawo, przepisy lub politykę, w tym wewnętrzne polityki organizacji. SAOP konsultuje się, w stosownych przypadkach, z radcą prawnym w celu zapewnienia, że organizacje spełniają wszystkie obowiązujące wymogi w zakresie sprawozdawczości dotyczącej ochrony prywatności.

Zabezpieczenia powiązane: IR-9, PM-19.

Zabezpieczenia rozszerzone: Brak.

Referencje: [FISMA], [OMB A-130], [OMB A-108].

PM-28 OPRACOWYWANIE RAM RYZYKA

Zabezpieczenie podstawowe:

a. Zidentyfikowanie i udokumentowanie:

   1. Założeń mających wpływ na ocenę ryzyka, reakcje na ryzyko i monitorowanie ryzyka;

   2. Ograniczeń mających wpływ na ocenę ryzyka, reakcje na ryzyko i monitorowanie ryzyka;

   3. Priorytetów i rozwiązań alternatywnych uwzględnianych przez organizację zarządzaniu ryzykiem; oraz

   4. Tolerancji ryzyka organizacyjnego;

b. Przekazywanie wyników działań związanych z określaniem ryzyka wśród [*Realizacja: personel wyznaczony przez organizację*]; oraz

c. Przeglądanie i aktualizowanie zagadnień związanych z ramami ryzyka [Realizacja: *częstotliwość określona przez organizację*].

Omówienie: Tworzenie ram dla ryzyka jest najbardziej efektywne, gdy jest prowadzone na poziomie organizacji i w porozumieniu z interesariuszami w całej organizacji, w tym z właścicielami misji, biznesu i systemów. Założenia, ograniczenia, tolerancja ryzyka, priorytety i rozwiązania alternatywne zidentyfikowane w ramach procesu definiowania ryzyka stanowią podstawę strategii zarządzania ryzykiem, która z kolei informuje o prowadzeniu oceny ryzyka, reakcji na ryzyko i działaniach monitorujących ryzyko. Wyniki procesu określania ryzyka są udostępniane personelowi organizacji, w tym właścicielom misji i firm, właścicielom lub zarządzającym informacjami, właścicielom systemów, osobom autoryzującym, SAISO, SAOP i SAORM.[79]

[79] Patrz: NSC 800-37; NSC 7298.

Zabezpieczenia powiązane: CA-7, PM-9, RA-3, RA-7.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [NIST SP 800-39].

PM-29 ROLE KIEROWNICZE PROGRAMU ZARZĄDZANIA RYZYKIEM

Zabezpieczenie podstawowe:

a. Powołanie SAORM[80] odpowiedzialnego za zarządzanie ryzykiem w celu dostosowania procesów zarządzania bezpieczeństwem informacji organizacyjnych i ochroną prywatności do procesów planowania strategicznego, operacyjnego i budżetowego; oraz

b. Ustanowienie funkcji RE[81], której zadaniem będzie przeglądanie i analizowanie ryzyka z perspektywy całej organizacji oraz zapewnienie spójności zarządzania ryzykiem w całej organizacji.

Omówienie: SAORM zarządza ryzykiem (funkcja) w działaniach związanych z zarządzaniem ryzykiem w całej organizacji.

Zabezpieczenia powiązane: PM-2, PM-19.

Zabezpieczenia rozszerzone: Brak.

Referencje: [NIST SP 800-37], [NIST SP 800-181].

[80] Patrz: NSC 800-37; NSC 7298.

[81] jw.

PM-30 STRATEGIA ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW

Zabezpieczenie podstawowe:

a. Opracowanie ogólnoorganizacyjnej strategii zarządzania ryzykiem związanym z łańcuchem dostaw, rozwojem, pozyskiwaniem, utrzymaniem i utylizacją systemów, komponentów systemu i usług systemowych;

b. Wdrożenie strategii zarządzania ryzykiem w łańcuchu dostaw w sposób spójny w całej organizacji; oraz

c. Przeglądanie i aktualizowanie strategii zarządzania ryzykiem w łańcuchu dostaw [*Realizacja: częstotliwość określona przez organizację*] lub w miarę potrzeb, w celu uwzględnienia zmian organizacyjnych.

Omówienie: Strategia zarządzania ryzykiem w łańcuchu dostaw obejmująca całą organizację obejmuje jednoznaczne określenie podatności na ryzyko w łańcuchu dostaw i tolerancji dla organizacji, akceptowalne strategie lub zabezpieczenia ograniczania ryzyka w łańcuchu dostaw, proces konsekwentnej oceny i monitorowania ryzyka w łańcuchu dostaw, podejście do wdrażania i informowania o strategii zarządzania ryzykiem w łańcuchu dostaw oraz związane z tym role i obowiązki. Zarządzanie ryzykiem w łańcuchu dostaw obejmuje kwestie związane z bezpieczeństwem i ochroną prywatności w związku z rozwojem, nabyciem, utrzymaniem i utylizacją systemów, elementów systemu i usług systemowych. Strategia zarządzania ryzykiem w łańcuchu dostaw może zostać włączona do nadrzędnej strategii zarządzania ryzykiem w organizacji oraz może stanowić wytyczne i źródło informacji na temat polityki dotyczącej łańcucha dostaw i planów zarządzania ryzykiem w łańcuchu dostaw na poziomie systemu. Ponadto, wykorzystanie funkcji zarządzania ryzykiem może ułatwić konsekwentne stosowanie strategii zarządzania ryzykiem łańcucha dostaw w całej organizacji. Strategia zarządzania ryzykiem w łańcuchu dostaw jest wdrażana na poziomie organizacji i misji/przedsiębiorstwa, natomiast plan zarządzania ryzykiem w łańcuchu dostaw (patrz zabezpieczenie SR-2) jest wdrażany na poziomie systemu.

Zabezpieczenia powiązane: CM-10, PM-9, SR-1, SR-2, SR-3, SR-4, SR-5, SR-6, SR-7, SR-8, SR-9, SR-11.

Zabezpieczenia rozszerzone:

(1) STRATEGIA ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW | DOSTAWCY ELEMENTÓW KRYTYCZNYCH LUB ISTOTNYCH Z PUNKTU WIDZENIA MISJI

Określanie, ustalanie priorytetów i ocenianie dostawców technologii, produktów i usług krytycznych lub istotnych z punktu widzenia misji organizacji.

Omówienie: Identyfikacja i priorytetyzacja dostawców krytycznych lub istotnych z punktu widzenia misji organizacji technologii, produktów i usług ma nadrzędne znaczenie dla misji/powodzenia biznesowego organizacji. Ocena dostawców jest przeprowadzana z wykorzystaniem przeglądów dostawców (patrz zabezpieczenie SR-6) oraz procesów oceny ryzyka łańcucha dostaw (patrz zabezpieczenie RA-3(1)). Analiza ryzyka łańcucha dostaw może pomóc organizacji w identyfikacji systemów lub komponentów, dla których wymagane jest dodatkowe ograniczenie ryzyka łańcucha dostaw.

Zabezpieczenia powiązane: RA-3, SR-6.

Referencje: [PRIVACT], [FASC18], [41 CFR 201], [E0 13873], [OMB A-130], [0MB M-17-06] [ISO 27036], [ISO 20243], [NIST SP 800-161], [IR 8272], [CNSSD 505].

PM-31 STRATEGIA CIĄGŁEGO MONITOROWANIA

Zabezpieczenie podstawowe: Opracowanie strategii ciągłego monitorowania w całej organizacji i wdrożenie programów ciągłego monitorowania, które obejmują:

a. Ustalenie następujących wskaźników dla całej organizacji, które będą monitorowane: [*Realizacja: wskaźniki zdefiniowane przez organizację*];

b. Ustalenie monitorowania [*Realizacja: częstotliwość określona przez organizację*] oraz oceny skuteczności zabezpieczeń [*Realizacja: częstotliwość określona przez organizację*];

c. Bieżące monitorowanie zdefiniowanych organizacyjnie wskaźników zgodnie ze strategią ciągłego monitorowania;

d. Korelacja i analiza informacji uzyskanych w wyniku oceny i monitorowania zabezpieczeń;

e. Działania w zakresie reagowania na wyniki analizy informacji dotyczących oceny zabezpieczeń i monitorowania; oraz

f. Zgłaszanie stanu bezpieczeństwa i ochrony prywatności systemów organizacyjnych do [*Realizacja: personel określony przez organizację lub role*] [*Realizacja: częstotliwość określona przez organizację*].

Omówienie: Ciągłe monitorowanie na poziomie organizacji usprawnia bieżącą świadomość dotyczącą stanu bezpieczeństwa i ochrony prywatności w całej organizacji w celu wsparcia decyzji dotyczących zarządzania ryzykiem organizacyjnym. Terminy "ciągły" i "bieżący" oznaczają, że organizacje oceniają i monitorują swoje zabezpieczenia i ryzyko z częstotliwością wystarczającą do wspierania decyzji opartych na ryzyku. Różne rodzaje zabezpieczeń mogą wymagać różnych częstotliwości monitorowania. Wyniki ciągłego monitorowania prowadzą i informują o działaniach podejmowanych przez organizacje w odpowiedzi na ryzyko. Programy ciągłego monitorowania pozwalają organizacjom na utrzymanie uprawnień systemów i zabezpieczeń wspólnych w wysoce dynamicznych środowiskach

działania, ze zmieniającą się misją i potrzebami biznesowymi, zagrożeniami, słabymi punktami i technologiami. Stały dostęp do informacji związanych z bezpieczeństwem i ochroną prywatności poprzez sprawozdania i diagramy daje pracownikom organizacji możliwość podejmowania skutecznych, terminowych i świadomych decyzji w zakresie zarządzania ryzykiem, w tym bieżących decyzji dotyczących autoryzacji. Celem dalszego ułatwienia zarządzania ryzykiem związanym z bezpieczeństwem i ochroną prywatności, organizacje rozważają dostosowanie zdefiniowanych przez siebie wskaźników monitorowania do tolerancji na ryzyko organizacyjne, określonej w strategii zarządzania ryzykiem. Wymogi dotyczące monitorowania, w tym potrzeba monitorowania, mogą być zawarte w innych zabezpieczeniach podstawowych i zabezpieczeniach rozszerzonych takich jak, : AC-2g, AC-2(7), AC-2(12)(a), AC-2(7)(b), AC-2(7)(c), AC-17(1), AT-4a, AU-13, AU-13(1), AU-13(2), CA-7, CM-3f, CM-6d, CM-11c, IR-5, MA-2b, MA-3a, MA-4a, PE-3d, PE-6, PE-14b, PE-16, PE-20, PM-6, PM-23, PS-7e, SA-9c, SC- 5(3)(b), SC-7a, SC-7(24)(b), SC-18b, SC-43b, SI-4.

Zabezpieczenia powiązane: AC-2, AC-6, AC-17, AT-4, AU-6, AU-13, CA-2, CA-5, CA-6, CA-7, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-16, PE-20, PL-2, PM-4, PM-6, PM-9, PM-10, PM-12, PM-14, PM-23, PM-28, PS-7, PT-7, RA-3, RA-5, RA-7, SA-9, SA-11, SC-5, SC- 7, SC-18, SC-38, SC-43, SI-3, SI-12, SR-2, SR-4.

Referencje: [NIST SP 800-37], [NIST SP 800-39], [NIST SP 800-137], [NIST SP 800-137A].

PM-32 PRZEZNACZENIE

Zabezpieczenie podstawowe: Analizowanie [*Realizacja: zdefiniowane przez organizację systemy lub komponenty systemów*] wspomagających podstawowe usługi lub funkcje misji organizacji w celu zapewnienia, że zasoby informacyjne są wykorzystywane zgodnie z ich przeznaczeniem.

Omówienie: Systemy są przeznaczone do wspierania konkretnej misji lub funkcji biznesowej. Z czasem jednak systemy i komponenty systemu mogą być wykorzystywane do wspierania usług i funkcji, które wykraczają poza zakres zamierzonej misji lub funkcji biznesowej. Może to skutkować narażeniem zasobów informacyjnych na działanie niewłaściwych warunków i wykorzystanie, które może znacznie zwiększyć stopień zagrożenia. W ten sposób systemy są bardziej podatne na kompromitację, co może ostatecznie wpłynąć na usługi i funkcje, do których zostały przeznaczone. Jest to szczególnie istotne w przypadku usług i funkcji o znaczeniu kluczowym dla misji. Poprzez analizę wykorzystania zasobów, organizacje mogą zidentyfikować tego typu potencjalne zagrożenia.

Zabezpieczenia powiązane: CA-7, PL-2, RA-3, RA-9.

Zabezpieczenia rozszerzone: Brak.

Referencje: [NIST SP 800-160-1], [NIST SP 800-160-2].

KATEGORIA PS – BEZPIECZEŃSTWO OSOBOWE

PS-1 POLITYKA I PROCEDURY

Zabezpieczenie podstawowe:

a. Opracowywanie, dokumentowanie i rozpowszechnianie wśród [Realizacja: *personel lub role określone przez organizację*]:

   1. [*Wybór (jeden lub więcej): poziom organizacji; poziom misji/procesu biznesowego; poziom systemu*] polityki bezpieczeństwa osobowego, która:

      (a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami; oraz

      (b) Jest zgodna z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi; oraz

   2. Procedur ułatwiających wdrożenie polityki bezpieczeństwa osobowego oraz powiązanych zabezpieczeń w zakresie bezpieczeństwa osobowego;

b. Wyznaczanie [Realizacja: *osoba wyznaczona przez organizację*] do zarządzania rozwojem, dokumentacją i rozpowszechnianiem polityki i procedur bezpieczeństwa osobowego; oraz

c. Przeglądanie i aktualizacja bieżącej:

   1. Polityki bezpieczeństwa osobowego z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*]; oraz

   2. Procedur bezpieczeństwa osobowego z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*].

Omówienie: Polityka i procedury w zakresie bezpieczeństwa osobowego dotyczą zabezpieczeń w kategorii *Bezpieczeństwo osobowe* (PS), które są wdrażane w ramach systemów i organizacji. Strategia zarządzania ryzykiem jest ważnym czynnikiem przy

tworzeniu takich polityk i procedur. Polityki i procedury przyczyniają się do zapewnienia bezpieczeństwa i ochrony prywatności. Dlatego ważne jest, aby programy bezpieczeństwa i ochrony prywatności były opracowywane wspólnie przy kształtowaniu polityki i procedur bezpieczeństwa osobowego. Polityki i procedury dotyczące programów bezpieczeństwa i ochrony prywatności na poziomie organizacji są ogólnie rzecz biorąc preferowane i mogą eliminować potrzeby tworzenia polityk i procedur specyficznych dla danej misji lub systemu. Polityka może być włączona, jako część ogólnej polityki bezpieczeństwa i ochrony prywatności lub reprezentowana przez wiele polityk odzwierciedlających złożony charakter organizacji. Procedury mogą być ustanowione dla programów bezpieczeństwa i ochrony prywatności, dla misji lub procesów biznesowych oraz dla systemów, jeśli to konieczne. Procedury opisują sposób wdrażania zasad lub zabezpieczeń i mogą być skierowane do osoby lub roli, która jest przedmiotem procedury. Procedury mogą być udokumentowane w planach bezpieczeństwa i ochrony prywatności systemu w jednym lub kilku oddzielnych dokumentach.

Zdarzenia, które mogą spowodować konieczność aktualizacji polityki i procedur bezpieczeństwa osobowego, obejmują wyniki oceny lub audytu, incydenty lub naruszenia bezpieczeństwa, lub zmiany w przepisach prawa, zarządzeniach, dyrektywach, rozporządzeniach, zasadach, standardach i wytycznych.

Oświadczenie o wprowadzeniu zabezpieczeń nie jest równoznaczne z ustanowieniem polityki lub procedury organizacyjnej.

Zabezpieczenia powiązane: PM-9, PS-8, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [NIST SP 800-12], [NIST SP 800-30], [NIST SP 800-39], [NIST SP 800-100].

PS-2 OKREŚLANIE RYZYKA DLA STANOWISKA PRACY

Zabezpieczenie podstawowe:

a. Przypisanie oznaczenia ryzyka do wszystkich stanowisk organizacyjnych;

b. Ustalenie kryteriów selekcji osób zajmujących te stanowiska; oraz

c. Przeglądanie i aktualizowanie oznaczeń ryzyka stanowisk [*Realizacja: częstotliwość określona przez organizację*].

Omówienie: Oznaczanie ryzyka stanowiska odzwierciedla politykę organizacji *(ang. Office of Personnel Management - OPM)*. Właściwe oznaczenie stanowiska jest podstawą skutecznego i spójnego programu predyspozycji i bezpieczeństwa personelu. System wyznaczania stanowisk (*ang. Position Designation System - PDS*) określa obowiązki i odpowiedzialność na danym stanowisku w celu określenia stopnia potencjalnego uszczerbku dla wydajności lub integralności usługi w wyniku niewłaściwego postępowania osoby zajmującej dane stanowisko i określa poziom ryzyka związanego z tym stanowiskiem. Ocena PDS określa również, czy obowiązki i zakres rozliczalności danego stanowiska mogą mieć istotny negatywny wpływ na bezpieczeństwo i stopień tego potencjalnego wpływu, co określa poziom wrażliwości danego stanowiska. Wyniki oceny określają, jaki poziom postępowania sprawdzającego jest przeprowadzany w odniesieniu do danego stanowiska. Oznaczenia ryzyka może być wskazówką i informacją o rodzajach upoważnień, które osoby fizyczne otrzymują podczas uzyskiwania dostępu do informacji organizacyjnych i systemów informatycznych. Kryteria sprawdzania stanowisk obejmują wyraźne wymogi dotyczące wyznaczania ról związanych z bezpieczeństwem informacji. Ustanawiają wymogi dla organizacji w zakresie oceny odpowiednich stanowisk objętych kontrolą pod kątem wrażliwości stanowiska oraz wyznaczania ryzyka związanego z danym stanowiskiem w sposób współmierny do obowiązków i rozliczalności na tych stanowiskach.

Zabezpieczenia powiązane: AC-5, AT-3, PE-2, PE-3, PL-2, PS-3, PS-6, SA-5, SA-21, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [5 CFR 731], [SP. 800-181].

PS-3 DOBÓR PERSONELU

Zabezpieczenie podstawowe:

a. Przeprowadzanie postępowania sprawdzającego osób przed autoryzowaniem dostępu do systemu; oraz

b. Ponowne sprawdzanie osób zgodnie z [Realizacja: *warunki określone przez organizację, które wymagają ponownego sprawdzenia oraz w przypadku, gdy ponowne postępowanie sprawdzające jest wskazane, częstotliwość ponownego sprawdzenia*].

Omówienie: Działania związane z postępowaniem sprawdzającym ponownym sprawdzaniem personelu odzwierciedlają obowiązujące prawo, zarządzenia, dyrektywy, rozporządzenia, zasady, standardy, wytyczne i konkretne kryteria ustalone dla określenia ryzyka przydzielonych stanowisk. Przykłady sprawdzania personelu obejmują badania przeszłości i weryfikacje urzędowe. Przepisy określają warunki i częstotliwość ponownych sprawdzeń personelu mającego dostęp do systemów w zależności od rodzaju informacji przetwarzanych, przechowywanych lub przesyłanych przez te systemy.

Zabezpieczenia powiązane: AC-2, IA-4, MA-5, PE-2, PM-12, PS-2, PS-6, PS-7, SA-21.

Zabezpieczenia rozszerzone:

(1) DOBÓR PERSONELU | INFORMACJE NIEJAWNE

Sprawdzanie, czy osoby mające dostęp do systemu przetwarzającego, przechowującego lub przekazującego informacje niejawne posiadają poświadczenia bezpieczeństwa do najwyższego poziomu klasyfikacji informacji, do których mają dostęp w systemie.

Omówienie: Informacje niejawne to najbardziej wrażliwe informacje, które organizacja przetwarza, przechowuje lub przekazuje. Przed uzyskaniem dostępu do takich informacji osoby fizyczne muszą koniecznie uzyskać wymagane poświadczenia bezpieczeństwa i uprawnienia dostęp do systemu. Uprawnienia

dostępu są egzekwowane za pomocą kontroli dostępu do systemu (patrz zabezpieczenie AC-3) i kontroli przepływu systemu (patrz zabezpieczenie. AC-4).

Zabezpieczenia powiązane: AC-3, AC-4.

(2) DOBÓR PERSONELU | POSTĘPOWANIA SPRAWDZAJĄCE

Sprawdzanie, czy osoby mające dostęp do systemu przetwarzającego, przechowującego lub przekazującego informacje niejawne, podlegały, zgodnie z ustawą o ochronie informacji niejawnych, stosownemu postępowaniu sprawdzającemu.

Omówienie: Rodzaje informacji klasyfikowanych, które wymagają specjalnego traktowanie, zawarte są w ustawie o ochronie informacji niejawnych.

Zabezpieczenia powiązane: AC-3, AC-4.

(3) DOBÓR PERSONELU | INFORMACJE WYMAGAJĄCE SZCZEGÓLNEJ OCHRONY

Sprawdzanie, czy osoby mające dostęp do systemu przetwarzającego, przechowującego lub przesyłającego informacje wymagające szczególnej ochrony:

(a) Posiadają ważne poświadczenia bezpieczeństwa zezwalające na dostęp do informacji, których posiadanie jest wymagane w związku z powierzonymi im obowiązkami służbowymi; oraz

(b) Spełniają dodatkowe kryteria [*Realizacja: zdefiniowane przez organizację dodatkowe kryteria selekcji personelu*].

Omówienie: Informacje organizacyjne, które wymagają specjalnej ochrony, obejmują kontrolowane informacje jawne. Przepisy określają warunki i częstotliwość ponownych sprawdzeń personelu mającego dostęp do systemów w zależności od rodzaju informacji przetwarzanych przez te systemy.

Zabezpieczenia powiązane: Brak.

(4) DOBÓR PERSONELU | WYMAGANIA DOTYCZĄCE OBYWATELSTWA

Sprawdzanie, czy osoby mające dostęp do systemu przetwarzającego, przechowującego lub przesyłającego [Realizacja: *typy informacji określone przez organizację*] spełniają [*Realizacja: wymagania dotyczące obywatelstwa określone przez organizację*].

Omówienie: Brak.

Zabezpieczenia powiązane: Brak.

Referencje: [EO 13526], [EO 13587], [FIPS 199], [FIPS 201-2], [NIST SP 800-60-1], [NIST SP 800-60-2], [NIST SP 800-73-4], [NIST SP 800-76-2], [NIST SP 800-78-4].

PS-4 ZAKOŃCZENIE ZATRUDNIENIA

Zabezpieczenie podstawowe: Po zakończeniu indywidualnego zatrudnienia organizacja:

a. Wyłącza dostęp do systemu w ciągu [*Realizacja: okres czasu określony przez organizację*];

b. Kończy / odwołuje wszelkie pełnomocnictwa / poświadczenia powiązane z osobą;

c. Prowadzi rozmowy końcowe, które obejmują omówienie tematów bezpieczeństwa [*Realizacja: tematy związane z bezpieczeństwem informacji określone przez organizację*];

d. Odbiera wszystkie aktywa związane z bezpieczeństwem systemu wykorzystywane, przydzielone oraz wytworzone przez pracownika na danym stanowisku; oraz

e. Zachowuje dostęp do informacji organizacyjnych i systemów nadzorowanych (użytkowanych) przez zwalnianą osobę.

Omówienie: Aktywa systemu obejmują sprzętowe tokeny uwierzytelniające, podręczniki techniczne administrowania systemem, klucze, karty identyfikacyjne i przepustki wstępu do obiektów. Rozmowy końcowe zapewniają, że osoby odchodzące z pracy są świadome ograniczeń w zakresie bezpieczeństwa wynikających z faktu bycia byłymi pracownikami oraz, że własność związana z systemem jest odpowiednio rozliczana. Tematy związane z bezpieczeństwem podczas rozmów końcowych obejmują przypominanie o ograniczeniach zawartych w umowach o zachowaniu poufności i potencjalnych ograniczeniach dotyczących przyszłego zatrudnienia. W przypadku niektórych osób przeprowadzenie rozmów końcowych nie zawsze jest możliwe, np. w przypadkach związanych z niedostępnością przełożonych, chorobą lub porzuceniem pracy. Rozmowy końcowe są ważne dla osób posiadających poświadczenia bezpieczeństwa. Terminowe zakończenie stosunku pracy jest istotne dla osób, z którymi rozwiązano stosunek

pracy z podaniem przyczyny. W pewnych sytuacjach organizacje rozważają wyłączenie kont systemowych osób, z którymi rozwiązuje się umowę, zanim te osoby zostaną o tym powiadomione.

Zabezpieczenia powiązane: AC-2, IA-4, PE-2, PM-12, PS-6, PS-7.

Zabezpieczenia rozszerzone:

(1) ZAKOŃCZENIE ZATRUDNIENIA | ZOBOWIĄZANIA PO ZAKOŃCZENIU ZATRUDNIENIA

(a) Powiadamianie osób, z którymi rozwiązano stosunek pracy, o obowiązujących, prawnie wiążących wymogach dotyczących ochrony informacji organizacyjnych po ustaniu stosunku pracy; oraz

(b) Wymaganie podpisania przez zwalniane osoby oświadczenie w zakresie zachowania tajemnicy organizacji po okresie zatrudnienia.

Omówienie: Organizacje konsultują się z radcą prawnym w sprawach dotyczących wymagań po ustaniu zatrudnienia w stosunku do osób, które utraciły pracę.

Zabezpieczenia powiązane: Brak.

(2) ZAKOŃCZENIE ZATRUDNIENIA | AUTOMATYCZNE POWIADAMIANIE

Używanie [Realizacja: *mechanizmy automatyczne zdefiniowane przez organizację*] do [*Wybór (jeden lub więcej): powiadomienie* [*Realizacja: personel lub role zdefiniowane przez organizację*] *o indywidualnym zakończeniu pracy przez daną osobę; wyłączenie dostępu do zasobów systemu*].

Omówienie: W organizacjach zatrudniających wielu pracowników nie wszyscy, którzy powinni być poinformowani o wypowiedzeniu, otrzymują na czas odpowiednie powiadomienia. Zautomatyzowane mechanizmy mogą być używane do wysyłania automatycznych alertów lub powiadomień personelu organizacyjnego lub ról, gdy poszczególne osoby są zwalniane. Takie automatyczne alerty lub powiadomienia mogą być przekazywane na różne sposoby, w tym przez telefon, pocztę elektroniczną, wiadomości tekstowe lub

strony internetowe. Zautomatyzowane mechanizmy mogą być również stosowane do szybkiego i dokładnego uniemożliwienia dostępu do zasobów systemowych po zakończeniu pracy przez pracownika.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

PS-5 OBSADZENIE LUB PRZENIESIENIE STANOWISKA

Zabezpieczenie podstawowe:

a. Przegląd i potwierdzenie bieżącej potrzeby operacyjnej w zakresie aktualnych logicznych i fizycznych uprawnień dostępu do systemów i obiektów w przypadku zmiany przydziału lub przeniesienia osób na inne stanowiska w organizacji;

b. Inicjowanie [*Realizacja: zdefiniowane przez organizację działania przeniesienia lub ponownego obsadzenia stanowiska*] w ciągu [*Realizacja: zdefiniowane przez organizację okres po formalnym przeniesieniu / ponownym obsadzeniu*];

c. Modyfikacja uprawnień dostępu w zależności od potrzeb, tak aby odpowiadały one wszelkim zmianom potrzeb operacyjnych wynikających ze zmiany przydziału lub przeniesienia; oraz

d. Powiadamianie [*Realizacja: personel lub role określone przez organizację*] w ciągu [*Realizacja: okres czasu określony przez organizację*].

Omówienie: Przeniesienie personelu ma zastosowanie, gdy przesunięcia lub przeniesienia osób są stałe lub mają tak długi okres trwania, że uzasadniają działania. Organizacje określają działania odpowiednie dla rodzajów przeniesień lub transferów, zarówno stałych, jak i długoterminowych. Działania, które mogą być wymagane w przypadku przeniesienia personelu lub zmiany stanowiska w organizacji, obejmują zwrot starych i wydanie nowych kluczy, kart identyfikacyjnych i przepustek do obiektów; zamknięcie kont systemowych i założenie nowych kont; zmianę uprawnień dostępu do systemu (tj. przywilejów); oraz zapewnienie dostępu do oficjalnych dokumentów, do których osoby miały dostęp w poprzednich miejscach pracy i przy użyciu poprzednich kont systemowych.

Zabezpieczenia powiązane: AC-2, IA-4, PE-2, PM-12, PS-4, PS-7.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

PS-6 UMOWY DOSTĘPU / WSPÓŁPRACY

Zabezpieczenie podstawowe:

a. Opracowywanie i dokumentowanie umów o dostępie do systemów organizacyjnych;

b. Przegląd i aktualizacja umów o dostępie/współpracy [*Realizacja: częstotliwość określona przez organizację*]*;* oraz

c. Sprawdzanie, czy osoby wymagające dostępu do informacji i systemów organizacyjnych:

1. Podpisały odpowiednie umowy o dostępie przed udzieleniem dostępu; oraz

2. Ponowne podpisały umowy o dostępie/współpracy w celu zachowania dostępu do systemów organizacyjnych po aktualizacji umów o dostępie lub z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Omówienie: Umowy o dostępie/współpracy obejmują umowy o nieujawnianiu informacji, umowy o dopuszczalnym użytkowaniu, zasady postępowania oraz umowy dotyczące konfliktu interesów. Podpisane umowy o dostępie/współpracy zawierają potwierdzenie, że osoby fizyczne przeczytały, zrozumiały i zgadzają się przestrzegać ograniczenia związane z systemami organizacyjnymi, do których mają uprawniony dostęp. Organizacje mogą używać podpisów elektronicznych do potwierdzania umów o dostępie, chyba że jest to wyraźnie zabronione przez politykę organizacyjną.

Zabezpieczenia powiązane: AC-17, PE-2, PL-4, PS-2, PS-3, PS-6, PS-7, PS-8, SA-21, SI-12.

Zabezpieczenia rozszerzone:

(1) UMOWY DOSTEPU / WSPÓŁPRACY | INFORMACJE WYMAGAJĄCE SZCZEGÓLNEJ OCHRONY

[Wycofane: Włączone do PS-3].

(2) UMOWY DOSTEPU / WSPÓŁPRACY | INFORMACJE NIEJAWNE WYMAGAJĄCE OCHRONY SPECJALNEJ

Sprawdzenie, czy dostęp do informacji niejawnych wymagających szczególnej ochrony jest udzielany wyłącznie osobom, które:

(a) Posiadają ważne poświadczenia bezpieczeństwa, wydane przez krajową władzę bezpieczeństwa;

(b) Spełniają kryteria bezpieczeństwa osobowego; oraz

(c) Przeczytały, zrozumiały i podpisały umowy o zachowaniu poufności.

Omówienie: Rodzaje informacji klasyfikowanych, które wymagają specjalnego traktowanie, zawarte są w ustawie o ochronie informacji niejawnych. Kryteria bezpieczeństwa personelu odzwierciedlają obowiązujące przepisy, zarządzenia, dyrektywy, regulacje, zasady, standardy i wytyczne.

Zabezpieczenia powiązane: Brak.

(3) UMOWY DOSTEPU / WSPÓŁPRACY | WYMOGI PO ZAKOŃCZENIU ZATRUDNIENIA

a) Powiadamianie osób o obowiązujących, prawnie wiążących wymogach dotyczących ochrony informacji organizacyjnych po zatrudnieniu; oraz

b) Wymaganie od osób podpisania oświadczenia o zachowaniu tajemnicy informacji organizacyjnych.

Omówienie: Organizacje konsultują się z radcą prawnym w sprawach dotyczących wymogów po ustaniu zatrudnienia osób, z którymi rozwiązano umowę o pracę.

Zabezpieczenia powiązane: PS-4.

Referencje: Brak.

PS-7 BEZPIECZEŃSTWO OSOBOWE STRON TRZECICH

Zabezpieczenie podstawowe:

a. Ustanowienie wymagań dotyczących bezpieczeństwa personelu, w tym ról i obowiązków dostawców zewnętrznych w zakresie bezpieczeństwa;

b. Wymaganie od dostawców zewnętrznych przestrzegania zasad i procedur bezpieczeństwa personelu ustanowionych przez organizację;

c. Dokumentowanie wymogów bezpieczeństwa personelu;

d. Wymaganie od zewnętrznych usługodawców powiadamiania [*Realizacja: personel lub role określone przez organizację*] o każdym przeniesieniu lub zakończeniu pracy personelu zewnętrznego, który posiada poświadczenia i / lub identyfikatory organizacyjne lub posiada uprawnienia systemowe nie później niż do [*Realizacja: okres czasu zdefiniowany przez organizację*]*;* oraz

e. Monitorowanie stosowania przez dostawcę zasad i procedur bezpieczeństwa.

Omówienie: Dostawca zewnętrzny odnosi się do organizacji innych niż organizacja obsługująca lub nabywająca system. Do zewnętrznych dostawców należą biura usług, kontrahenci i inne organizacje świadczące usługi w zakresie rozwoju systemu, usługi informatyczne, usługi testowania lub oceny, aplikacje zlecane na zewnątrz oraz zarządzanie siecią/bezpieczeństwem. Organizacje jednoznacznie uwzględniają wymagania dotyczące bezpieczeństwa personelu w dokumentach związanych z nabywaniem. Dostawcy zewnętrzni mogą zatrudniać personel pracujący w obiektach organizacyjnych z poświadczeniami, identyfikatorami lub uprawnieniami systemowymi wydanymi przez organizację. Powiadomienia o zmianach personelu zewnętrznego gwarantują odpowiednią likwidację przywilejów i poświadczeń. Organizacje definiują przeniesienia i wypowiedzenia uznawane za podlegające zgłaszaniu na podstawie cech związanych z bezpieczeństwem, które obejmują funkcje, role oraz charakter poświadczeń lub przywilejów związanych z przeniesionymi lub wypowiedzianymi osobami.

Zabezpieczenia powiązane: AT-2, AT-3, MA-5, PE-3, PS-2, PS-3, PS-4, PS-5, PS-6, SA-5, SA-9, SA-21.

Zabezpieczenia rozszerzone: Brak.

Referencje: [NIST SP 800-35], [NIST SP 800-63-3].

PS-8 SANKCJE PERSONALNE

Zabezpieczenie podstawowe:

a. Stosowanie formalnej procedury sankcji organizacyjnych wobec osób, które nie przestrzegają ustalonych zasad i procedur dotyczących bezpieczeństwa informacji i ochrony prywatności; oraz

b. Powiadamianie [*Realizacja: zdefiniowany przez organizację personel lub role*] w ciągu [*Realizacja: zdefiniowany przez organizację okres czasu*] o rozpoczęciu formalnego procesu sankcji pracowniczych, określając osobę, na którą nałożono sankcje oraz powód nałożenia sankcji.

Omówienie: Sankcje organizacyjne odzwierciedlają obowiązujące przepisy prawa, zarządzenia, dyrektywy, regulacje, zasady, standardy i wytyczne. Procesy związane z sankcjami są opisane w umowach o dostępie i mogą być włączone, jako część ogólnych zasad dotyczących personelu organizacji i/lub określone w zasadach bezpieczeństwa i ochrony prywatności. Organizacje konsultują się z radcą prawnym w sprawach dotyczących sankcji pracowniczych.

Zabezpieczenia powiązane: Wszystkie zabezpieczenia XX-1, PL-4, PM-12, PS-6, PT-1.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

PS-9 OPISY STANOWISK PRACY

Zabezpieczenie podstawowe: Włączenie ról i obowiązków w zakresie bezpieczeństwa i ochrony prywatności do opisów stanowisk organizacyjnych.

Omówienie: Wyszczególnienie ról związanych z bezpieczeństwem i ochroną prywatności w opisach poszczególnych stanowisk organizacyjnych ułatwia zrozumienie obowiązków w zakresie bezpieczeństwa i ochrony prywatności związanych z tymi rolami oraz wymogów dotyczących szkoleń w zakresie bezpieczeństwa i ochrony prywatności odnoszących się do tych ról.

Zabezpieczenia powiązane: Brak.

Zabezpieczenia rozszerzone: Brak.

KATEGORIA PT - PRZEJRZYSTOŚĆ PRZETWARZANIA DANYCH OSOBOWYCH

PT-1 POLITYKA I PROCEDURY

Zabezpieczenie podstawowe:

a. Opracowywanie, dokumentowanie i rozpowszechnianie wśród [Realizacja: *personel lub role określone przez organizację*]:

   1. [*Wybór (jeden lub więcej): poziom organizacji; poziom misji/procesu biznesowego; poziom systemu*] polityki przejrzystości przetwarzania danych osobowych, która:

      (a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami; oraz

      (b) Jest zgodna z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi; oraz

   2. Procedur ułatwiających wdrożenie polityki przejrzystości przetwarzania danych osobowych oraz powiązanych zabezpieczeń przejrzystości przetwarzania danych osobowych;

b. Wyznaczanie [Realizacja: *osoba wyznaczona przez organizację*] do zarządzania rozwojem, dokumentacją i rozpowszechnianiem polityki i procedur przejrzystości przetwarzania danych osobowych; oraz

c. Przeglądanie i aktualizacja bieżącej:

   1. Polityki przejrzystości przetwarzania danych osobowych z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*]; oraz

   2. Procedur przejrzystości przetwarzania danych osobowych z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*].

Omówienie: Polityka i procedury w zakresie przejrzystości przetwarzania danych osobowych dotyczą zabezpieczeń w kategorii *Przejrzystość przetwarzania danych osobowych* (PT), które są wdrażane w ramach systemów i organizacji. Strategia zarządzania ryzykiem jest ważnym czynnikiem przy tworzeniu takich polityk i procedur. Polityki i procedury przyczyniają się do zapewnienia bezpieczeństwa i ochrony prywatności. Dlatego ważne jest, aby programy bezpieczeństwa i ochrony prywatności były opracowywane wspólnie przy kształtowaniu polityki i procedur przejrzystości przetwarzania danych osobowych. Polityki i procedury dotyczące programów bezpieczeństwa i ochrony prywatności na poziomie organizacji są ogólnie rzecz biorąc preferowane i mogą eliminować potrzeby tworzenia polityk i procedur specyficznych dla danej misji lub systemu. Polityka może być włączona, jako część ogólnej polityki bezpieczeństwa i ochrony prywatności lub reprezentowana przez wiele polityk odzwierciedlających złożony charakter organizacji. Procedury mogą być ustanowione dla programów bezpieczeństwa i ochrony prywatności, dla misji lub procesów biznesowych oraz dla systemów, jeśli to konieczne. Procedury opisują sposób wdrażania zasad lub zabezpieczeń i mogą być skierowane do osoby lub roli, która jest przedmiotem procedury. Procedury mogą być udokumentowane w planach bezpieczeństwa i ochrony prywatności systemu w jednym lub kilku oddzielnych dokumentach.

Zdarzenia, które mogą spowodować konieczność aktualizacji polityki i procedur przejrzystości przetwarzania danych osobowych, obejmują wyniki oceny lub audytu, incydenty lub naruszenia bezpieczeństwa, lub zmiany w przepisach prawa, zarządzeniach, dyrektywach, rozporządzeniach, zasadach, standardach i wytycznych.

Oświadczenie o wprowadzeniu zabezpieczeń nie jest równoznaczne z ustanowieniem polityki lub procedury organizacyjnej.

Zabezpieczenia powiązane: Brak.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130].

PT 2 UPRAWNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Zabezpieczenie podstawowe:

a. Określenie i udokumentowanie [*Realizacja: organ zdefiniowany przez organizację*], który zezwala na [*Realizacja: przetwarzanie zdefiniowane przez organizację*] informacji umożliwiających identyfikację osób; oraz

b. Ograniczenie [*Realizacja: zdefiniowane przez organizację przetwarzanie*] informacji umożliwiających identyfikację osób do tych, które są autoryzowane.

Omówienie: Przetwarzanie informacji umożliwiających identyfikację osób jest operacją lub zestawem operacji, które system informatyczny lub organizacja wykonuje w odniesieniu do informacji umożliwiających identyfikację osób w całym cyklu życia informacji. Przetwarzanie obejmuje, ale nie ogranicza się do tworzenia, gromadzenia, wykorzystywania, przetwarzania, przechowywania, obsługi, rozpowszechniania, ujawniania i usuwania. Operacje przetwarzania obejmują również logowanie, generowanie i przekształcanie, jak również techniki analizy, takie jak eksploracja danych.

Organizacje podlegają stosownym przepisom prawa, przepisom wykonawczym, dyrektywom, rozporządzeniom lub zasadom, które ustanawiają uprawnienia organizacji i tym samym ograniczają niektóre rodzaje przetwarzania danych osobowych lub ustanawiają określone wymagania związane z przetwarzaniem. Personel organizacji konsultuje się z SAOP[82] i radcą prawnym w sprawie takich uprawnień, szczególnie jeśli organizacja podlega wielu jurysdykcjom lub źródłom uprawnień. W przypadku organizacji, których przetwarzanie nie jest określone zgodnie z przepisami prawa, zasady i ustalenia organizacji regulują sposób, w jaki przetwarzają one informacje osobowe, które można zidentyfikować. Podczas gdy przetwarzanie informacji umożliwiających identyfikację osób może być prawnie

[82] Patrz: NSC 800-37; NSC 7298.

dopuszczalne, nadal może pojawić się ryzyko naruszenia prywatności. Ocena ryzyka związanego z ochroną prywatności może zidentyfikować zagrożenia dla prywatności związane z autoryzowanym przetwarzaniem informacji umożliwiających identyfikację osób oraz wspierać rozwiązania służące zarządzaniu takimi zagrożeniami.

Organizacje biorą pod uwagę obowiązujące wymogi i polityki organizacyjne, aby określić, jak udokumentować to uprawnienie. Uprawnienia do przetwarzania informacji umożliwiających identyfikację osób są udokumentowane w politykach i zawiadomieniach dotyczących prywatności, zawiadomieniach o systemie rejestrów, ocenach wpływu na prywatność, oświadczeniach, umowach i zawiadomieniach dotyczących kojarzenia danych za pomocą systemów komputerowych, kontraktach, umowach o wymianie informacji, protokołach ustaleń i innych dokumentach.

Organizacje podejmują działania mające na celu zapewnienie, że dane osobowe są przetwarzane wyłącznie w dozwolonych celach, szkoląc personel organizacyjny w zakresie dozwolonego przetwarzania danych osobowych oraz monitorują i kontrolują organizacyjne wykorzystanie danych osobowych.

Zabezpieczenia powiązane: AC-2, AC-3, CM-13, IR-9, PM-9, PM-24, PT-1, PT-3, PT-5, PT-6, RA-3, RA-8, SI-12, SI-18.

Zabezpieczenia rozszerzone:

(1) UPRAWNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH | OZNACZANIE DANYCH

Dołączanie znaczników (tagów) danych zawierających [*Realizacja: określone przez organizację autoryzowane przetwarzanie*] do [*Realizacja: zdefiniowane przez organizację elementy informacji umożliwiające identyfikację osoby*].

Omówienie: Tagi danych wspierają śledzenie i egzekwowanie autoryzowanego przetwarzania poprzez przekazywanie w całym systemie typów przetwarzania, które są autoryzowane wraz z odpowiednimi elementami danych osobowych.

Znaczniki danych mogą również wspomagać korzystanie ze zautomatyzowanych narzędzi.

Zabezpieczenia powiązane: AC-16, CA-6, CM-12, PM-5, PM-22, PT-4, SC-16, SC-43, SI-10, SI-15, SI-19.

(2) UPRAWNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH | AUTOMATYZACJA

Zarządzanie egzekwowaniem upoważnień do przetwarzania danych osobowych przy użyciu [***Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację***]**.**

Omówienie: Zautomatyzowane mechanizmy wspomagają weryfikowanie, czy ma miejsce wyłącznie autoryzowane przetwarzanie danych.

Zabezpieczenia powiązane: CA-6, CM-12, PM-5, PM-22, PT-4, SC-16, SC-43, SI-10, SI-15, SI-19.

Referencje: [PRIVACT], [0MB A-130], [IR 8112].

PT-3 CELE PRZETWARZANIA DANYCH OSOBOWYCH

Zabezpieczenie podstawowe:

a. Zidentyfikowanie i udokumentowanie celi przetwarzania danych osobowych [*Realizacja: cele zdefiniowane przez organizację*];

b. Opisanie celów przetwarzania danych osobowych w publicznie dostępnej informacji o prywatności i polityce organizacji;

c. Ograniczenie [*Realizacja: przetwarzane informacje zdefiniowane przez organizację*] umożliwiających identyfikację osoby tylko do tych, które są zgodne ze zidentyfikowanymi celami; oraz

d. Monitorowanie zmian w przetwarzaniu danych osobowych i wdrożenie [*Realizacja: mechanizmy określone przez organizację*] *w* celu zapewnienia, że wszelkie zmiany są dokonywane zgodnie z [*Realizacja: wymagania określone przez organizację*].

Omówienie: Określenie i udokumentowanie celu przetwarzania zapewnia organizacjom wiedzę o tym, co może być powodem przetwarzania informacji umożliwiających identyfikację osób. Termin " przetwarzanie danych osobowych" obejmuje każdy etap cyklu życia informacji, w tym tworzenie, gromadzenie, wykorzystywanie, przetwarzanie, przechowywanie, utrzymywanie, rozpowszechnianie, ujawnianie i usuwanie. Określenie i udokumentowanie celu przetwarzania jest warunkiem wstępnym umożliwiającym właścicielom i operatorom systemu oraz osobom, których informacje są przetwarzane przez system, zrozumienie, w jaki sposób informacje te będą przetwarzane. Umożliwia to osobom podejmowanie świadomych decyzji dotyczących sposobu korzystania z systemów informatycznych i organizacji oraz zarządzanie swoimi interesami związanymi z prywatnością. Po zidentyfikowaniu konkretnego celu przetwarzania, cel ten jest opisany w informacjach o ochronie prywatności, politykach organizacji i wszelkiej powiązanej dokumentacji dotyczącej zgodności z zasadami ochrony prywatności, w tym w ocenach wpływu na prywatność, informacjach o systemie ewidencji,

oświadczeniach o ochronie prywatności, informacjach o kojarzeniu danych komputerowych i innych stosownych informacjach.

Organizacje podejmują kroki mające na celu zapewnienie, że informacje umożliwiające identyfikację osób są przetwarzane wyłącznie w określonych celach, w tym szkolą personel organizacyjny oraz monitorują i kontrolują przetwarzanie informacji umożliwiających identyfikację osób przez organizacje.

Organizacje monitorują zmiany w przetwarzaniu danych osobowych. Personel organizacji konsultuje się z SAOP[83] i radcą prawnym w celu zapewnienia, że wszelkie nowe cele wynikające ze zmian w przetwarzaniu danych są zgodne z celem, dla którego informacje zostały zebrane, lub jeśli nowy cel nie jest zgodny, wdrażają mechanizmy zgodnie z określonymi wymogami, aby umożliwić nowe przetwarzanie, jeśli jest to właściwe. Mechanizmy mogą obejmować uzyskanie zgody od osób, zmianę polityki prywatności lub inne środki służące zarządzaniu ryzykiem w zakresie prywatności wynikającym ze zmian w celach przetwarzania danych osobowych.

Zabezpieczenia powiązane: AC-2, AC-3, AT-3, CM-13, IR-9, PM-9, PM-25, PT-2, PT-5, PT-6, PT-7, RA-8, SC- 43, SI-12, SI-18.

Zabezpieczenia rozszerzone:

(1) CELE PRZETWARZANIA DANYCH OSOBOWYCH | OZNACZANIE DANYCH

Dołączanie do [***Realizacja: zdefiniowane przez organizację elementy informacji umożliwiających identyfikację osoby***] **znaczników danych zawierających następujące cele*:*** [***Realizacja: zdefiniowane przez organizację cele przetwarzania***]***.***

Omówienie: Znaczniki danych wspierają śledzenie celów przetwarzania danych poprzez przekazywanie celów wraz z odpowiednimi elementami informacji umożliwiających identyfikację osób w całym systemie. Dzięki przekazywaniu

[83] Patrz: NSC 800-37; NSC 7298.

celów przetwarzania w znaczniku danych wraz z informacjami umożliwiającymi identyfikację osoby w miarę jak informacje przechodzą przez system, właściciel lub operator systemu może określić, czy zmiana w przetwarzaniu byłaby zgodna ze zidentyfikowanymi i udokumentowanymi celami. Znaczniki danych mogą również wspomagać korzystanie ze zautomatyzowanych narzędzi.

Zabezpieczenia powiązane: CA-6, CM-12, PM-5, PM-22, SC-16, SC-43, SI-10, SI-15, SI-19.

(2) CELE PRZETWARZANIA DANYCH OSOBOWYCH | AUTOMATYZACJA

Śledzenie celów przetwarzania danych osobowych przy użyciu [***Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację***]**.**

Omówienie: Zautomatyzowane mechanizmy zwiększające możliwość śledzenia celów przetwarzania.

Zabezpieczenia powiązane: CA-6, CM-12, PM-5, PM-22, SC-16, SC-43, SI-10, SI-15, SI-19.

Referencje: [PRIVACT], [0MB A-130, załącznik II], [IR 8112].

PT-4 ZGODY

Zabezpieczenie podstawowe: Wdrożenie [*Realizacja: zdefiniowane przez organizację narzędzia lub mechanizmy ułatwiające osobom podejmowanie świadomych decyzji*] pozwalające osobom fizycznym na wyrażanie zgody na przetwarzanie ich danych osobowych przed ich zebraniem.

Omówienie: Możliwość wyrażania zgody pozwala osobom uczestniczyć w podejmowaniu decyzji dotyczących przetwarzania ich danych osobowych i przenosi część ryzyka, które wynika z przetwarzania tych danych z organizacji na daną osobę. Zgoda może być wymagana przez obowiązujące prawo, zarządzenia, dyrektywy, regulacje, zasady, standardy lub wytyczne. W przeciwnym razie, wybierając zgodę jako środek zabezpieczenia, organizacje rozważają, czy można racjonalnie oczekiwać, że osoby zrozumieją i zaakceptują ryzyko związane z ochroną prywatności, które wynika z udzielonej przez nie zgody. Organizacje rozważają, czy inne zabezpieczenia mogą skuteczniej ograniczyć ryzyko związane z prywatnością, samodzielnie lub w połączeniu z udzieleniem zgody. Organizacje biorą również pod uwagę wszelkie czynniki demograficzne lub kontekstowe, które mogą mieć wpływ na zrozumienie lub zachowanie osób w odniesieniu do przetwarzania danych prowadzonego przez system lub organizację. Zwracając się o zgodę do osób, organizacje rozważają odpowiedni mechanizm uzyskiwania zgody, w tym rodzaj zgody (np. opt-in, opt-out), sposób właściwego uwierzytelniania i potwierdzania tożsamości osób oraz sposób uzyskiwania zgody drogą elektroniczną. Ponadto organizacje, w stosownych przypadkach, rozważają stworzenie mechanizmu umożliwiającego osobom wycofanie zgody po jej udzieleniu. Ostatecznie, organizacje biorą pod uwagę czynniki użyteczności, aby pomóc osobom zrozumieć ryzyko akceptowane przy udzielaniu zgody, w tym użycie prostego języka i unikanie technicznego żargonu.

Zabezpieczenia powiązane: AC-16, PKT-2, PT-5.

Zabezpieczenia rozszerzone:

(1) ZGODY | ZGODA NA PODSTAWIE ART. 6 UST. 1 RODO

Dostarczanie [***Realizacja: mechanizmy zdefiniowane przez organizację***] **umożliwiających osobom dostosowanie uprawnień do przetwarzania wybranych elementów danych osobowych.**

Omówienie: Podczas gdy jedne przetwarzanie danych osobowych może być niezbędne dla podstawowej funkcjonalności produktu lub usługi, inne przetwarzanie może nie być uzasadnione. W takich okolicznościach organizacje umożliwiają osobom wybór sposobu przetwarzania określonych elementów danych osobowych. Bardziej dostosowana zgoda może pomóc w zmniejszeniu ryzyka związanego z prywatnością, zwiększyć zadowolenie użytkowników i zapobiec niepożądanym zachowaniom, takim jak rezygnacja z produktu lub usługi.

Zabezpieczenia powiązane: PT-2.

(2) ZGODY | ZGODA TYPU „JUST-IN TIME”

Prezentowanie [***Realizacja: zdefiniowane przez organizację mechanizmy zgody***] **osobom z [Realizacja: zdefiniowana przez organizację częstotliwość] i w połączeniu z [*Realizacja*: *zdefiniowane przez organizację przetwarzanie danych osobowych*].**

Omówienie: Zgoda typu „Just-in-time” umożliwia osobom udział w przetwarzaniu ich danych osobowych w danym momencie lub w związku z określonymi rodzajami przetwarzania danych, gdy udział ten może być najbardziej przydatny dla danej osoby. Indywidualne założenia dotyczące sposobu przetwarzania danych osobowych mogą nie być dokładne lub wiarygodne, jeżeli od ostatniej wyrażonej przez daną osobę zgody upłynęło dużo czasu lub rodzaj przetwarzania stwarza znaczne zagrożenie dla prywatności. Organizacje decydują według własnego uznania, kiedy stosować zgodę "just-in-time", i mogą korzystać z

informacji uzupełniających dotyczących danych demograficznych, grup dyskusyjnych lub ankiet, aby dowiedzieć się więcej o zainteresowaniach i obawach osób na temat ochrony prywatności.

Zabezpieczenia powiązane: PT-2.

(3) ZGODY | WYCOFANIE ZGODY

Wdrożenie [***Realizacja: narzędzia lub mechanizmy określone przez organizację***] **umożliwiające osobom wycofanie zgody na przetwarzanie ich danych osobowych.**

Omówienie: Odwołanie zgody umożliwia osobom sprawowanie kontroli nad swoją pierwotną decyzją o wyrażeniu zgody w przypadku zmiany okoliczności. Organizacje biorą pod uwagę aspekty użyteczności, umożliwiając łatwe w użyciu funkcje cofnięcia zgody..

Zabezpieczenia powiązane: PT-2.

Referencje: [PRIVACT], [0MB A-130], [SP. 800-63-3].

PT-5 INFORMACJA O OCHRONIE PRYWATNOŚCI

Zabezpieczenie podstawowe: Dostarczanie osobie powiadomienia o przetwarzaniu danych osobowych, które:

a. Jest dostępne dla osób po pierwszym kontakcie z organizacją, a następnie *[Realizacja: częstotliwość określona przez organizację];*

b. Jest jasne i łatwe do zrozumienia, przedstawia informacje o przetwarzaniu danych osobowych w prostym języku;

c. Określa organ, który upoważnia do przetwarzania danych osobowych;

d. Określa cele, dla których dane osobowe mają być przetwarzane; oraz

e. Obejmuje [*Realizacja: informacje określone przez organizację*].

Omówienie: Informacje o ochronie prywatności pomagają w informowaniu osób o tym, jak ich dane osobowe są przetwarzane przez system lub organizację. Organizacje wykorzystują informacje o ochronie prywatności do informowania osób o tym, w jaki sposób, na podstawie jakich uprawnień i w jakim celu ich dane osobowe są przetwarzane, a także inne informacje, takie jak przysługujące osobom możliwości wyboru w odniesieniu do tego przetwarzania i innych stron, którym informacje są udostępniane. Przepisy prawne, zarządzenia, dyrektywy, rozporządzenia lub zasady mogą wymagać, aby noty o ochronie prywatności zawierały określone elementy lub były dostarczane w określonych formatach. Personel organizacji konsultuje się z SAOP[84] i radcą prawnym w sprawie terminu i sposobu przekazania informacji o ochronie prywatności, a także elementów, które należy uwzględnić w informacjach o ochronie prywatności i wymaganych formatach. W okolicznościach, w których obowiązujące prawo lub zasady nie wymagają podawania informacji o ochronie prywatności, zasady i ustalenia organizacyjne mogą wymagać prezentowania

[84] Patrz: NSC 800-37; NSC 7298.

informacji o ochronie prywatności i mogą służyć jako źródło elementów, które należy uwzględnić w informacjach o ochronie prywatności.

Oceny ryzyka w zakresie ochrony prywatności identyfikują zagrożenia dla prywatności związane z przetwarzaniem danych osobowych i mogą pomóc organizacjom w określeniu odpowiednich elementów, które należy uwzględnić w informacji o ochronie prywatności, aby zarządzać takim ryzykiem. Aby pomóc osobom fizycznym zrozumieć, jak przetwarzane są ich informacje, organizacje piszą materiały prostym językiem i unikają technicznego żargonu.

Zabezpieczenia powiązane: PM-20, PM-22, PT-2, PT-3, PT-4, PT-7, RA-3, SI-18.

Zabezpieczenia rozszerzone:

(1) INFORMACJA O OCHRONIE PRYWATNOŚCI | INFORMACJA NA ŻĄDANIE

Przedstawianie osobom powiadomień o przetwarzaniu danych osobowych w czasie i miejscu, w którym osoba udostępnia informacje umożliwiające identyfikację, lub prowadzonych działaniach na danych, lub [***Realizacja: częstotliwość określona przez organizację***]**.**

Omówienie: Powiadomienia "just-in-time" informują osoby o tym, jak organizacje przetwarzają ich dane osobowe w czasie, gdy takie powiadomienia mogą być dla nich najbardziej użyteczne. Indywidualne założenia dotyczące sposobu przetwarzania danych osobowych mogą być niedokładne lub niewiarygodne, jeżeli upłynął czas od ostatniego przedstawienia zawiadomienia przez organizację lub jeżeli zmieniły się okoliczności, w których dana osoba została ostatnio powiadomiona. Powiadomienia Just-in-time informują osoby o tym, jak organizacje przetwarzają ich dane osobowe w sytuacji, gdy takie powiadomienia mogą być najbardziej przydatne dla tych osób. Indywidualne założenia dotyczące sposobu przetwarzania danych osobowych mogą nie być dokładne lub wiarygodne, jeśli upłynął czas od ostatniego powiadomienia przez organizację lub zmieniły się okoliczności, w których dana osoba została ostatnio powiadomiona. Powiadomienie "just-in-time" może wyjaśniać działania dotyczące danych, które

organizacje zidentyfikowały jako potencjalnie powodujące większe zagrożenie dla prywatności osób. Organizacje mogą wykorzystywać powiadomienia just-in-time do aktualizowania lub przypominania osobom o konkretnych działaniach na danych w miarę ich występowania lub podkreślania konkretnych zmian, które zaszły od ostatniego powiadomienia. Powiadomienie just-in-time może być stosowane w połączeniu ze zgodą just-in-time, aby wyjaśnić, co się stanie, jeśli zgoda zostanie odrzucona. Organizacje mają swobodę w określaniu, kiedy należy stosować powiadomienia "just-in-time" i mogą korzystać z informacji pomocniczych dotyczących danych demograficznych użytkowników, grup dyskusyjnych lub ankiet, aby poznać zainteresowania i obawy użytkowników dotyczące prywatności.

Zabezpieczenia powiązane: PM-21.

(2) INFORMACJA O OCHRONIE PRYWATNOŚCI | OŚWIADCZENIE O OCHRONIE PRYWATNOŚCI

Zamieszczanie oświadczeń zgodnych z Ustawą RODO na formularzach zbierających informacje, które będą przechowywane w systemie rejestrów zgodnych z tą Ustawą, lub dostarczenie oświadczeń zgodnych z Ustawą RODO na oddzielnych formularzach, które mogą być przechowywane przez osoby.

Omówienie: Jeżeli organizacja zwróci się do osoby o dostarczenie informacji, które staną się częścią systemu rejestrów, jest ona zobowiązana do dostarczenia oświadczenia o ochronie danych na formularzu używanym do zbierania informacji lub na oddzielnym formularzu, który może być zachowany przez daną osobę. W takich okolicznościach organizacja dostarcza oświadczenie o ochronie danych, niezależnie od tego, czy informacje będą zbierane w formie papierowej, elektronicznej, na stronie internetowej, w aplikacji mobilnej, telefonicznie, czy za pośrednictwem innego medium. Wymóg ten zapewnia, że osoba uzyska wystarczające informacje na temat wniosku o udzielenie informacji, aby mogła podjąć świadomą decyzję, czy udzielić odpowiedzi, czy też nie.

Oświadczenia zapewniają formalne powiadomienie osób o organie, który upoważnia do uzyskania informacji; o tym, czy podanie informacji jest obowiązkowe czy dobrowolne; o głównym celu lub głównych celach, do których informacje mają być wykorzystane; o opublikowanych rutynowych sposobach wykorzystania informacji; o skutkach, jakie dla danej osoby może mieć ewentualne niepodanie wszystkich lub części żądanych informacji; oraz o właściwym odwołaniu i linku do odpowiedniego zawiadomienia o systemie rejestrów. Personel organizacji konsultuje się z SAOP i z radcą prawnym w sprawie przepisów dotyczących zawiadomień zawartych w oświadczeniu.

Zabezpieczenia powiązane: PT-6.

Zabezpieczenia rozszerzone: Brak.

Referencje: [PRIVACT], [0MB A-130], [0MB A-108].

PT-6 SYSTEM ZAWIADOMIEŃ O REJESTRACH

Zabezpieczenie podstawowe: W przypadku systemów przetwarzających informacje, które będą przechowywane w systemie rejestrów:

a. Sporządzanie zawiadomień o systemie rejestrów zgodnie z przepisami prawa oraz przedkładanie nowych i znacząco zmodyfikowanych zawiadomień o systemie rejestrów odpowiednim komisjom organizacyjnym celu dokonania wcześniejszego przeglądu;

b. Publikowanie informacji o systemie rejestrów; oraz

c. Utrzymywanie dokładności, aktualności i zakresu informacji o systemie rejestrów zgodnie z polityką.

Omówienie:[85] [PRIVACT] wymaga, aby agencje federalne publikowały w Rejestrze Federalnym zawiadomienie dotyczące systemu rejestrów z chwilą ustanowienia lub zmiany systemu rejestrów [PRIVACT]. Ogólnie rzecz biorąc, zawiadomienie o systemie rejestrów jest wymagane, gdy agencja prowadzi grupę dowolnych rejestrów, z których informacje są wyszukiwane na podstawie nazwiska osoby lub na podstawie numeru identyfikacyjnego, symbolu lub innego identyfikatora. Powiadomienie opisuje pochodzenie i specyfikę systemu oraz identyfikuje system rejestrów, cel(e) systemu, upoważnienie do prowadzenia rejestrów, kategorie rejestrów prowadzonych w systemie, kategorie osób, których dotyczą prowadzone rejestry, standardowe sposoby wykorzystania, którym podlegają rejestry, oraz dodatkowe szczegóły dotyczące systemu opisane w [OMB A-108].

Zabezpieczenia powiązane: AC-3, PM-20, PT-2, PT-5.

Zabezpieczenia rozszerzone:

(1) SYSTEM ZAWIADOMIEŃ O REJESTRACH | RUTYNOWE ZASTOSOWANIA

[85] Omówienie dotyczy rynku USA.

Przeglądanie wszystkich rutynowych zastosowań opublikowanych w zawiadomieniu o systemie rejestrów z [***Realizacja: częstotliwość określona przez organizację***] **w celu zapewnienia nieprzerwanej zgodności z celem, dla którego informacja została zebrana.**

Omówienie: Rutynowe wykorzystanie [PRIVACT] jest szczególnym rodzajem ujawnienia zapisu poza agencją federalną prowadzącą system zapisów. Rutynowe wykorzystanie jest wyjątkiem od zakazu [PRIVACT] dotyczącego ujawniania zapisu w systemie rejestrów bez uprzedniej pisemnej zgody osoby, której zapis dotyczy. Aby zakwalifikować ujawnienie jako rutynowe wykorzystanie, musi ono nastąpić w związku z celem, który jest zgodny z powodem, dla którego informacje zostały pierwotnie zgromadzone. [PRIVACT] wymaga od agencji opisania każdego rutynowego wykorzystania zapisów przechowywanych w systemie rejestrów, w tym kategorii użytkowników tych zapisów i celu ich wykorzystania. Agencje mogą ustanowić rutynowe zastosowania wyłącznie poprzez wyraźne opublikowanie ich w stosownym obwieszczeniu odnoszącym się do systemu rejestrów.

Zabezpieczenia powiązane: Brak.

(2) SYSTEM ZAWIADOMIEŃ O REJESTRACH | ZASADY WYŁĄCZENIA

Przeglądanie wszystkich zwolnień z ustawy o ochronie danych zgłoszonych do systemu rejestrów [Realizacja: ***częstotliwość określona przez organizację*****] w celu zapewnienia, że pozostają one właściwe i niezbędne zgodnie z prawem, że zostały ogłoszone jako przepisy i że są dokładnie opisane w systemie zgłaszania rejestrów.**

Omówienie: [PRIVACT] zawiera dwa zestawy przepisów, które umożliwiają agencjom federalnym ubieganie się o zwolnienie z niektórych wymogów zawartych w ustawie. W pewnych okolicznościach przepisy te pozwalają agencjom na promulgowanie rozporządzeń w celu zwolnienia systemu rejestrów z wybranych przepisów [PRIVACT]. Rozporządzenia w sprawie wyłączeń

organizacji z [PRIVACT] zawierają, co najmniej konkretną nazwę(-y) systemu(-ów) dokumentacji, który(-e) zostanie(-ą) wyłączony(-e), szczegółowe przepisy [PRIVACT], z których system(-y) dokumentacji ma(-ją) zostać wyłączony(-e), przyczyny wyłączenia oraz wyjaśnienie, dlaczego wyłączenie jest zarówno konieczne, jak i właściwe.

Zabezpieczenia powiązane: Brak.

Referencje: [PRIVACT], [OMB A-108].

PT-7 SZCZEGÓŁOWE KATEGORIE DANYCH OSOBOWYCH

Zabezpieczenie podstawowe: Zastosowanie [*Realizacja: warunki przetwarzania określone przez organizację*] dla określonych kategorii informacji umożliwiających identyfikację osób.

Omówienie: Organizacje stosują wszelkie warunki lub zabezpieczenia, które mogą być niezbędne dla określonych kategorii danych osobowych. Warunki te mogą być wymagane przez prawo, zarządzenia, dyrektywy, rozporządzenia, zasady, standardy lub wytyczne. Wymagania te mogą również wynikać z wyników oceny ryzyka związanego z ochroną prywatności, która jest czynnikiem zmian kontekstowych mogących prowadzić do ustalenia przez organizację, że dana kategoria informacji umożliwiających identyfikację osoby jest szczególnie wrażliwa lub stwarza szczególne ryzyko dla prywatności. Organizacje konsultują się z SAOP[86] i radcą prawnym w sprawie wszelkich niezbędnych zabezpieczeń.

Zabezpieczenia powiązane: IR-9, PT-2, PT-3, RA-3.

Zabezpieczenia rozszerzone:

(1) SZCZEGÓŁOWE KATEGORIE DANYCH OSOBOWYCH | IDENTYFIKATOR OSOBY - NP. NUMER PESEL

Przy przetwarzaniu przez system numerów identyfikatorów osobowych należy:

(a) Wyeliminować zbędne gromadzenie, utrzymywanie i wykorzystywanie identyfikatorów osobowych oraz zbadać alternatywy dla ich wykorzystywania jako identyfikatorów osobowych;

b) Nie odmawiać żadnej osobie jakichkolwiek praw, korzyści lub przywilejów przewidzianych prawem z powodu odmowy ujawnienia numeru identyfikacji osobistej przez tę osobę; oraz

[86] Patrz: NSC 800-37; NSC 7298.

(c) Informowania każdej osoby, która jest proszona o ujawnienie swojego identyfikatora osobowego o tym, czy ujawnienie to jest obowiązkowe czy dobrowolne, na podstawie jakich przepisów ustawowych lub innych uprawnień taki identyfikator jest wymagany i w jaki sposób będzie wykorzystywany.

Omówienie: Prawo ustanawia szczególne wymagania dotyczące przetwarzania przez organizacje identyfikatorów osobistych. Organizacje podejmują działania w celu wyeliminowania niepotrzebnego wykorzystywania identyfikatorów osobistych i innych wrażliwych informacji oraz przestrzegają wszelkich szczególnych wymagań, które mają zastosowanie.

Zabezpieczenia powiązane: IA-4.

(2) SZCZEGÓŁOWE KATEGORIE DANYCH OSOBOWYCH | PRZETWARZANIE WRAŻLIWYCH DANYCH OSOBOWYCH[87]

Zakazanie przetwarzania informacji opisujących, w jaki sposób dana osoba wykonuje prawa gwarantowane przez Pierwszą Poprawkę, chyba że jest to wyraźnie dozwolone przez ustawę lub przez osobę, lub jeśli nie jest to istotne dla i w zakresie dozwolonej działalności organów ścigania.

Omówienie: [PRIVACT] ogranicza zdolność agencji do przetwarzania informacji, które opisują sposób, w jaki osoby korzystają z praw gwarantowanych przez pierwszą poprawkę. Organizacje konsultują te wymogi z SAOP i radcą prawnym.

Zabezpieczenia powiązane: Brak.

Referencje: [PRIVACT], [OMB A-130], [OMB A-108], [NARA CUI].

[87] Zabezpieczenie dotyczy regulacji prawnych obowiązujących w USA.

PT-8 WYMAGANIA DOTYCZĄCE ZGODNOŚCI PRZY PRZETWARZANIU KOMPUTEROWOWYM[88]

Zabezpieczenie podstawowe: System lub organizacja przetwarza informacje w celu przeprowadzenia programu dopasowania po:

a. Uzyskaniu zgody komisji ds. integralności danych na przeprowadzenie programu dopasowywania;

b. Opracowaniu i zawarciu umowy o porównywaniu danych komputerowych;

c. Opublikowaniu zawiadomienia o przeprowadzeniu programu dopasowania;

d. Niezależnym sprawdzeniu informacji uzyskanych przez program dopasowujący przed podjęciem negatywnych działań wobec danej osoby, jeżeli jest to wymagane; oraz

e. Dostarczeniu osobie zawiadomienia i umożliwienie jej zakwestionowania ustaleń przed podjęciem niekorzystnych działań wobec danej osoby.

Omówienie: [PRIVACT] ustanawia wymagania dla agencji federalnych i niefederalnych, jeśli zangażowane są one w odpowiedni program. Ogólnie rzecz biorąc, program dopasowujący to skomputeryzowane porównanie zapisów z dwóch lub więcej zautomatyzowanych systemów zapisów [PRIVACT] lub zautomatyzowanego systemu zapisów i zapisów prowadzonych przez agencję niefederalną (lub jej agenta). Program dopasowujący odnosi się albo do programów świadczeń federalnych, albo do zapisów dotyczących personelu federalnego, albo do zapisów dotyczących płac. Program dopasowywania świadczeń federalnych jest przeprowadzany w celu ustalenia lub weryfikacji uprawnień do płatności w ramach programów świadczeń federalnych lub w celu odzyskania płatności lub zaległych długów w ramach programów świadczeń federalnych. Program dopasowujący

[88] Zabezpieczenie dotyczy regulacji prawnych obowiązujących w USA.

obejmuje nie tylko samą działalność dopasowującą, ale również działania dochodzeniowe i działania końcowe, jeśli takie istnieją.

Zabezpieczenia powiązane: PM-24.

Zabezpieczenia rozszerzone: Brak.

Referencje: [PRIVACT], [OMB A-130], [0MB A-108], [CMPPA].

KATEGORIA RA – OCENA RYZYKA

RA-1 POLITYKA I PROCEDURY

Zabezpieczenie podstawowe:

a. Opracowywanie, dokumentowanie i rozpowszechnianie wśród [Realizacja: *personel lub role określone przez organizację*]:

   1. [*Wybór (jeden lub więcej): poziom organizacji; poziom misji/procesu biznesowego; poziom systemu*] polityki oceny ryzyka, która:

      (a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami; oraz

      (b) Jest zgodna z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi; oraz

   2. Procedur ułatwiających wdrożenie polityki oceny ryzyka oraz powiązanych zabezpieczeń w zakresie oceny ryzyka;

b. Wyznaczanie [Realizacja: *osoba wyznaczona przez organizację*] do zarządzania rozwojem, dokumentacją i rozpowszechnianiem polityki i procedur oceny ryzyka; oraz

c. Przeglądanie i aktualizacja bieżącej:

   1. Polityki oceny ryzyka z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*]; oraz

   2. Procedur oceny ryzyka z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*].

Omówienie: Polityka i procedury w zakresie oceny ryzyka dotyczą zabezpieczeń w kategorii *Ocena ryzyka* (RA), które są wdrażane w ramach systemów i organizacji. Strategia zarządzania ryzykiem jest ważnym czynnikiem przy tworzeniu takich polityk i procedur. Polityki i procedury przyczyniają się do zapewnienia bezpieczeństwa

i ochrony prywatności. Dlatego ważne jest, aby programy bezpieczeństwa i ochrony prywatności były opracowywane wspólnie przy kształtowaniu polityki i procedur oceny ryzyka. Polityki i procedury dotyczące programów bezpieczeństwa i ochrony prywatności na poziomie organizacji są ogólnie rzecz biorąc preferowane i mogą eliminować potrzeby tworzenia polityk i procedur specyficznych dla danej misji lub systemu. Polityka może być włączona, jako część ogólnej polityki bezpieczeństwa i ochrony prywatności lub reprezentowana przez wiele polityk odzwierciedlających złożony charakter organizacji. Procedury mogą być ustanowione dla programów bezpieczeństwa i ochrony prywatności, dla misji lub procesów biznesowych oraz dla systemów, jeśli to konieczne. Procedury opisują sposób wdrażania zasad lub zabezpieczeń i mogą być skierowane do osoby lub roli, która jest przedmiotem procedury. Procedury mogą być udokumentowane w planach bezpieczeństwa i ochrony prywatności systemu w jednym lub kilku oddzielnych dokumentach.

Zdarzenia, które mogą spowodować konieczność aktualizacji polityki i procedur oceny ryzyka, obejmują wyniki oceny lub audytu, incydenty lub naruszenia bezpieczeństwa, lub zmiany w przepisach prawa, zarządzeniach, dyrektywach, rozporządzeniach, zasadach, standardach i wytycznych.

Oświadczenie o wprowadzeniu zabezpieczeń nie jest równoznaczne z ustanowieniem polityki lub procedury organizacyjnej.

Zabezpieczenia powiązane: PM-9, PS-8, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [NIST SP 800-12], [NIST SP 800-30], [NIST SP 800-39], [NIST SP 800-100].

RA-2 KATEGORYZACJA BEZPIECZEŃSTWA

Zabezpieczenie podstawowe:

a. Klasyfikowanie systemu oraz przetwarzanych, przechowywanych i przekazywanych informacji;

b. Dokumentowanie wyników kategoryzacji bezpieczeństwa, w tym uzasadnienie, w planie bezpieczeństwa systemu; oraz

c. Zapewnienie, że osoba autoryzująca lub wyznaczony przez niego przedstawiciel sprawdza i zatwierdza decyzję o kategoryzacji bezpieczeństwa.

Omówienie: Kategorie bezpieczeństwa opisują potencjalny niekorzystny wpływ lub negatywne konsekwencje dla działalności organizacji, jej aktywów i osób, jeśli informacje i systemy organizacyjne zostaną narażone na kompromitację w wyniku utraty poufności, integralności lub dostępności. Kategoryzacja bezpieczeństwa jest również rodzajem charakterystyki utraty aktywów w procesach inżynierii bezpieczeństwa systemów, która jest przeprowadzana przez cały cykl życia systemu. Organizacje mogą korzystać z ocen ryzyka utraty prywatności lub ocen wpływu na prywatność, aby lepiej zrozumieć potencjalne negatywne skutki dla osób. NSC 199 zawiera dodatkowe wytyczne dotyczące kategoryzacji bezpieczeństwa krajowych systemów cyberbezpieczeństwa.

Organizacje przeprowadzają proces kategoryzacji bezpieczeństwa, jako działalność obejmującą całą organizację z bezpośrednim zaangażowaniem CIO, SAISO, SAOP, właścicieli systemów, właścicieli misji i biznesu oraz właścicieli lub władających informacją.[89] Organizacje rozważają potencjalne negatywne skutki dla innych organizacji oraz potencjalne negatywne skutki na poziomie krajowym.

Procesy kategoryzacji bezpieczeństwa ułatwiają opracowanie inwentaryzacji zasobów informatycznych oraz, wraz z zabezpieczeniem CM-8, mapowanie do

[89] Patrz: NSC 800-37; NSC 7298.

konkretnych komponentów systemu, w którym informacje są przetwarzane, przechowywane lub przekazywane. Proces kategoryzacji bezpieczeństwa jest weryfikowany przez cały cykl życia systemu, aby zapewnić, że kategorie bezpieczeństwa pozostają dokładne i istotne.

Zabezpieczenia powiązane: CM-8, MP-4, PL-2, PL-10, PL-11, PM-7, RA-3, RA-5, RA-7, RA-8, SA-8, SC-7, SC- 38, SI-12.

Zabezpieczenia rozszerzone:

(1) KATEGORYZACJA BEZPIECZEŃSTWA | PRIORYTETYZACJA POZIOMÓW WPŁYWU

Przeprowadzanie priorytetyzacji poziomu wpływu systemów organizacyjnych w celu uzyskania dodatkowej szczegółowości na poziomie wpływu systemu.

Omówienie: Organizacje stosują koncepcję "najwyższej wartości" (*ang. high-water mark - HWM*) w odniesieniu do każdego systemu sklasyfikowanego zgodnie z [FIPS 199], co skutkuje klasyfikacją systemów, jako systemy o niskim, umiarkowanym lub wysokim wpływie na zagrożenia. Organizacje, które potrzebują dodatkowej szczegółowości w oznaczeniach wpływu na system w celu podejmowania decyzji w oparciu o ryzyko, mogą podzielić systemy na podkategorie w początkowej kategoryzacji systemu. Na przykład, ustalenie priorytetów na poziomie wpływu w przypadku systemu o umiarkowanym wpływie może prowadzić do powstania trzech nowych podkategorii: systemy o niskim wpływie niskim, systemy o umiarkowanym wpływie umiarkowanym i systemy o wysokim wpływie umiarkowanym. Ustalanie priorytetów na poziomie wpływu i wynikające z tego podkategorie systemu dają organizacjom możliwość skoncentrowania inwestycji związanych z wyborem środków bezpieczeństwa i dostosowaniem zabezpieczeń bazowych w reakcji na zidentyfikowane ryzyko. Priorytety na poziomie wpływu mogą być również wykorzystywane do określenia tych systemów, które mogą mieć zwiększone zainteresowanie lub wartość dla przeciwników lub stanowić krytyczną stratę dla organizacji, czasami określaną jako aktywa o wysokiej wartości. W przypadku aktywów o tak wysokiej wartości,

organizacje mogą być bardziej skoncentrowane na złożoności, agregacji i wymianie informacji. Alternatywnie, organizacje mogą stosować wytyczne zawarte w [NSC 199] w zakresie kategoryzacji związanej z celami bezpieczeństwa.

Zabezpieczenia powiązane: Brak.

Referencje: [FIPS 199], [FIPS 200], [NIST SP 800-30], [NIST SP 800-37], [NIST SP 800-39], [NIST SP 800-60-1], [NIST SP 800- 60-2], [NIST SP 800-160-1], [CNSSI 1253], [NARA CUI].

RA-3 SZACOWANIE RYZYKA

Zabezpieczenie podstawowe:

a. Przeprowadzenie oceny ryzyka, w tym:

   1. Identyfikacja zagrożeń i podatności w systemie;

   2. Określanie prawdopodobieństwa i skali szkód wynikających z nieautoryzowanego dostępu, użytkowania, ujawniania, zakłócania, modyfikacji lub zniszczenia systemu, informacji, które system przetwarza, przechowuje lub przekazuje oraz wszelkich powiązanych informacji; oraz

   3. Określanie prawdopodobieństwa wystąpienia i wpływu niekorzystnych skutków dla osób, wynikających z przetwarzania danych osobowych;

b. Integrowanie wyników oceny ryzyka i decyzji dotyczących zarządzania ryzykiem z punktu widzenia organizacji i misji lub procesów biznesowych z oceną ryzyka na poziomie systemu;

c. Dokumentowanie wyników oceny ryzyka w [*Wybór: plan bezpieczeństwa i ochrony prywatności; raport z oceny ryzyka;* [*Realizacja: dokument określony przez organizację*]]*;*

d. Przeglądanie wyników oceny ryzyka [*Realizacja: częstotliwość określona przez organizację*]*;*

e. Rozpowszechnianie wyników oceny ryzyka wśród [*Realizacja: personel lub role określone przez organizację*]; oraz

f. Aktualizowanie oceny ryzyka [*Realizacja: częstotliwość określona przez organizację*] lub w przypadku istotnych zmian w systemie, środowisku jego działania lub innych warunków, które mogą mieć wpływ na stan bezpieczeństwa lub prywatności systemu.

Omówienie: Oceny ryzyka dotyczą zagrożeń, podatności, prawdopodobieństwa wystąpienia i wpływu na działalność organizacji i jej aktywa, osoby, inne organizacje

i Państwo. Oceny ryzyka uwzględniają również ryzyko ze strony podmiotów zewnętrznych, w tym wykonawców, którzy obsługują systemy w imieniu organizacji, osób mających dostęp do systemów organizacyjnych, dostawców usług i podwykonawców.

Organizacje mogą przeprowadzać oceny ryzyka na wszystkich trzech poziomach hierarchii zarządzania ryzykiem (tj. na poziomie organizacji, misji/procesu biznesowego lub systemu informatycznego) oraz na każdym etapie cyklu życia systemu. Oceny ryzyka mogą być również przeprowadzane w różnych etapach ram zarządzania ryzykiem, w tym na etapie przygotowania, kategoryzacji, wyboru zabezpieczeń, wdrażania zabezpieczeń, oceny zabezpieczeń, autoryzacji i monitorowania zabezpieczeń. Ocena ryzyka jest działaniem ciągłym, prowadzonym w całym cyklu życia systemu.

Oceny ryzyka mogą również dotyczyć informacji związanych z systemem, w tym projektu systemu, zamierzonego wykorzystania systemu, wyników badań oraz informacji lub artefaktów związanych z łańcuchem dostaw. Oceny ryzyka mogą odgrywać ważną rolę w procesach wyboru zabezpieczeń, szczególnie podczas stosowania wytycznych dotyczących dostosowania do indywidualnych potrzeb oraz w początkowych fazach określania właściwości.

Zabezpieczenia powiązane: CA-3, CA-6, CM-4, CM-13, CP-6, CP-7, IA-8, MA-5, PE-3, PE-8, PE-18, PL-2, PL- 10, PL-11, PM-8, PM-9, PM-28, PT-2, PT-7, RA-2, RA-5, RA-7, SA-8, SA-9, SC-38, SI-12.

Zabezpieczenia rozszerzone:

(1) SZACOWANIE RYZYKA | SZACOWANIE RYZYKA ŁAŃCUCHA DOSTAW

(a) Ocenianie ryzyka łańcucha dostaw związanego z [***Realizacja: systemy, komponenty systemu i usługi systemowe zdefiniowane przez organizację***]***;*** **oraz**

(b) Aktualizowanie oceny ryzyka łańcucha dostaw [***Realizacja: częstotliwość określona przez organizację***] **w przypadku wystąpienia istotnych zmian w danym łańcuchu dostaw lub gdy zmiany w systemie, środowisku pracy lub innych warunkach mogą wymagać zmiany w łańcuchu dostaw.**

Omówienie: Ryzyko związane z łańcuchem dostaw obejmuje zakłócenia, użycie wadliwych komponentów, wprowadzanie podróbek, kradzieże, złośliwe praktyki rozwojowe, niewłaściwe praktyki dostaw oraz wprowadzanie złośliwego kodu. Zdarzenia te mogą mieć istotny wpływ na poufność, integralność lub dostępność systemu i jego informacji, a zatem mogą mieć również negatywny wpływ na działalność organizacji (w tym na misję, funkcje, wizerunek lub reputację), zasoby organizacyjne, osoby, inne organizacje i Państwo. Zdarzenia związane z łańcuchem dostaw mogą być niezamierzone lub złośliwe i mogą wystąpić w dowolnym momencie cyklu życia systemu. Analiza ryzyka związanego z łańcuchem dostaw może pomóc organizacji w identyfikacji systemów lub komponentów, w przypadku których wymagane jest dodatkowe ograniczenie ryzyka związanego z łańcuchem dostaw.

Zabezpieczenia powiązane: RA-2, RA-9, PM-17, PM-30, SR-2.

(2) SZACOWANIE RYZYKA | WYMIANA INFORMACJI O ZAGROŻENIACH

Korzystanie podczas analizy ryzyka ze wszystkich źródeł informacji.

Omówienie: Organizacje wykorzystują informacje wywiadowcze ze wszystkich źródeł do podejmowania decyzji w zakresie inżynierii, zakupów i zarządzania ryzykiem. Informacje wywiadowcze o wszystkich źródłach składają się z informacji uzyskanych ze wszystkich dostępnych źródeł, w tym informacji dostępnych publicznie lub z otwartych źródeł, danych wywiadowczych dotyczących pomiarów i sygnatur, danych wywiadowczych dotyczących ludzi, danych wywiadowczych dotyczących sygnałów oraz danych wywiadowczych dotyczących obrazów. Informacje wywiadowcze obejmujące wszystkie źródła są wykorzystywane do analizy ryzyka związanego z podatnościami (zarówno zamierzonymi, jak

i niezamierzonymi) w procesach rozwoju, produkcji i dostaw, ludziach i środowisku. Analiza ryzyka może być przeprowadzana w odniesieniu do dostawców na wielu poziomach łańcucha dostaw, co pozwala na zarządzanie ryzykiem. Organizacje mogą zawierać umowy o dzieleniu się informacjami pochodzącymi z wywiadu obejmującego wszystkie źródła lub wynikającymi z nich decyzjami, z innymi organizacjami, w zależności od potrzeb..

Zabezpieczenia powiązane: Brak.

(3) SZACOWANIE RYZYKA | ŚWIADOMOŚĆ DYNAMIKI ZAGROŻEŃ

Określanie na bieżąco aktualnego środowiska cyberzagrożeń za pomocą [Realizacja: *środki zdefiniowane przez organizację*].

Omówienie: Zebrane informacje dotyczące rozpoznawania zagrożeń są wykorzystywane w procesach związanych z bezpieczeństwem informacji w organizacji w celu zapewnienia, że procedury są aktualizowane w odpowiedzi na zmieniające się środowisko zagrożeń. Na przykład, przy wyższych poziomach zagrożenia, organizacje mogą zmienić progi uprawnień lub uwierzytelniania obowiązujące przy wykonywaniu określonych operacji.

Zabezpieczenia powiązane: AT-2.

(4) SZACOWANIE RYZYKA | PROGNOZOWANA CYBERANALITYKA

Wykorzystywanie zaawansowanych możliwości w zakresie automatyzacji i analizy [*Realizacja: zaawansowane możliwości w zakresie automatyzacji i analizy zdefiniowane w organizacji*] w celu przewidywania i identyfikacji zagrożeń [***Realizacja: systemy lub komponenty systemu zdefiniowane w organizacji***]***:***

Omówienie: Odpowiednio wyposażone operacyjne centrum bezpieczeństwa (*ang. Security Operations Center - SOC*) lub zespół reagowania na incydenty bezpieczeństwa komputerowego (*Computer Security Incident Response Team - CSIRT*) może zostać przeciążony ilością informacji generowanych przez

rozpowszechnianie się narzędzi i urządzeń bezpieczeństwa, jeśli nie zastosuje zaawansowanej automatyzacji i analityki do analizy danych. Zaawansowane funkcje automatyzacji i analizy są zazwyczaj wspierane przez koncepcje sztucznej inteligencji, w tym uczenie maszynowe. Przykłady obejmują zautomatyzowane wykrywanie i reagowanie na zagrożenia (które obejmuje szeroko zakrojone gromadzenie danych, analizę kontekstową i możliwości adaptacyjnego reagowania), zautomatyzowane operacje przepływu informacji oraz narzędzia do podejmowania decyzji wspomagane maszynowo.

Zabezpieczenia powiązane: Brak.

Referencje: [OMB A-130], [NIST SP 800-30], [NIST SP 800-39], [NIST SP 800-161], [IR 8023], [IR 8062], [IR 8272].

RA-4 AKTUALIZACJA SZACOWANIA RYZYKA

[Wycofane: Włączone do RA-3].

RA-5 MONITOROWANIE I SKANOWANIE PODATNOŚCI

Zabezpieczenie podstawowe:

a. Monitorowanie i skanowanie podatności w systemie i aplikacjach hostingowych [*Realizacja: częstotliwość zdefiniowana przez organizację i/lub losowo, zgodnie z procesem zdefiniowanym przez organizację*] oraz w przypadku wykrycia i zgłoszenia nowych podatności , które mogą mieć wpływ na system;

b. Stosowanie narzędzi i technik monitorowania podatności na zagrożenia, które ułatwiają interoperacyjność narzędzi i automatyzują część procesu zarządzania podatnością na zagrożenia, wykorzystując do tego celu standardy:

   1. Wyliczania platform, błędów w oprogramowaniu i nieprawidłowych konfiguracji;

   2. Formatowania list kontrolnych i procedur badawczych; oraz

   3. Pomiaru wpływu podatności na zagrożenia;

c. Analizowanie raportów ze skanowania podatności i wyników monitorowania podatności;

d. Usuwanie uzasadnionych podatności [*Realizacja: zdefiniowany przez organizację czas reakcji*] *zgodnie* z organizacyjną oceną ryzyka;

e. Dzielenie się informacjami uzyskanymi z procesu monitorowania podatności i oceny zabezpieczeń z [*Realizacja: personel lub role określone przez organizację*] *w* celu wyeliminowania podobnych podatności w innych systemach (tj. słabości lub braków systemowych); oraz

f. Zastosowanie narzędzi do monitorowania podatności, które obejmują możliwość szybkiego aktualizowania podatności, które mają być skanowane..

Omówienie: Kategoryzacja bezpieczeństwa informacji i systemów wyznacza częstotliwość i kompleksowość monitorowania podatności (w tym skanowania). Organizacje określają wymagane monitorowanie podatności dla komponentów

systemu, upewniając się, że potencjalne źródła podatności - takie jak komponenty infrastruktury (np. przełączniki, routery, zapory, czujniki), drukarki sieciowe, skanery i kopiarki - nie są pomijane. Możliwość szybkiej aktualizacji narzędzi do monitorowania podatności w miarę odkrywania i ogłaszania nowych podatności oraz w miarę opracowywania nowych metod skanowania pomaga zapewnić, że nowe podatności nie zostaną pominięte przez stosowane narzędzia do monitorowania podatności. Proces aktualizacji narzędzi do monitorowania podatności pomaga zapewnić, że potencjalne podatności w systemie są identyfikowane i usuwane tak szybko, jak to możliwe. Monitorowanie i analiza podatności dla niestandardowego oprogramowania może wymagać dodatkowych podejść, takich jak analiza statyczna, dynamiczna, binarna lub hybrydowa tych trzech podejść. Organizacje mogą wykorzystywać te podejścia analityczne w przeglądach kodu źródłowego oraz w różnych narzędziach, w tym w skanerach aplikacji internetowych, narzędziach analizy statycznej i analizatorach binarnych.

Monitorowanie podatności obejmuje skanowanie pod kątem poziomu poprawek; skanowanie pod kątem funkcji, portów, protokołów i usług, które nie powinny być dostępne dla użytkowników lub urządzeń; oraz skanowanie pod kątem mechanizmów kontroli przepływu, które są niewłaściwie skonfigurowane lub działają niepoprawnie. Monitorowanie podatności może również obejmować narzędzia do ciągłego monitorowania podatności, które wykorzystują oprzyrządowanie do ciągłego analizowania komponentów. Narzędzia oparte na oprzyrządowaniu mogą zwiększyć dokładność i mogą być uruchamiane w całej organizacji bez konieczności skanowania. Narzędzia do monitorowania podatności, które ułatwiają interoperacyjność, obejmują narzędzia, które są walidowane przez Security Content Automated Protocol (SCAP). W związku z tym, organizacje rozważają użycie narzędzi skanujących, które wyrażają podatności w konwencji nazewnictwa Common Vulnerabilities and Exposures (CVE) i które wykorzystują Open Vulnerability Assessment Language (OVAL) do określania obecności podatności. Źródła informacji o podatnościach obejmują listę Common Weakness Enumeration (CWE) oraz

National Vulnerability Database (NVD). Oceny zgodności, takie jak ćwiczenia "czerwonego zespołu", dostarczają dodatkowych źródeł potencjalnych podatności, które należy przeskanować. Organizacje mogą również rozważyć użycie narzędzi skanujących, które wyrażają wpływ podatności za pomocą Common Vulnerability Scoring System (CVSS).

Monitorowanie podatności obejmuje kanał i proces umożliwiający otrzymywanie raportów o podatnościach bezpieczeństwa od ogółu społeczeństwa. Programy ujawniania podatności mogą być tak uproszczone, jak opublikowanie monitorowanego adresu e-mail lub formularza internetowego, który może odbierać raporty, w tym powiadomienia upoważniające do badania w dobrej wierze i ujawniania podatności bezpieczeństwa. Organizacje zazwyczaj spodziewają się, że takie badania odbywają się za ich zgodą lub bez niej i mogą wykorzystać publiczne kanały ujawniania podatności, aby zwiększyć prawdopodobieństwo, że odkryte podatności zostaną zgłoszone bezpośrednio do organizacji w celu ich usunięcia.

Organizacje mogą również stosować zachęty finansowe (znane również jako "bug bounty"), aby jeszcze bardziej zachęcić zewnętrznych badaczy bezpieczeństwa do zgłaszania odkrytych podatności. Programy "bug bounty" mogą być dopasowane do potrzeb organizacji. Zachęty finansowe mogą być stosowane bezterminowo lub przez określony czas i mogą być oferowane ogółowi społeczeństwa lub wybranej grupie. Organizacje mogą jednocześnie prowadzić publiczne i prywatne programy nagród i mogą zdecydować się na zaoferowanie niektórym uczestnikom częściowo uwierzytelnionego dostępu w celu oceny podatności bezpieczeństwa z uprzywilejowanych poziomów.

Zabezpieczenia powiązane: CA-2, CA-7, CA-8, CM-2, CM-4, CM-6, CM-8, RA-2, RA-3, SA-11, SA-15, SC-38, SI-2, SI-3, SI-4, SI-7, SR-11.

Zabezpieczenia rozszerzone:

(1) MONITOROWANIE I SKANOWANIE PODATNOŚCI | AKTUALIZACJA NARZĘDZI [Wycofane: Włączone do RA-5].

(2) MONITOROWANIE I SKANOWANIE PODATNOŚCI | NADZOROWANIE WYKRYTYCH PODATNOŚCI

Aktualizacja podatności systemowych, które mają zostać zeskanowane [***Wybór (jedna lub więcej)***]*:* [***Realizacja: częstotliwość określona przez organizację***]*;* ***przed nowym skanowaniem; po zidentyfikowaniu i zgłoszeniu nowych podatności***]**.**

Omówienie: Ze względu na złożoność współczesnego oprogramowania, systemów i innych czynników, regularnie odkrywane są nowe podatności. Ważne jest, aby nowo odkryte podatności były dodawane do listy podatności, które mają być skanowane w celu zapewnienia, że organizacja może podjąć kroki w celu ograniczenia tych podatności w odpowiednim czasie.

Zabezpieczenia powiązane: SI-5.

(3) MONITOROWANIE I SKANOWANIE PODATNOŚCI | ZAKRES PODATNOŚCI

Definiowanie zakresu i szczegółowości skanowania podatności.

Omówienie: Zakres skanowania podatności może być wyrażony, jako stosunek procentowy komponentów w systemie do konkretnej kategorią systemów, do krytyczności systemów, lub do liczby podatności do sprawdzenia. I odwrotnie, szczegółowość skanowania podatności może być wyrażona, jako poziom projektu systemu, który organizacja zamierza monitorować (np. komponent, moduł, podsystem, element).

Organizacje mogą określić, czy zakres skanowania podatności na zagrożenia jest wystarczający, biorąc pod uwagę jego tolerancję na ryzyko i inne czynniki. Narzędzia skanujące i sposób ich konfiguracji mogą mieć wpływ na szczegółowość i zakres. Do osiągnięcia pożądanej szczegółowości i zakresu może być potrzebnych wiele narzędzi skanujących. Publikacja [NSC 800-53A] zawiera dodatkowe informacje na temat zakresu i szczegółowości (GŁĘBOKOŚCI) pokrycia.

Zabezpieczenia powiązane: Brak.

(4) MONITOROWANIE I SKANOWANIE PODATNOŚCI NA ZAGROŻENIA | WYKRYWANIE SKANOWANIA

Ustalenie informacji dotyczących systemu, które są możliwe do wykrycia i przejęcia [Realizacja: zdefiniowane przez organizację działania korygujące].

Omówienie: Informacje możliwe do wykrycia obejmują informacje, które przeciwnicy mogą uzyskać bez skompromitowania lub naruszenia systemu, np. poprzez zbieranie informacji, które system ujawnia lub poprzez prowadzenie szeroko zakrojonych skanowań sieci. Działania naprawcze obejmują powiadomienie odpowiedniego personelu organizacyjnego, usunięcie wskazanych informacji lub zmodyfikowanie systemu w taki sposób, aby wskazane informacje stały się mniej istotne lub atrakcyjne dla przeciwników. To udoskonalenie nie obejmuje celowo wykrywanych informacji, które mogą być częścią wabika (np. honeypots, honeynets lub deception nets) wdrożonego przez organizację.

Zabezpieczenia powiązane: AU-13, SC-26.

(5) MONITOROWANIE I SKANOWANIE SŁABYCH PUNKTÓW | DOSTĘP UPRZYWILEJOWANY

Wprowadzenie autoryzowanego dostępu uprzywilejowanego do [*Realizacja: zdefiniowane* przez organizację *komponenty systemu*] dla wybranych działań [*Realizacja: zdefiniowane przez organizację działania w zakresie skanowania podatności*].

Omówienie: W pewnych sytuacjach charakter skanowania podatności na zagrożenia może być bardziej inwazyjny lub też element systemu, który jest przedmiotem skanowania, może zawierać informacje niejawne lub kontrolowane informacje jawne, takie jak informacje umożliwiające identyfikację osób. Autoryzacja uprzywilejowanego dostępu do wybranych komponentów systemu ułatwia dokładniejsze skanowanie podatności i chroni wrażliwą naturę takiego skanowania.

Zabezpieczenia powiązane: Brak.

(6) MONITOROWANIE I SKANOWANIE PODATNOŚCI | AUTOMATYCZNE ANALIZY TRENDÓW

Porównanie wyników wielokrotnych skanowań podatności za pomocą [*Realizacja: zdefiniowane przez organizację zautomatyzowane mechanizmy*].

Omówienie: Wykorzystanie automatycznych mechanizmów do analizy wielokrotnych w czasie skanowań podatności może pomóc w określeniu trendów w podatnościach systemu i identyfikacji wzorców ataków.

Zabezpieczenia powiązane: Brak.

(7) MONITOROWANIE I SKANOWANIE PODATNOŚCI NA ZAGROŻENIA | AUTOMATYCZNE WYKRYWANIE I POWIADAMIANIE O NIEAUTORYZOWANYCH KOMPONENTACH

[Wycofane: Włączone do CM-8].

(8) MONITOROWANIE I SKANOWANIE PODATNOŚCI | PRZEGLĄD HISTORYCZNYCH LOGÓW AUDYTU

Przeglądanie historycznych logów audytu w celu ustalenia, czy podatność zidentyfikowana w [Realizacja: *system zdefiniowany przez organizację*] została wcześniej wykorzystana [*Realizacja: okres czasu zdefiniowany przez organizację*].

Omówienie: Przegląd historycznych logów audytu w celu ustalenia, czy wykryta niedawno podatność w systemie została wcześniej wykorzystana przez adwersarza, może dostarczyć ważnych informacji dla analiz kryminalistycznych. Analizy takie mogą pomóc w określeniu, na przykład, zakresu poprzedniego włamania, technik wykorzystanych podczas ataku, informacji organizacyjnych, które zostały przefiltrowane lub zmodyfikowane, misji lub możliwości biznesowych, na które miał wpływ oraz czasu trwania ataku.

Zabezpieczenia powiązane: AU-6, AU-11.

(9) MONITOROWANIE I SKANOWANIE PODATNOŚCI | TESTY PENETRACYJNE I ANALIZY

[Wycofane: Włączone do CA-8].

(10) MONITOROWANIE I SKANOWANIE PODATNOŚCI | KORELACJA SKANOWANYCH DANYCH

Korelowanie danych wyjściowych z narzędzi skanowania podatności w celu określenia obecności wektorów ataków typu „multi-vulnerability" i „multi-hop".

Omówienie: Wektor ataku to droga lub sposoby, za pomocą których przeciwnik może uzyskać dostęp do systemu w celu dostarczenia złośliwego kodu lub eksfiltracji informacji. Organizacje mogą wykorzystywać drzewa ataków, aby pokazać, w jaki sposób wrogie działania przeciwników oddziałują na siebie i łączą się w celu wywołania negatywnych skutków lub negatywnych konsekwencji dla systemów i organizacji. Takie informacje, wraz ze skorelowanymi danymi z narzędzi skanowania podatności, mogą zapewnić większą przejrzystość w odniesieniu do wektorów ataków typu „multi-vulnerability" i „multi-hop". Korelacja informacji ze skanowania podatności jest szczególnie ważna, gdy organizacje przechodzą ze starszych technologii na nowsze (np. przejście z protokołów sieciowych IPv4 na IPv6). Podczas takich transformacji, niektóre komponenty systemu mogą być nieumyślnie niezarządzane i stwarzać możliwości wykorzystania przez przeciwnika.

Zabezpieczenia powiązane: Brak.

(11) MONITOROWANIE I SKANOWANIE PODATNOŚCI | PROGRAM UPUBLICZNIANIA PODATNOŚCI

Ustanowienie ogólnie dostępnego kanału zgłaszania podatności w systemach organizacyjnych i ich komponentach.

Omówienie: Kanał zgłoszeniowy jest publicznie dostępny i zawiera przejrzyste informacje umożliwiające przeprowadzanie działań w dobrej wierze oraz ujawnianie podatności organizacji. Organizacja nie uzależnia swojej zgody na przeprowadzenie badań od oczekiwania, że raportowany podmiot nie ujawni ich do wiadomości publicznej, ale może zażądać określonego czasu na odpowiednie usunięcie podatności.

Zabezpieczenia powiązane: Brak.

Referencje: [ISO 29147], [NIST SP 800-40], [NIST SP 800-53A], [NIST SP 800-70], [NIST SP 800-115], [NIST SP 800-126], [IR 7788], [IR 8011-4], [IR 8023].

RA-6 TECHNICZNE ZABEZPIECZENIE PRZED PODGLĄDEM I PODSŁUCHEM

Zabezpieczenie podstawowe: Stosowanie technicznych zabezpieczeń przed podglądem i podsłuchem w [*Realizacja: lokalizacja określona przez organizację*] z [[*Wybór (jeden lub więcej)*]: [*Realizacja: częstotliwość określona przez organizację*]; *w* przypadku wystąpienia następujących zdarzeń lub wskaźników: [Realizacja: *zdarzenia lub wskaźniki określone przez organizację*]].

Omówienie Stosowanie technicznych zabezpieczeń przed podglądem i podsłuchem jest usługą świadczoną przez wykwalifikowany personel w celu wykrycia obecności urządzeń do podglądu i podsłuchu oraz zidentyfikowania słabości zabezpieczeń technicznych, które mogłyby zostać wykorzystane do przeprowadzenia penetracji technicznej badanego obiektu. Przeglądy technicznych zabezpieczeń przed podglądem i podsłuchem umożliwiają również ocenę kondycji bezpieczeństwa technicznego organizacji i obiektów i obejmują wizualne, elektroniczne i fizyczne sprawdzanie badanych obiektów, wewnątrz i na zewnątrz. Badania te dostarczają również użytecznych danych do oceny ryzyka i informacji dotyczących narażenia organizacji na potencjalne zagrożenia.

Zabezpieczenia powiązane: Brak.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

RA-7 REAKCJA NA RYZYKO

Zabezpieczenie podstawowe: Reagowanie na informacje z oceny bezpieczeństwa i prywatności, monitorowania i audytów zgodnie z tolerancją ryzyka organizacyjnego.

Omówienie: Organizacje mają wiele możliwości reagowania na ryzyko, w tym ograniczanie ryzyka poprzez wdrażanie nowych zabezpieczeń lub wzmacnianie istniejących, akceptowanie ryzyka z odpowiednim uzasadnieniem lub racją, dzielenie się lub przenoszenie ryzyka, lub unikanie ryzyka. Tolerancja ryzyka organizacji wpływa na decyzje i działania podejmowane w odpowiedzi na ryzyko. Reakcja na ryzyko jest odpowiedzią na potrzebę określenia właściwej reakcji na ryzyko przed wygenerowaniem planu i etapów działań. Na przykład, reakcją na ryzyko może być zaakceptowanie lub odrzucenie ryzyka, lub też natychmiastowe ograniczenie ryzyka tak, aby plan działania i wprowadzanie etapów kluczowych nie było konieczne. Jeżeli jednak reakcja na ryzyko ma na celu ograniczenie ryzyka, a ograniczenie go nie może zostać zrealizowane natychmiast, generowany jest plan i etapy działania.

Zabezpieczenia powiązane: CA-5, IR-9, PM-4, PM-28, RA-2, RA-3, SR-2.

Zabezpieczenia rozszerzone: Brak.

Referencje: [FIPS 199], [FIPS 200], [NIST SP 800-30], [NIST SP 800-37], [NIST SP 800-39], [NIST SP 800-160-1].

RA-8 OCENY WPŁYWU NA PRYWATNOŚĆ

Zabezpieczenie podstawowe: Przeprowadzenie oceny wpływu systemów, programów lub innych działań na prywatność, przed:

a. Opracowaniem lub zamówieniem technologii informatycznych, która przetwarzać będą informacje umożliwiające identyfikację osób; oraz

b. Rozpoczęciem nowego zbierania informacji umożliwiających identyfikację osób, które:

1. Będą przetwarzane przy użyciu technologii informatycznych; oraz
2. Zawierają dane osobowe pozwalające na fizyczny lub wirtualny (online) kontakt z określoną osobą, jeżeli identyczne kwestionariusze zostały przedstawione lub identyczne wymagania sprawozdawcze zostały postawione dziesięciu lub więcej osobom innych niż organizacje, instytucje lub pracownicy państwowi.

Omówienie: Ocena wpływu na prywatność to analiza sposobu, w jaki przetwarzane są dane osobowe w celu zapewnienia, że ich przetwarzanie jest zgodne z obowiązującymi wymogami w zakresie ochrony prywatności, określenia zagrożeń dla prywatności związanych z systemem informatycznym lub działalnością organizacji oraz oceny sposobów ograniczenia zagrożeń dla prywatności. Ocena wpływu na prywatność jest zarówno analizą, jak i formalnym dokumentem, który szczegółowo opisuje proces i wyniki analizy.

Organizacje przeprowadzają i opracowują ocenę wpływu na prywatność w sposób wystarczająco jasny i szczegółowy, aby wykazać, że organizacja w pełni uwzględniła ochronę prywatności i wprowadziła odpowiednie środki ochrony prywatności od najwcześniejszych etapów działalności organizacji i w całym cyklu życia informacji. W celu przeprowadzenia znaczącej oceny wpływu na prywatność, SAOP[90] ściśle współpracuje z kierownikami programów, właścicielami systemów, ekspertami ds.

[90] Patrz: NSC 800-37; NSC 7298.

technologii informatycznych, personelem ds. bezpieczeństwa, doradcami i innymi odpowiednimi pracownikami organizacji. Co więcej, ocena wpływu na prywatność nie jest działaniem limitowanym czasowo i nie ogranicza się do określonego etapu działania lub stanu rozwoju systemu informatycznego lub cykli życia danych osobowych. Analiza prywatności jest raczej kontynuowana przez cały czas trwania systemu i cykli życia informacji umożliwiających identyfikację osoby. W związku z tym ocena wpływu na prywatność jest żywym dokumentem, który organizacje aktualizują za każdym razem, gdy zmiany w technologii informatycznej, zmiany w praktykach organizacji lub inne czynniki wpływają na zagrożenia dla prywatności związane z wykorzystaniem takiej technologii informatycznej.

W celu przeprowadzenia oceny wpływu na prywatność, organizacje mogą korzystać z ocen bezpieczeństwa i ryzyka związanego z prywatnością. Organizacje mogą również korzystać z innych powiązanych procesów, które mogą mieć różne nazwy, w tym z analiz progów prywatności. Ocena wpływu na prywatność może również służyć jako informacja dla opinii publicznej na temat praktyk organizacji w odniesieniu do prywatności. Chociaż przeprowadzanie i publikowanie ocen wpływu na prywatność może być wymagane przez prawo, organizacje mogą opracować takie polityki w przypadku braku stosownych przepisów.

Zabezpieczenia powiązane: CM-4, CM-9, CM-13, PT-2, PT-3, PT-5, RA-1, RA-2, RA-3, RA-7.

Zabezpieczenia rozszerzone: Brak.

Referencje: [EGOV], [OMB A-130], [OMB M-03-22].

RA-9 ANALIZA KRYTYCZNOŚCI

Zabezpieczenie podstawowe: Identyfikowanie krytycznych komponentów i funkcji systemu poprzez przeprowadzenie analizy krytyczności dla [*Realizacja: zdefiniowane przez organizację systemy, komponenty systemu lub usługi systemowe*] w [*Realizacja: zdefiniowane przez organizację punkty decyzyjne w cyklu życia systemu*].

Omówienie: Nie wszystkie komponenty systemu, funkcje lub usługi wymagają istotnych zabezpieczeń. Na przykład, analiza krytyczności jest kluczowym elementem zarządzania ryzykiem w łańcuchu dostaw i stanowi podstawę do ustalenia priorytetów działań ochronnych. Identyfikacja krytycznych komponentów i funkcji systemu uwzględnia obowiązujące prawa, rozporządzenia, regulacje, dyrektywy, zasady, standardy, wymagania dotyczące funkcjonalności systemu, interfejsy systemu i komponentów oraz zależności systemu i komponentów. Inżynierowie systemowi przeprowadzają dekompozycję funkcjonalną systemu w celu identyfikacji krytycznych funkcji i komponentów. Dekompozycja funkcjonalna obejmuje identyfikację misji organizacyjnych wspieranych przez system, dekompozycję na konkretne funkcje w celu wykonania tych misji oraz śledzenie sprzętu, aplikacji i komponentów oprogramowania układowego, które implementują te funkcje, również wtedy, gdy funkcje te są współdzielone przez wiele komponentów wewnątrz i na zewnątrz systemu.

Środowisko operacyjne systemu lub komponentu systemu może mieć wpływ na krytyczność, w tym na połączenia z systemami, urządzeniami, systemami i zleconymi na zewnątrz usługami informatycznymi oraz zależności od nich. Komponenty systemu, które umożliwiają dostęp bez pośrednictwa do krytycznych elementów lub funkcji systemu, uznaje się za krytyczne ze względu na nieodłączne podatności, które takie elementy stwarzają. Krytyczność komponentów i funkcji oceniana jest pod kątem wpływu awarii komponentów lub funkcji na misje organizacyjne, które są wspierane przez system zawierający komponenty i funkcje.

Analiza krytyczności jest przeprowadzana podczas opracowywania, modyfikowania lub ulepszania architektury lub projektu. Jeżeli taka analiza jest przeprowadzana we wczesnym etapie cyklu życia systemu, organizacje mogą być w stanie zmodyfikować projekt systemu w celu ograniczenia krytycznej natury tych komponentów i funkcji, np. poprzez dodanie redundancji lub alternatywnych ścieżek w projekcie systemu. Analiza krytyczności może również wpływać na środki ochrony wymagane przez wykonawców prac rozwojowych. Oprócz analizy krytyczności systemów, komponentów systemu i usług systemowych, ważnym elementem jest analiza krytyczności informacji. Analiza taka przeprowadzana jest w ramach kategoryzacji bezpieczeństwa w zabezpieczeniu RA-2.

Zabezpieczenia powiązane: CP-2, PL-2, PL-8, PL-11, PM-1, PM-11, RA-2, SA-8, SA-15, SA-20, SR-5.

Zabezpieczenia rozszerzone: Brak.

Referencje: [IR 8179].

RA-10 WYSZUKIWANIE ZAGROŻEŃ

Zabezpieczenie podstawowe:

a. Ustanowienie i utrzymanie zdolności do wyszukiwania cyberzagrożeń w celu:

   1. Poszukiwania czynników świadczących o zagrożeniu w systemach organizacyjnych; oraz

   2. Wykrywania, śledzenia i likwidowania zagrożeń, które omijają istniejącą zabezpieczenie; oraz

b. Wykorzystanie zdolności do wyszukiwania cyberzagrożeń [*Realizacja: częstotliwość określona przez organizację*].

Omówienie: Wykorzystanie zagrożenia jest aktywnym środkiem cyberobrony w przeciwieństwie do tradycyjnych środków bezpieczeństwa, takich jak zapory ogniowe, systemy wykrywania i zapobiegania włamaniom, kwarantanna złośliwego kodu w środowiskach zamkniętych (piaskownicach) oraz technologie i systemy zarządzania bezpieczeństwem informacji i zdarzeń. Wyszukiwanie cyberzagrożeń polega na aktywnym poszukiwaniu zaawansowanych zagrożeń w systemach organizacyjnych, sieciach i infrastrukturze. Celem jest śledzenie i zakłócanie działania cyberprzestępców na jak najwcześniejszym etapie sekwencji ataku oraz wymierne zwiększenie szybkości i dokładności reakcji organizacyjnych. Oznakami kompromitacji są m.in. nietypowy ruch sieciowy, nietypowe zmiany plików oraz obecność złośliwego kodu. Zespoły zajmujące się poszukiwaniem zagrożeń wykorzystują istniejącą wiedzę o zagrożeniach i mogą tworzyć nowe, udostępniane organizacjom partnerskim, organizacjom zajmującym się wymianą informacji i analizą (*ang. Sharing and Analysis Organizations - ISAO*), Centrom Wymiany i Analizy Informacji (*ang. Information Sharing and Analysis Centers - ISAC*) oraz odpowiednim organizacjom i instytucjom rządowym.

Zabezpieczenia powiązane: CA-2, CA-7, CA-8, RA-3, RA-5, RA-6, SI-4.

Zabezpieczenia rozszerzone: Brak.

KATEGORIA SA – NABYWANIE SYSTEMU I USŁUG

SA-1 POLITYKA I PROCEDURY

Zabezpieczenie podstawowe:

a. Opracowywanie, dokumentowanie i rozpowszechnianie wśród [Realizacja: *personel lub role określone przez organizację*]:

   1. [*Wybór (jeden lub więcej): poziom organizacji; poziom misji/procesu biznesowego; poziom systemu*] polityki nabywania systemu i usług, która:

      (a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami; oraz

      (b) Jest zgodna z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi; oraz

   2. Procedur ułatwiających wdrożenie polityki nabywania systemu i usług oraz powiązanych zabezpieczeń w zakresie nabywania systemu i usług;

b. Wyznaczanie [Realizacja: *osoba wyznaczona przez organizację*] do zarządzania rozwojem, dokumentacją i rozpowszechnianiem polityki i procedur nabywania systemu i usług; oraz

c. Przeglądanie i aktualizacja bieżącej:

   1. Polityki nabywania systemu i usług z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*]; oraz

   2. Procedur nabywania systemu i usług z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*].

Omówienie: Polityka i procedury w zakresie nabywania systemu i usług dotyczą zabezpieczeń w kategorii *Nabywanie systemu i usług* (SA), które są wdrażane w ramach systemów i organizacji. Strategia zarządzania ryzykiem jest ważnym

czynnikiem przy tworzeniu takich polityk i procedur. Polityki i procedury przyczyniają się do zapewnienia bezpieczeństwa i ochrony prywatności. Dlatego ważne jest, aby programy bezpieczeństwa i ochrony prywatności były opracowywane wspólnie przy kształtowaniu polityki i procedur nabywania systemu i usług. Polityki i procedury dotyczące programów bezpieczeństwa i ochrony prywatności na poziomie organizacji są ogólnie rzecz biorąc preferowane i mogą eliminować potrzeby tworzenia polityk i procedur specyficznych dla danej misji lub systemu. Polityka może być włączona jako część ogólnej polityki bezpieczeństwa i ochrony prywatności lub reprezentowana przez wiele polityk odzwierciedlających złożony charakter organizacji. Procedury mogą być ustanowione dla programów bezpieczeństwa i ochrony prywatności, dla misji lub procesów biznesowych oraz dla systemów, jeśli to konieczne. Procedury opisują sposób wdrażania zasad lub zabezpieczeń i mogą być skierowane do osoby lub roli, która jest przedmiotem procedury. Procedury mogą być udokumentowane w planach bezpieczeństwa i ochrony prywatności systemu w jednym lub kilku oddzielnych dokumentach.

Zdarzenia, które mogą spowodować konieczność aktualizacji polityki i procedur nabywania systemu i usług, obejmują wyniki oceny lub audytu, incydenty lub naruszenia bezpieczeństwa, lub zmiany w przepisach prawa, zarządzeniach, dyrektywach, rozporządzeniach, zasadach, standardach i wytycznych.

Oświadczenie o wprowadzeniu zabezpieczeń nie jest równoznaczne z ustanowieniem polityki lub procedury organizacyjnej.

Zabezpieczenia powiązane: PM-9, PS-8, SA-8, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [NIST SP 800-12], [NIST SP 800-30], [NIST SP 800-39], [NIST SP 800-100], [NIST SP 800-160-1].

SA-2 PRZYDZIAŁ ZASOBÓW

Zabezpieczenie podstawowe:

a. Określanie wysokiego poziomu wymagań bezpieczeństwa informacji i prywatności systemu lub usługi systemowej w planowaniu misji i procesów biznesowych;

b. Określanie, dokumentowanie i przydzielanie zasobów niezbędnych do ochrony systemu lub usługi systemowej w ramach procesu planowania kapitału organizacyjnego i zabezpieczeń inwestycji; oraz

c. Ustanowienie odrębnej pozycji dotyczącej bezpieczeństwa informacji izochrony prywatności w dokumentacji organizacyjnej dotyczącej programowania i budżetowania.

Omówienie: Alokacja zasobów na bezpieczeństwo informacji i ochronę prywatności obejmuje finansowanie ryzyka związanego z nabywaniem systemów i usług, utrzymania i łańcucha dostaw w całym cyklu życia systemu.

Zabezpieczenia powiązane: PL-7, PM-3, PM-11, SA-9, SR-3, SR-5.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [NIST SP 800-37], [NIST SP 800-160-1].

SA-3 CYKL ŻYCIA SYSTEMU

Zabezpieczenie podstawowe:

a. Nabywanie, rozwijanie i zarządzanie systemem przy użyciu [*Realizacja: zdefiniowany przez organizację cykl życia systemu*], który obejmuje kwestie bezpieczeństwa i ochrony prywatności informacji;

b. Zdefiniowanie i udokumentowanie ról i obowiązków w zakresie bezpieczeństwa i ochrony prywatności informacji w całym cyklu życia systemu;

c. Określanie osób pełniących funkcje i obowiązki w zakresie bezpieczeństwa i ochrony prywatności informacji; oraz

d. Włączenie procesu zarządzania bezpieczeństwem informacji organizacyjnych i ryzykiem związanym z ochroną prywatności do działań związanych z rozwojem systemu w cyklu życia.

Omówienie: Proces cyklu życia systemu stanowi podstawę pomyślnego rozwoju, wdrażania i funkcjonowania systemów organizacyjnych. Integracja kwestii bezpieczeństwa i ochrony prywatności na wczesnym etapie cyklu życia systemu jest podstawową zasadą inżynierii bezpieczeństwa i ochrony prywatności systemów. Zastosowanie wymaganych zabezpieczeń w ramach cyklu życia systemu wymaga podstawowego zrozumienia bezpieczeństwa i ochrony prywatności informacji, zagrożeń, podatności, negatywnych skutków i ryzyka dla krytycznych misji i funkcji biznesowych. Zasady inżynierii bezpieczeństwa zawarte w zabezpieczeniu SA-8 pomagają w prawidłowym projektowaniu, kodowaniu i testowaniu systemów i komponentów systemu. Organizacje angażują wykwalifikowany personel (np. SAISO, SAOP, architektów ds. bezpieczeństwa i ochrony prywatności oraz inżynierów ds. bezpieczeństwa i ochrony prywatności)[91] w procesach cyklu życia systemów w celu zapewnienia, że ustalone wymagania dotyczące bezpieczeństwa

[91] Patrz: NSC 800-37; NSC 7298.

i ochrony prywatności są włączone do systemów organizacyjnych. Programy szkoleniowe w zakresie bezpieczeństwa i ochrony prywatności oparte na rolach mogą zapewnić, że osoby pełniące kluczowe role i obowiązki w zakresie bezpieczeństwa i ochrony prywatności będą miały doświadczenie, umiejętności i wiedzę specjalistyczną do prowadzenia przypisanych im działań w ramach cyklu życia systemu.

Skuteczna integracja wymagań w zakresie bezpieczeństwa i ochrony prywatności z architekturą korporacyjną pomaga również zapewnić, że ważne względy bezpieczeństwa i ochrony prywatności są uwzględniane w całym cyklu życia systemu i że aspekty te są bezpośrednio związane z misją organizacji i procesami biznesowymi. Proces ten ułatwia również integrację architektur bezpieczeństwa i ochrony prywatności informacji z architekturą korporacyjną, zgodną ze strategią zarządzania ryzykiem organizacji. Ponieważ w cyklu życia systemu zaangażowanych jest wiele organizacji (np. dostawcy zewnętrzni, programiści, integratorzy, usługodawcy), funkcje i zabezpieczenia nabywania i zarządzania ryzykiem w łańcuchu dostaw odgrywają znaczącą rolę w efektywnym zarządzaniu systemem w całym cyklu życia.

Zabezpieczenia powiązane: AT-3, PL-8, PM-7, SA-4, SA-5, SA-8, SA-11, SA-15, SA-17, SA-22, SR-3, SR-4, SR-5, SR-9.

Zabezpieczenia rozszerzone:

(1) CYKL ŻYCIA SYSTEMU | ZARZĄDZANIE ŚRODOWISKIEM PRZEDPRODUKCYJNYM

Zabezpieczanie środowiska przedprodukcyjnego systemu, współmiernie do ryzyka, przez cały cykl życia systemu, komponentu systemu lub usługi systemu.

Omówienie: Środowisko przedprodukcyjne obejmuje środowiska rozwojowe, testowe i integracyjne. Ustanowione procesy planowania programów bezpieczeństwa są przykładami zarządzania środowiskiem przedprodukcyjnym. Analiza krytyczności i stosowanie zabezpieczeń nad programistami również

przyczyniają się do zwiększenia bezpieczeństwa środowiska programistycznego systemu.

Zabezpieczenia powiązane: CM-2, CM-4, RA-3, RA-9, SA-4.

(2) CYKL ŻYCIA SYSTEMU | KORZYSTANIE Z DANYCH BIEŻĄCYCH LUB OPERACYJNYCH

(a) Zatwierdzanie, dokumentowanie i kontrolowanie wykorzystania danych bieżących w środowiskach przedprodukcyjnych w odniesieniu do systemu, komponentu systemu lub usługi systemowej; oraz

(b) Zabezpieczanie środowiska przedprodukcyjnego systemu, komponentu systemu lub usługi systemowej na tym samym poziomie wpływu lub klasyfikacji, co wszystkie dane bieżące używane w środowiskach przedprodukcyjnych.

Omówienie: Dane bieżące odnoszą się również do danych operacyjnych. Wykorzystanie danych bieżących lub operacyjnych w środowiskach przedprodukcyjnych (tj. w środowiskach rozwojowych, testowych i integracyjnych) może wiązać się ze znacznym ryzykiem dla organizacji. Ponadto, wykorzystanie danych osobowych w testach, badaniach i szkoleniach zwiększa ryzyko nieuprawnionego ujawnienia lub niewłaściwego wykorzystania takich informacji. Dlatego ważne jest, aby organizacja zarządzała wszelkimi dodatkowymi zagrożeniami, które mogą wynikać z wykorzystania danych bieżących lub operacyjnych. Organizacje mogą minimalizować takie ryzyko, wykorzystując testowe lub fikcyjne dane podczas projektowania, rozwoju i testowania systemów, komponentów systemu i usług systemowych. Techniki oceny ryzyka mogą być stosowane w celu określenia, czy ryzyko związane z wykorzystaniem danych bieżących lub operacyjnych jest dopuszczalne.

Zabezpieczenia powiązane: PM-25, RA-3.

(3) CYKL ŻYCIA SYSTEMU | ODŚWIEŻANIE TECHNOLOGII

Zaplanowanie i wdrożenie harmonogramu odświeżania technologii przez cały cykl życia systemu.

Omówienie: Planowanie odświeżania technologii może obejmować sprzęt, aplikacje, oprogramowanie układowe, procesy, kompetencje personelu, dostawców, usługodawców i infrastrukturę. Korzystanie z przestarzałych lub nieprodukowanych technologii może zwiększyć ryzyko związane z używaniem nieobsługiwanych, podrobionych lub zmienionych komponentów, elementami, które nie są w stanie wdrożyć wymogów bezpieczeństwa lub ochrony prywatności, elementami powolnymi lub niedziałającymi, elementami pochodzącymi z niezaufanych źródeł, niezamierzonym błędem personelu lub zwiększoną złożonością. Odświeżanie technologii następuje zazwyczaj na etapie eksploatacji i konserwacji w cyklu życia systemu.

Zabezpieczenia powiązane: MA-6.

Referencje: [OMB A-130], [NIST SP 800-30], [NIST SP 800-37], [NIST SP 800-160-1], [NIST SP 800-171], [NIST SP 800-172].

SA-4 PROCES NABYCIA

Zabezpieczenie podstawowe: Uwzględnianie zgodnie z obowiązującymi przepisami prawnymi, zarządzeniami wykonawczymi, dyrektywami, politykami, przepisami, standardami, oraz wytycznymi - wprost lub przez odniesienie - następujących wymagań, opisów i kryteriów stosując [*Wybór (jeden lub więcej): standardowy język umowy;* [*Realizacja: język umowy określony przez organizację*]] w umowie nabycia systemu, komponentu systemu lub usługi systemu, dotyczących:

a. Funkcji bezpieczeństwa i ochrony prywatności;

b. Siły mechanizmów bezpieczeństwa i ochrony prywatności;

c. Pewności w zakresie bezpieczeństwa i ochrony prywatności;

d. Zabezpieczeń niezbędnych do spełnienia wymogów bezpieczeństwa i ochrony prywatności.

e. Dokumentacji w zakresie bezpieczeństwa i ochrony prywatności;

f. Ochrony dokumentacji dotyczącej bezpieczeństwa i ochrony prywatności;

g. Opisu środowiska rozwoju systemu i środowiska, w którym system ma funkcjonować;

h. Podziału rozliczalności lub określenie stron odpowiedzialnych za bezpieczeństwo informacji, prywatność i zarządzanie ryzykiem w łańcuchu dostaw; oraz

i. Kryteriów akceptacji.

Omówienie: Wymagania funkcjonalne w zakresie bezpieczeństwa i ochrony prywatności wynikają zazwyczaj z wysokiego poziomu wymagań bezpieczeństwa i ochrony prywatności opisanych w zabezpieczeniu SA-2. Wymagania te obejmują możliwości, funkcje i mechanizmy w zakresie bezpieczeństwa i ochrony prywatności. Wymagania wytrzymałościowe związane z takimi możliwościami, funkcjami i mechanizmami obejmują stopień poprawności, kompletności, odporności na ingerencję lub obejście oraz odporności na bezpośredni atak. Wymagania dotyczące

wiarygodności obejmują procesy, procedury i metodologie rozwojowe, a także dowody z działań rozwojowych i oceniających, które dają podstawy do pewności, że wymagana funkcjonalność jest wdrażana i posiada wymaganą siłę mechanizmu. [NIST SP 800-160-1] opisuje proces inżynierii wymagań, jako część cyklu życia systemu.

Zabezpieczenia mogą być postrzegane, jako opisy zabezpieczeń i możliwości ochrony odpowiednich dla osiągnięcia konkretnych celów organizacji w zakresie bezpieczeństwa i ochrony prywatności oraz dla odzwierciedlenia wymogów bezpieczeństwa i ochrony prywatności interesariuszy. Zabezpieczenia są wybierane i wdrażane w celu spełnienia wymagań systemowych i obejmują odpowiedzialność dewelopera i organizacji. Zabezpieczenia mogą obejmować aspekty techniczne, administracyjne i fizyczne. W niektórych przypadkach, wybór i wdrożenie zabezpieczeń może wymagać dodatkowej specyfikacji przez organizację w postaci wymagań pochodnych lub wartości parametrów zabezpieczeń. Wymagania pochodne i wartości parametrów zabezpieczeń mogą być niezbędne do zapewnienia odpowiedniego poziomu szczegółowości implementacji zabezpieczeń w ramach cyklu życia systemu.

Wymagania dotyczące dokumentacji w zakresie bezpieczeństwa i ochrony prywatności odnoszą się do wszystkich etapów cyklu życia systemu. Dokumentacja zawiera wskazówki dla użytkowników i administratorów dotyczące wdrażania i obsługi zabezpieczeń. Poziom szczegółowości wymaganej w takiej dokumentacji opiera się na kategoryzacji lub poziomie klasyfikacji bezpieczeństwa systemu oraz na stopniu, w jakim organizacje zależą od możliwości, funkcji lub mechanizmów umożliwiających spełnienie oczekiwań dotyczących reakcji na ryzyko. Wymagania mogą obejmować obowiązkowe ustawienia konfiguracyjne, które określają dozwolone funkcje, porty, protokoły i usługi. Kryteria akceptacji dla systemów, komponentów systemu i usług systemowych są zdefiniowane w taki sam sposób, jak kryteria dla wszelkich zakupów lub zamówień organizacyjnych.

Zabezpieczenia powiązane: CM-6, CM-8, PS-7, SA-3, SA-5, SA-8, SA-11, SA-15, SA-16, SA-17, SA-21, SR-3, SR-5.

Zabezpieczenia rozszerzone:

(1) PROCES NABYCIA | WŁAŚCIWOŚCI FUNKCJONALNE ZABEZPIECZEŃ

Zażądanie od twórcy systemu, komponentu systemu lub usługi systemowej przedstawienia opisu właściwości funkcjonalnych wdrażanego zabezpieczenia.

Omówienie: Właściwości funkcjonalne środków bezpieczeństwa i ochrony prywatności opisują funkcjonalność (tzn. możliwości w zakresie zapewnienia bezpieczeństwa lub prywatności, funkcje lub mechanizmy) widoczne na interfejsach środków bezpieczeństwa, a w szczególności wykluczają struktury funkcjonalne i struktury danych wewnętrznych dla działania środków bezpieczeństwa.

Zabezpieczenia powiązane: Brak.

(2) PROCES NABYCIA | PROJEKTOWANIE / IMPLEMENTACJA ZABEZPIECZEŃ

Wymaganie od producenta systemu, komponentu systemu lub usługi systemowej dostarczenia informacji o projekcie i wdrożeniu systemu zabezpieczeń, które obejmują: *Wybór (jeden lub więcej): istotne dla bezpieczeństwa zewnętrzne interfejsy systemu; projekt wysokopoziomowy; projekt niskopoziomowy; kod źródłowy lub schematy sprzętu;* [*Realizacja: informacje dotyczące projektu i wdrożenia określone przez organizację*] na poziomie [Realizacja: *poziom szczegółowości projektu określony przez organizację*].

Omówienie: Organizacje mogą wymagać różnych poziomów szczegółowości w dokumentacji dotyczącej projektowania i wdrażania zabezpieczeń w systemach organizacyjnych, komponentach systemu lub usługach systemowych w oparciu o misję i wymagania biznesowe, wymagania dotyczące odporności i wiarygodności oraz wymagania dotyczące analizy i testowania. Systemy mogą

być podzielone na wiele podsystemów. Każdy podsystem w ramach systemu może zawierać jeden lub więcej modułów. Wysokopoziomowy projekt systemu jest wyrażony w kategoriach podsystemów oraz interfejsów między podsystemami zapewniających funkcje istotne dla bezpieczeństwa. Projekt niskopoziomowy systemu jest wyrażony w kategoriach modułów i interfejsów między modułami zapewniającymi funkcje istotne dla bezpieczeństwa. Dokumentacja projektowa i wdrożeniowa może zawierać informacje o producencie, wersji, numerze seryjnym, podpisie skrótu weryfikacyjnego, wykorzystanych bibliotekach oprogramowania, dacie zakupu lub pobrania oraz o sprzedawcy lub źródle pobrania. Kod źródłowy i schematy sprzętowe są określane, jako reprezentacja wdrożenia systemu.

Zabezpieczenia powiązane: Brak.

(3) PROCES NABYCIA | METODY, TECHNIKI I PRAKTYKI ROZWOJU

Żądanie od twórcy systemu, komponentu systemu lub usługi systemu wykazania zastosowania procesu cyklu życia systemu, który obejmuje:

(a) [***Realizacja: zdefiniowane przez organizację metody inżynierii systemów***]**;**

(b) [***Realizacja: zdefiniowane przez organizację*** [***Wybór (jeden lub więcej): metody inżynierii bezpieczeństwa systemów; ochrony prywatności***]]**; oraz**

(c) [***Realizacja: zdefiniowane przez organizację metody tworzenia oprogramowania; metody testowania, oceny, weryfikacji i certyfikacji; oraz procesy kontroli jakości***]**.**

Omówienie: Postępowanie oparte na cyklu życia systemu, który obejmuje najnowocześniejsze metody tworzenia oprogramowania, metody inżynierii systemów, metody inżynierii bezpieczeństwa i prywatności systemów oraz procesy kontroli jakości, pomaga zmniejszyć liczbę i dotkliwość błędów ukrytych w systemach, komponentach systemów i usługach systemowych. Zmniejszenie liczby i dotkliwości takich błędów zmniejsza liczbę podatności w tych systemach,

komponentach i usługach. Przejrzystość metod i technik wybieranych i wdrażanych przez twórców w zakresie inżynierii systemów, bezpieczeństwa systemów i ochrony prywatności, tworzenia oprogramowania, oceny komponentów i systemów oraz procesów kontroli jakości zapewnia zwiększony poziom pewności co do wiarygodności nabywanego systemu, komponentu systemu lub usługi systemowej.

Zabezpieczenia powiązane: Brak.

(4) PROCES NABYCIA | PRZYPISANIE KOMPONENTÓW DO SYSTEMÓW

[Wycofane: Włączone do CM-8(9)]

(5) PROCES NABYCIA | KONFIGURACJI SYSTEMÓW, KOMPONENTÓW I USŁUG

Wymaganie od producenta systemu, komponentu systemu lub usługi systemowej:

(a) Dostarczania systemu, komponentu lub usługi z zaimplementowanymi [***Realizacja: konfiguracje zabezpieczeń zdefiniowane przez organizację***]**; oraz**

(b) Domyślnego ustawiania konfiguracji przy każdej następnej ponownej instalacji lub aktualizacji systemu, komponentu lub usługi.

Omówienie: Przykłady konfiguracji zabezpieczeń obejmują domyślne ustawianie zabezpieczeń bazowych (np. konfigurację bazową U.S. Government Configuration Baseline - USGCB), techniczny przewodnik wdrażania zabezpieczeń (Security Technical Implementation Guides - STIGs) oraz wszelkie ograniczenia funkcji, portów, protokołów i usług. Charakterystyki zabezpieczeń mogą obejmować wymóg zmiany domyślnych haseł.

Zabezpieczenia powiązane: Brak.

(6) PROCES NABYCIA | KORZYSTANIE Z PRODUKTÓW ZAPEWNIAJĄCYCH BEZPIECZEŃSTWO INFORMACJI

(a) Stosowanie wyłącznie ogólnodostępnych produktów rządowych lub produktów komercyjnych pomyślnie ocenionych przez krajową władzę bezpieczeństwa w celu ochrony informacji niejawnych, jeżeli sieci wykorzystywane do przesyłania informacji są opatrzone niższym poziomem klauzuli tajności niż informacje przesyłane; oraz

(b) Upewnienie się, że produkty te zostały ocenione i/lub zatwierdzone przez krajową władzę bezpieczeństwa zgodnie z obowiązującymi przepisami i zatwierdzonymi procedurami.

Omówienie: W przypadku komercyjnych produktów informatycznych dostępnych w sprzedaży lub produktów informatycznych zapewniających bezpieczeństwo informacji, które są wykorzystywane do ochrony informacji niejawnych za pomocą środków kryptograficznych, istnieje wymóg stosowania zatwierdzonego przez krajową władzę bezpieczeństwa zarządzania kluczami.[92]

Zabezpieczenia powiązane: SC-8, SC-12, SC-13.

(7) PROCES NABYCIA | ZATWIERDZONE PROFILE OCHRONY

(a) Ograniczenie stosowania komercyjnie dostarczanych produktów technologii informatycznych zwiększających pewność informacji do tych produktów, które zostały pozytywnie ocenione pod kątem zgodności z profilem ochronnym zatwierdzonym przez Krajowe Partnerstwo na rzecz Zapewnienia Bezpieczeństwa Informacji (*ang. National Information Assurance partnership - NIAP*) dla danego rodzaju technologii, jeżeli taki profil istnieje; oraz

[92] Patrz: [NSA CSFC] – dotyczy rynku USA.

(b) Jeżeli dla danego rodzaju technologii nie istnieje profil ochronny zatwierdzony przez NIAP, a produkt informatyczny dostępny w handlu opiera się na funkcjach kryptograficznych służących egzekwowaniu polityki bezpieczeństwa, wymaganie, aby moduł kryptograficzny posiadał świadectwo FIPS (*ang. Federal Information Processing Standards*) lub został zatwierdzony przez NSA (*ang. National Security Agency*)[93] lub Krajową Władzę Bezpieczeństwa[94].

Omówienie: Patrz [NIAP CCEVS], aby uzyskać dodatkowe informacje na temat NIAP. Dodatkowe informacje na temat modułów kryptograficznych zatwierdzonych przez system FIPS można znaleźć w dokumencie [NIST CMVP].

Zabezpieczenia powiązane: IA-7, SC-12, SC-13.

(8) PROCES NABYCIA | PLAN CIĄGŁEGO MONITOROWANIA ZABEZPIECZEŃ

Wymaganie od twórcy systemu, komponentu systemu lub usługi systemowej opracowania planu ciągłego monitorowania skuteczności zabezpieczeń, który jest zgodny z programem ciągłego monitorowania organizacji.

Omówienie: Celem planów ciągłego monitorowania jest określenie, czy zaplanowane, wymagane i wdrożone zabezpieczenia w ramach systemu, komponentu systemu lub usługi systemowej są nadal skuteczne z upływem czasu w oparciu o nieuniknione zmiany, które zachodzą. Rozwijające się plany ciągłego monitorowania zawierają wystarczający poziom szczegółowości, aby informacje mogły być włączone do programów ciągłego monitorowania wdrożonych przez organizacje. Plany ciągłego monitorowania mogą zawierać rodzaje oceny zabezpieczeń i planowanych działań monitorujących, częstotliwość

[93] Dotyczy rynku USA.

[94] Zgodnie z ustawą o ochronie informacji niejawnych.

monitorowania zabezpieczeń oraz działania, które należy podjąć w przypadku, gdy zabezpieczenia nie spełniają swojej funkcji lub stają się nieefektywne.

Zabezpieczenia powiązane: CA-7.

(9) PROCES NABYCIA | FUNKCJE, PORTY, PROTOKOŁY / USŁUGI

Wymaganie od twórcy systemu, komponentu systemu lub usługi systemowej określenia funkcji, portów, protokołów i usług przeznaczonych do użytku organizacyjnego.

Omówienie: Identyfikacja funkcji, portów, protokołów i usług we wczesnym etapie cyklu życia systemu (np. podczas początkowych etapów definiowania wymagań i projektowania) pozwala organizacjom wpływać na projekt systemu, komponentu systemu lub usługi systemowej. Takie wczesne zaangażowanie w cykl życia rozwoju systemu pomaga organizacjom uniknąć lub zminimalizować wykorzystanie funkcji, portów, protokołów lub usług, które stwarzają niepotrzebnie wysokie ryzyko, a także zrozumieć korzyści związane z blokowaniem określonych portów, protokołów lub usług albo wymaganiem od dostawców usług systemowych, przestrzegania tych zasad. Wczesna identyfikacja funkcji, portów, protokołów i usług pozwala na uniknięcie kosztownej modernizacji zabezpieczenia po wdrożeniu systemu, komponentu lub usługi systemowej. Zabezpieczenie SA-9 opisuje wymagania stawiane zewnętrznym usługom systemowym. Organizacje identyfikują, które funkcje, porty, protokoły i usługi są dostarczane ze źródeł zewnętrznych.

Zabezpieczenia powiązane: CM-7, SA-9.

(10) PROCES NABYCIA | WYKORZYSTANIE ZATWIERDZONYCH PRODUKTÓW

Stosowanie wyłącznie produkty informatyczne z listy produktów zatwierdzonych przez [*Realizacja: zgodnie z wewnętrznymi regulacjami organizacji lub wymaganiami ustalonymi przepisem prawa*] do celów

weryfikacji tożsamości osobistej zaimplementowanych w organizacyjnych systemach informatycznych.

Omówienie:[95] Produkty znajdujące się na liście produktów zatwierdzonych przez FIPS 201 spełniają wymagania NIST dotyczące weryfikacji tożsamości osobistej (*ang. Personal Identity Verification - PIV*) of Federal Employees and Contractors. Karty PIV są wykorzystywane do uwierzytelniania wieloskładnikowego w systemach i organizacjach.

Zabezpieczenia powiązane: IA-2, IA-8, PM-9.

(11) PROCES NABYCIA | SYSTEM DOKUMENTOWANIA

Uwzględnianie [***Realizacja: wymogi ustawy o ochronie danych określone przez organizację***] ***w*** **umowie przejęcia dotyczącej funkcjonowania systemu ewidencji w imieniu organizacji w celu realizacji misji lub funkcji organizacji.**

Omówienie: Jeżeli na mocy umowy organizacja przewiduje prowadzenie systemu ewidencji w celu realizacji misji lub funkcji organizacji, to organizacja, zgodnie ze swoimi uprawnieniami, powoduje, że wymagania [RODO] mają zastosowanie do systemu dokumentacji.

Zabezpieczenia powiązane: PT-6.

(12) PROCES NABYCIA | WŁASNOŚĆ DANYCH

(a) Uwzględnienie w umowie nabycia wymogów dotyczących własności danych organizacyjnych; oraz

(b) Wymaganie usunięcia wszystkich danych z systemu wykonawcy i zwrócenia ich do organizacji w ciągu [***Realizacja: ramy czasowe określone przez organizację***]**.**

[95] Omówienie dotyczy rynku USA.

Omówienie: Wykonawcy obsługujący system zawierający dane należące do organizacji inicjującej umowę, posiadają zasady i procedury umożliwiające usunięcie danych z ich systemów i/lub zwrócenie danych w terminie określonym w umowie.

Zabezpieczenia powiązane: Brak.

Referencje: [PRIVACT], [OMB A-130], [ISO 15408-1], [ISO 15408-2], [ISO 15408-3], [FIPS 140-3], [FIPS 201-2], [NIST SP 800-35], [NIST SP 800-37], [NIST SP 800-70], [NIST SP 800-73-4], [NIST SP 800-137], [NIST SP 800-160-1], [NIST SP 800-161], [IR 7539], [IR 7622], [IR 7676], [IR 7870], [IR 8062], [NIAP CCEVS], [NSA CSFC], [ISO 29148].

SA-5 DOKUMENTACJA SYSTEMU

Zabezpieczenie podstawowe:

a. Uzyskanie lub opracowanie dokumentacji administratora systemu, komponentu systemu lub usługi systemowej, która opisuje:

   1. Bezpieczną konfigurację, instalację i obsługę systemu, komponentu lub uslugi;

   2. Skuteczne wykorzystanie i utrzymanie funkcji i mechanizmów bezpieczeństwa i ochrony prywatności; oraz

   3. Znane podatności dotyczące konfiguracji i korzystania z funkcji administracyjnych lub uprzywilejowanych;

b. Uzyskanie lub opracowanie dokumentacji użytkownika systemu, komponentu systemu lub usługi systemowej, która opisuje:

   1. Dostępne dla użytkownika funkcje i mechanizmy bezpieczeństwa i ochrony prywatności oraz sposób efektywnego wykorzystania tych funkcji i mechanizmów;

   2. Metody interakcji z użytkownikiem, które umożliwiają mu bezpieczniejsze korzystanie z systemu, komponentu lub usługi oraz chronią prywatność; oraz

   3. Obowiązki użytkownika w zakresie utrzymania bezpieczeństwa systemu, komponentu lub usługi oraz prywatności osób;

c. Dokumentuje próby uzyskania dokumentacji systemu, komponentu systemu lub usługi systemowej, gdy taka dokumentacja jest niedostępna lub nie istnieje i w odpowiedzi podejmuje [*Realizacja: działania zdefiniowane przez organizację*]; oraz

d. Dystrybuuje dokumentację do [*Realizacja: personel określony przez organizację lub role*].

Omówienie: Dokumentacja systemu pomaga pracownikom zrozumieć proces wdrażania i działania zabezpieczeń. Organizacje rozważają ustanowienie konkretnych

środków w celu określenia jakości i kompletności dostarczanych treści. Dokumentacja systemowa może być wykorzystywana do wspierania zarządzania ryzykiem w łańcuchu dostaw, reagowania na incydenty i innych funkcji. Do personelu lub ról, które wymagają dokumentacji, należą właściciele systemu, personel ds. bezpieczeństwa systemu oraz administratorzy systemu. Próby uzyskania dokumentacji obejmują kontaktowanie się z producentami lub dostawcami oraz przeszukiwanie stron internetowych. Brak możliwości uzyskania dokumentacji może wynikać z wieku systemu lub komponentu lub z braku wsparcia ze strony programistów i wykonawców. W przypadku, gdy nie można uzyskać dokumentacji, organizacje mogą być zmuszone do jej odtworzenia, jeśli jest ona niezbędna do wdrożenia lub działania zabezpieczeń. Ochrona przewidziana dla dokumentacji jest współmierna do kategorii bezpieczeństwa lub klasyfikacji systemu. Dokumentacja, która dotyczy podatności systemu na zagrożenia, może wymagać zwiększonego poziomu ochrony. Bezpieczne działanie systemu obejmuje początkowe uruchomienie systemu oraz wznowienie bezpiecznego funkcjonowania systemu po przerwie w jego działaniu.

Zabezpieczenia powiązane: CM-4, CM-6, CM-7, CM-8, PL-2, PL-4, PL-8, PS-2, SA-3, SA-4, SA-8, SA-9, SA-10, SA-11, SA-15, SA-16, SA-17, SI-12, SR-3.

Zabezpieczenia rozszerzone:

(1) DOKUMENTACJA SYSTEMU | WŁAŚCIWOŚCI FUNKCJONALNE ZABEZPIECZEŃ

[Wycofane: Włączone do SA-4(1)].

(2) DOKUMENTACJA SYSTEMU | BEZPIECZEŃSTWO INTERFEJSÓW SYSTEMU ZEWNĘTRZNEGO

[Wycofane: Włączone do SA-4(2)]

(3) DOKUMENTACJA SYSTEMU | PROJEKTOWANIE WYSOKOPOZIOMOWE

[Wycofane: Włączone do SA-4(2)]

(4) DOKUMENTACJA SYSTEMU | PROJEKTOWANIE NISKOPOZIOMOWE

[Wycofane: Włączone do SA-4(2)]

(5) DOKUMENTACJA SYSTEMU | KOD ŹRÓDŁOWY

[Wycofane: Włączone do SA-4(2)]

Referencje: [NIST SP 800-160-1].

SA-6 OGRANICZENIA W UŻYCIU OPROGRAMOWANIA

[Wycofane: Włączone do CM-10 i SI-7].

SA-7 OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA

[Wycofane: Włączone do CM-11 i SI-7].

SA-8 ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Zabezpieczenie podstawowe: Stosowanie następujących zasad bezpieczeństwa systemów i inżynierii prywatności w specyfikacji, projektowaniu, rozwoju, wdrażaniu i modyfikacji systemu i jego komponentów: [*Realizacja: określone przez organizację zasady bezpieczeństwa systemów i inżynierii prywatności*].

Omówienie: Zasady bezpieczeństwa systemów i inżynierii prywatności są ściśle związane i wdrażane w całym cyklu życia systemu (patrz zabezpieczenie SA-3). Organizacje mogą stosować zasady dotyczące bezpieczeństwa systemów i inżynierii prywatności w odniesieniu do nowo opracowywanych systemów lub do systemów poddawanych modernizacji. W przypadku istniejących systemów organizacje stosują zasady bezpieczeństwa i inżynierii prywatności do aktualizacji i modyfikacji systemów w zakresie, w jakim jest to możliwe, biorąc pod uwagę obecny stan sprzętu, aplikacji i oprogramowania układowego w tych systemach.

Zastosowanie zasad bezpieczeństwa systemów i inżynierii prywatności pomaga organizacjom rozwijać wiarygodne, bezpieczne i odporne systemy oraz zmniejsza podatność na zakłócenia, zagrożenia, niebezpieczeństwa i powstawanie problemów związanych z prywatnością osób. Przykłady zasad inżynierii bezpieczeństwa systemów obejmują: opracowanie zabezpieczeń warstwowych; ustanowienie polityki bezpieczeństwa i ochrony prywatności, architektury i zabezpieczeń jako podstawy projektowania i rozwoju; włączenie wymagań dotyczących bezpieczeństwa i ochrony prywatności do cyklu życia systemu; wyznaczenie fizycznych i logicznych granic bezpieczeństwa; zapewnienie szkoleń programistów w zakresie budowania bezpiecznego oprogramowania; dostosowanie zabezpieczeń do potrzeb organizacji; oraz prowadzenie modelowania zagrożeń w celu identyfikacji przypadków użycia, agentów zagrożeń, wektorów i wzorców ataku, wzorców projektowych oraz mechanizmów zabezpieczeń niezbędnych do ograniczania ryzyka.

Organizacje, które stosują koncepcje i zasady bezpieczeństwa systemów i inżynierii prywatności, mogą wspomagać rozwój wiarygodnych, bezpiecznych systemów,

komponentów systemu i usług systemowych; ograniczyć ryzyko do akceptowalnego poziomu oraz podejmować świadome decyzje dotyczące zarządzania ryzykiem. Zasady inżynierii bezpieczeństwa systemu mogą być również wykorzystywane do ochrony przed niektórymi rodzajami ryzyka w łańcuchu dostaw, w tym do włączania do projektu sprzętu odpornego na manipulacje.

Zabezpieczenia powiązane: PL-8, PM-7, RA-2, RA-3, RA-9, SA-3, SA-4, SA-15, SA-17, SA-20, SC-2, SC-3, SC- 32, SC-39, SR-2, SR-3 , SR-5.

Zabezpieczenia rozszerzone:

(1) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | PRZEJRZYSTE ABSTRAKCJE

Wdrożenie zasady projektowania bezpieczeństwa w postaci przejrzystych abstrakcji.

Omówienie: Zasada przejrzystych abstrakcji mówi, że system posiada proste, dobrze zdefiniowane interfejsy i funkcje, które zapewniają spójny i intuicyjny wgląd w dane i sposób zarządzania nimi. Przejrzystość, prostota, konieczność i wystarczalność interfejsów systemu - w połączeniu z precyzyjnym określeniem ich funkcjonalnego zachowania - sprzyjają łatwości analizy, inspekcji i testowania, a także poprawnemu i bezpiecznemu korzystaniu z systemu. Przejrzystość abstrakcji jest subiektywna. Przykłady, które odzwierciedlają zastosowanie tej zasady obejmują unikanie zbędnych, nieużywanych interfejsów, maskowanie informacji oraz unikanie semantycznego przeciążania interfejsów lub ich parametrów. Maskowanie informacji (tj. programowanie niezależne od sposobu odwzorowywania) jest dziedziną projektowania stosowaną w celu zapewnienia, że wewnętrzna reprezentacja informacji w jednym z komponentów systemu nie jest widoczna dla innego komponentu systemu wywołującego lub przywołującego

pierwszy komponent tak, że na opublikowaną abstrakcję nie ma wpływu sposób, w jaki dane mogą być zarządzane wewnętrznie.

Zabezpieczenia powiązane: Brak.

(2) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | MINIMALIZACJA MECHANIZMÓW WSPÓLNYCH

Wdrożenie zasady minimalizacji wspólnych mechanizmów bezpieczeństwa w [***Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację***]**.**

Omówienie: Zasada minimalizacji mechanizmów wspólnych mówi, że ilość mechanizmów wspólnych dla więcej niż jednego użytkownika i zależnych od wszystkich użytkowników jest minimalizowana [POPEK74]. Minimalizacja mechanizmów oznacza, że różne komponenty systemu powstrzymują się od używania tego samego mechanizmu w celu uzyskania dostępu do zasobu systemowego. Każdy współdzielony mechanizm (szczególnie mechanizm zawierający współdzielone zmienne) stanowi potencjalną ścieżkę informacji pomiędzy użytkownikami i jest projektowany z uwagą, aby nie zagrażał bezpieczeństwu [SALTZER75]. Implementacja zasady minimalizacji mechanizmu wspólnego pozwala ograniczyć negatywne konsekwencje współdzielenia zasobów systemu przez różne programy. Pojedynczy program, który naruszy współdzielony stan (w tym współdzielone zmienne) może potencjalnie naruszyć inne programy, które są zależne od tego stanu. Zasada minimalizacji mechanizmu wspólnego wspiera również zasadę przejrzystości projektu i odnosi się do kwestii ukrytych kanałów przechowywania danych [LAMPSON73].

Zabezpieczenia powiązane: Brak.

(3) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | MODUŁOWOŚĆ I WARSTWOWOŚĆ

Wdrożenie zasad projektowania bezpieczeństwa modułowego i warstwowego w [***Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację***]**.**

Omówienie: Zasady modułowości i warstwowości są fundamentalne dla wszystkich dziedzin inżynierii systemowej. Modułowość i warstwowość wynikające z dekompozycji funkcjonalnej są skuteczne w zarządzaniu złożonością systemu poprzez umożliwienie zrozumienia jego struktury. Modułowa dekompozycja, czyli udoskonalanie w projektowaniu systemów, jest wyzwaniem i jest niepodatna na ogólne formułowanie zasad. Modułowość służy do wyodrębnienia funkcji i powiązanych struktur danych w dokładnie zdefiniowane jednostki logiczne. Warstwowość pozwala na lepsze zrozumienie relacji pomiędzy tymi jednostkami, dzięki czemu zależności są jasne i można uniknąć niepożądanej złożoności. Zasada modularności w projektowaniu bezpieczeństwa rozszerza modułową strukturę funkcjonalną o kwestie związane z zaufaniem, wiarygodnością, przywilejami i polityką bezpieczeństwa. Modułowa dekompozycja uwzględniająca bezpieczeństwo obejmuje przypisanie polityk do systemów w sieci, rozdzielenie aplikacji systemowych na procesy z odrębnymi przestrzeniami adresowymi, przypisanie polityk systemowych do warstw oraz rozdzielenie procesów na podmioty z odrębnymi przywilejami opartymi na wspieranych sprzętowo domenach przywilejów.

Zabezpieczenia powiązane: SC-2, SC-3.

(4) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | UPORZĄDKOWANIE ZALEŻNOŚCI POMIĘDZY SEGMENTAMI SYSTEMU

Wdrożenie zasady bezpiecznego projektowania uporządkowanych zależności pomiędzy segmentami sieci w [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację].

Omówienie: Zasada uporządkowanych zależności pomiędzy segmentami sieci mówi, że synchronizacja, wywoływanie i inne zależności w systemie są częściowo uporządkowane. Podstawowym pojęciem w projektowaniu systemu jest układ warstwowy, w którym system jest zorganizowany w dobrze zdefiniowane, funkcjonalnie powiązane moduły lub komponenty. Warstwy są uporządkowane liniowo w odniesieniu do zależności międzywarstwowych w taki sposób, że warstwy wyższe są zależne od warstw niższych Zapewnienie funkcjonalności wyższym warstwom może spowodować, że niektóre warstwy będą autonomiczne i nie będą zależne od warstw niższych. Podczas gdy częściowe uporządkowanie wszystkich funkcji w danym systemie może nie być możliwe, to jeśli zależności kołowe są ograniczone do występowania w obrębie warstw, nieodłączne problemy związane z cyklicznością mogą być łatwiejsze do zarządzania. Częściowo uporządkowane zależności i warstwowość systemu w znacznym stopniu przyczyniają się do prostoty i spójności projektu systemu. Częściowo uporządkowane zależności ułatwiają również testowanie i analizę systemu.

Zabezpieczenia powiązane: Brak.

(5) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | DOSTĘP Z EFEKTYWNĄ MEDIACJĄ

Wdrożenie zasady projektowania bezpieczeństwa dostępu z efektywną mediacją w [***Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację***]**.**

Omówienie: Zasada skutecznego dostępu za pośrednictwem mediacji stanowi, że mechanizmy egzekwowania polityki wykorzystują najmniej powszechny dostępny mechanizm, spełniając jednocześnie wymagania zainteresowanych stron w ramach określonych ograniczeń. Mediacja w dostępie do zasobów systemowych (tj. procesora, pamięci, urządzeń, portów komunikacyjnych, usług, infrastruktury, danych i informacji) jest często dominującą funkcją bezpieczeństwa systemów. Umożliwia to również ochronę funkcjonalności

zapewnianych interesariuszom przez system. Pośredniczenie w dostępie do zasobów może skutkować ograniczeniem wydajności, jeśli system nie jest zaprojektowany prawidłowo. Na przykład, dzięki zastosowaniu mechanizmów sprzętowych można uzyskać efektywnie wyreżyserowany dostęp. Po uzyskaniu dostępu do zasobu niskiego poziomu, takiego jak pamięć, mechanizmy ochrony sprzętowej mogą zapewnić, że dostęp poza ustalone granice nie będzie miał miejsca.

Zabezpieczenia powiązane: AC-25.

(6) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | MINIMALIZACJA WSPÓŁUŻYTKOWANIA

Wdrożenie zasady projektowania bezpieczeństwa polegającej na minimalizacji współużytkowania w [***Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację***]**.**

Omówienie: Zasada minimalizacji współużytkowania mówi, że żaden zasób komputerowy nie jest współdzielony pomiędzy komponentami systemu (np. obiekty, procesy, funkcje) chyba, że jest to absolutnie konieczne. Zminimalizowane współużytkowanie pomaga uprościć projektowanie i wdrażanie systemu. W celu ochrony zasobów domeny użytkownika przed arbitralnie aktywnymi podmiotami, żadne zasoby nie są współdzielone, chyba że takie współdzielenie zostało wyraźnie zażądane i przyznane. Potrzeba współużytkowania zasobów może być motywowana zasadą minimalizacji mechanizmu wspólnego w przypadku podmiotów wewnętrznych lub wynikać z wymagań interesariuszy. Dzielenie się zasobami wewnętrznymi jest jednak starannie zaprojektowane, aby uniknąć problemów z wydajnością i ukrytym przechowywaniem oraz kanałami czasowymi. Dzielenie się danymi i informacjami za pośrednictwem mechanizmu wspólnego może zwiększyć podatność danych i informacji na nieautoryzowany dostęp, ujawnienie, wykorzystanie lub modyfikację oraz może mieć negatywny wpływ na wydajność

systemu. W celu zminimalizowania współdzielenia wywołanego przez mechanizmy wspólne, takie mechanizmy mogą być zaprojektowane jako rezydualne lub zwirtualizowane, aby zachować separację. Ponadto, wykorzystanie danych globalnych do współdzielenia informacji jest dokładnie sprawdzane. Brak hermetyzacji może zaciemniać relacje pomiędzy współdzielonymi jednostkami.

Zabezpieczenia powiązane: SC-31.

(7) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | ZMNIEJSZONA ZŁOŻONOŚĆ

Wdrożenie zasady projektowania bezpieczeństwa polegającej na zmniejszeniu złożoności w [Realizacja: zdefiniowane przez organizację systemy lub komponenty systemu].

Omówienie: Zasada zmniejszonej złożoności mówi, że projekt systemu jest tak uproszczony i minimalistyczny, jak to tylko możliwe. Minimalna i uproszczona konstrukcja jest bardziej zrozumiała, bardziej analizowalna i mniej podatna na błędy. Zasada zmniejszonej złożoności odnosi się do każdego aspektu systemu, ale ma szczególne znaczenie dla bezpieczeństwa ze względu na różne analizy przeprowadzane w celu uzyskania dowodów na istnienie właściwości systemu związanych z bezpieczeństwem. Aby takie analizy zakończyły się sukcesem, niezbędna jest minimalna i prosta konstrukcja. Zastosowanie zasady zmniejszonej złożoności przyczynia się do tego, że twórcy systemu są w stanie zrozumieć poprawność i kompletność funkcji bezpieczeństwa systemu. Ułatwia to również identyfikację potencjalnych luk w zabezpieczeniach. Konsekwencją zmniejszonej złożoności jest to, że prostota systemu jest bezpośrednio związana z liczbą podatności, które będzie zawierał, czyli prostsze systemy zawierają mniej podatności. Korzyścią ze zmniejszonej złożoności jest to, że łatwiej jest zrozumieć, czy zamierzona polityka bezpieczeństwa została uwzględniona w projekcie systemu, i że prawdopodobnie mniej luk zostanie wprowadzonych podczas opracowywania inżynierii. Dodatkową korzyścią jest to, że każdy taki wniosek

dotyczący poprawności, kompletności i istnienia podatności może zostać wyciągnięty z większym stopniem pewności w przeciwieństwie do wniosków wyciągniętych w sytuacjach, gdy projekt systemu jest z natury bardziej złożony. Przejście ze starszych technologii na nowsze (np. przejście z IPv4 na IPv6) może wymagać jednoczesnego wdrożenia starszych i nowszych technologii w okresie przejściowym. Może to spowodować tymczasowe zwiększenie złożoności systemu w okresie przejściowym.

Zabezpieczenia powiązane: Brak.

(8) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | BEZPIECZNA EWOLUCJA

Wdrożenie zasady bezpiecznej ewolucji w [***Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację***]**.**

Omówienie: Zasada bezpiecznej ewolucji stanowi, że system jest rozwijany w celu umożliwienia utrzymania jego właściwości bezpieczeństwa w przypadku zmian w strukturze, interfejsach, wzajemnych połączeniach (tj. architekturze systemu), funkcjonalności lub konfiguracji (tj. egzekwowaniu polityki bezpieczeństwa). Zmiany obejmują nowe, rozszerzone lub unowocześnione możliwości systemu, działania konserwacyjne i podtrzymujące oraz rekonfigurację. Mimo, że nie jest możliwe zaplanowanie każdego aspektu ewolucji systemu, unowocześnienia i zmiany systemu można przewidzieć poprzez analizę strategicznego kierunku misji lub działalności, przewidywane zmiany w środowisku zagrożeń oraz przewidywane potrzeby w zakresie utrzymania i konserwacji. Nierealistyczne jest oczekiwanie, że złożone systemy pozostaną bezpieczne w kontekstach nieprzewidzianych podczas ich opracowywania, niezależnie od tego, czy takie konteksty są związane ze środowiskiem operacyjnym, czy z użytkowaniem. System może być bezpieczny w niektórych nowych kontekstach, ale nie ma gwarancji, że jego pojawiające się zachowanie będzie zawsze bezpieczne. Łatwiej jest wbudować wiarygodność w system od samego początku i wynika z tego, że

utrzymanie wiarygodności systemu wymaga planowania zmian, a nie dostosowywania się w sposób doraźny lub nie metodyczny. Korzyści płynące z tej zasady obejmują zmniejszenie wydatków dostawcy związanych z cyklem życia, zmniejszenie kosztów posiadania, poprawę bezpieczeństwa systemu, bardziej efektywne zarządzanie ryzykiem bezpieczeństwa oraz zmniejszenie niepewności ryzyka.

Zabezpieczenia powiązane: CM-3.

(9) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | ZAUFANE KOMPONENTY

Implementacja zasady projektowania bezpieczeństwa z wykorzystaniem zaufanych komponentów w [Realizacja: zdefiniowane przez organizację systemy lub komponenty systemu].

Omówienie: Zasada zaufanych komponentów zakłada, że komponent jest godny zaufania przynajmniej na poziomie współmiernym do zależności bezpieczeństwa, które obsługuje (tzn. na ile inne komponenty są godne zaufania). Zasada ta umożliwia zestawianie komponentów w taki sposób, aby wiarygodność nie została przypadkowo zmniejszona, a zaufanie nie zostało w konsekwencji źle rozplanowane. Ostatecznie, zasada ta wymaga pewnej metryki, dzięki której zaufanie do komponentu i wiarygodność komponentu mogą być mierzone tą samą abstrakcyjną skalą. Zasada zaufanych komponentów jest szczególnie istotna przy rozpatrywaniu systemów i komponentów, w których występują złożone łańcuchy zależności od stopnia zaufania. Zależność od poziomu zaufania jest również określana jako relacja zaufania i mogą istnieć łańcuchy relacji zaufania.

Zasada zaufanych komponentów odnosi się również do komponentu złożonego, który składa się z subkomponentów (np. podsystemu), które mogą mieć różny poziom wiarygodności. Konserwatywne założenie mówi, że wiarygodność komponentu złożonego jest taka, jak wiarygodność jego najmniej godnego zaufania podkomponentu. Może być możliwe przedstawienie uzasadnienia

inżynierii bezpieczeństwa, że wiarygodność danego komponentu złożonego jest większa niż konserwatywne założenie. Jednakże każde takie uzasadnienie odzwierciedla logiczne rozumowanie oparte na jasnym określeniu celów wiarygodności, jak również na odpowiednich i wiarygodnych dowodach. Wiarygodność komponentu złożonego to nie to samo, co zwiększone zastosowanie warstwowej obrony dogłębnej w ramach komponentu lub replikacja komponentów. Techniki "defense-in-depth" nie zwiększają wiarygodności całości ponad wiarygodność najmniej godnego zaufania komponentu.

Zabezpieczenia powiązane: Brak.

(10) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | ZAUFANIE HIERARCHICZNE

Wdrożenie zasady projektowania bezpieczeństwa polegającej na hierarchicznym zaufaniu do [*Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację*].

Omówienie: Zasada hierarchicznego zaufania do komponentów opiera się na zasadzie zaufanych komponentów i stwierdza, że zależności bezpieczeństwa w systemie będą tworzyły częściowe uporządkowanie, jeśli zachowają zasadę zaufanych komponentów. Uporządkowanie częściowe stanowi podstawę rozumowania wiarygodności lub przypadek asekuracyjny (argument asekuracyjny) przy komponowaniu bezpiecznego systemu na bazie różnorodnie godnych zaufania komponentów. Aby przeanalizować system składający się z niejednorodnie godnych zaufania komponentów pod kątem jego wiarygodności, konieczne jest wyeliminowanie cyklicznych zależności w odniesieniu do wiarygodności. Jeżeli bardziej wiarygodny komponent znajdujący się w niższej warstwie systemu byłby zależny od mniej wiarygodnego komponentu znajdującego się w wyższej warstwie, to w efekcie komponenty te znalazłyby się w tej samej "mniej wiarygodnej" klasie równoważności według

zasady zaufanych komponentów. Relacje zaufania, lub łańcuchy zaufania, mogą mieć różne postacie. Na przykład, certyfikat główny w hierarchii certyfikatów jest najbardziej zaufanym węzłem w hierarchii, podczas gdy jej poszczególne elementy mogą być węzłami najmniej godnymi zaufania. Inny przykład występuje w warstwowym systemie o wysokim poziomie zaufania, w którym jądro zabezpieczeń (wraz z jego bazą sprzętową), znajdujące się w najniższej warstwie systemu, jest najbardziej godnym zaufania komponentem. Zasada hierarchicznego zaufania nie zabrania jednak stosowania komponentów o zbyt dużym zaufaniu. W systemie o niskim poziomie zaufania mogą wystąpić przypadki, w których uzasadnione jest zastosowanie komponentu o wysokim poziomie zaufania zamiast komponentu mniej godnego zaufania (np. ze względu na dostępność lub inny czynnik wpływający na koszty i korzyści). W takim przypadku zależność wysoce godnego zaufania komponentu od komponentu mniej godnego zaufania nie pogarsza wiarygodności systemu o niskim poziomie zaufania.

Zabezpieczenia powiązane: Brak.

(11) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | ODWROTNY PRÓG MODYFIKACJI

Wdrożenie zasady projektowania bezpieczeństwa opartej na odwrotnym progu modyfikacji w [*Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację*].

Omówienie: Zasada odwrotnego progu modyfikacji opiera się na zasadzie zaufanych komponentów oraz zasadzie hierarchicznego zaufania i stwierdza, że stopień ochrony zapewnianej komponentowi jest współmierny do jego wiarygodności. Wraz ze wzrostem zaufania pokładanego w komponencie wzrasta również w tym samym stopniu ochrona przed nieuprawnioną modyfikacją komponentu. Ochrona przed nieautoryzowaną modyfikacją może mieć formę samoochrony komponentu i jego wrodzonej wiarygodności lub może wynikać

z ochrony zapewnionej komponentowi przez inne elementy lub atrybuty architektury bezpieczeństwa (w tym ochrony w środowisku działania).

Zabezpieczenia powiązane: Brak.

(12) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | OCHRONA HIERARCHICZNA

Wdrożenie zasady projektowania bezpieczeństwa opartej na ochronie hierarchicznej w [*Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację*].

Omówienie: Zasada hierarchicznej ochrony mówi, że komponent nie musi być chroniony przed bardziej zaufanymi komponentami. W sytuacji, gdy najbardziej zaufany komponent jest zdegenerowany, to chroni on siebie przed wszystkimi innymi komponentami. Na przykład, jeśli jądro systemu operacyjnego jest uważane za najbardziej godny zaufania komponent w systemie, to chroni się ono przed wszystkimi niezaufanymi aplikacjami, które obsługuje, ale aplikacje, odwrotnie, nie muszą chronić się przed jądrem. Wiarygodność użytkowników jest czynnikiem decydującym o zastosowaniu zasady ochrony hierarchicznej. Zaufany system nie musi chronić się przed równie godnym zaufania użytkownikiem, co odzwierciedla wykorzystanie niezaufanych systemów w środowiskach o "wysokim poziomie zaufania", gdzie użytkownicy są wysoce godni zaufania i gdzie inne zabezpieczenia są niewystarczające.

Zabezpieczenia powiązane: Brak.

(13) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | MINIMALIZACJA ELEMENTÓW BEZPIECZEŃSTWA

Wdrożenie zasady projektowania bezpieczeństwa opartej na minimalizacji elementów bezpieczeństwa w [*Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację*].

Omówienie: Zasada minimalizacji elementów bezpieczeństwa stanowi, że system nie posiada zewnętrznych, zaufanych elementów. Zasada minimalizacji elementów bezpieczeństwa ma dwa aspekty: ogólny koszt analizy bezpieczeństwa oraz złożoność analizy bezpieczeństwa. Zaufane komponenty są na ogół bardziej kosztowne do zbudowania i wdrożenia ze względu na zwiększony rygor procesów rozwojowych. Zaufane komponenty wymagają większej analizy bezpieczeństwa, aby określić ich wiarygodność. Dlatego też, aby obniżyć koszty i zmniejszyć złożoność analizy bezpieczeństwa, system zawiera tak mało wiarygodnych komponentów, jak to tylko możliwe. Analiza interakcji zaufanych komponentów z innymi komponentami systemu jest jednym z najważniejszych aspektów weryfikacji bezpieczeństwa systemu. Jeśli interakcje pomiędzy komponentami są nadmiernie złożone, bezpieczeństwo systemu będzie również trudniejsze do sprawdzenia niż w przypadku, gdy wewnętrzne relacje zaufania są proste i starannie skonstruowane. Ogólnie rzecz biorąc, mniejsza liczba zaufanych komponentów skutkuje mniejszą liczbą wewnętrznych relacji zaufania i prostszym systemem.

Zabezpieczenia powiązane: Brak.

(14) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | ZASADA NAJMNIEJSZEGO UPRZYWILEJOWANIA

Wdrożenie zasady projektowania bezpieczeństwa opartej na najmniejszych uprawnieniach w [***Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację***]**.**

Omówienie: Zasada najmniejszego uprzywilejowania stanowi, że każdemu komponentowi systemu przydzielane są uprawnienia wystarczające do realizacji jego określonych funkcji, jednakże nie szersze. Stosowanie zasady najmniejszego uprzywilejowania ogranicza zakres działania komponentu, co ma dwa pożądane aspekty: wpływ awarii, uszkodzenia lub niewłaściwego użycia komponentu na bezpieczeństwo będzie zminimalizowany, a analiza bezpieczeństwa komponentu

zostanie uproszczona. Zasada najmniejszego uprzywilejowania jest powszechnie obowiązującą zasadą, która jest odzwierciedlona we wszystkich aspektach projektowania bezpiecznego systemu. Interfejsy wykorzystywane do uruchamiania funkcji komponentu są dostępne tylko dla określonych podzbiorów użytkowników, a konstrukcja komponentu wspiera wystarczająco precyzyjną granulację podziału uprawnień. Na przykład, w przypadku mechanizmu audytu, może istnieć interfejs dla menedżera audytu, który konfiguruje ustawienia audytu; interfejs dla operatora audytu, który zapewnia, że dane audytu są bezpiecznie gromadzone i przechowywane; i wreszcie jeszcze jeden interfejs dla recenzenta audytu, który ma jedynie potrzebę przeglądania danych audytu, które zostały zgromadzone, ale nie ma potrzeby wykonywania operacji na tych danych.

Oprócz stosowania tego rozwiązania do interfejsu systemu, zasada najmniejszego uprzywilejowania może być wykorzystywana jako zasada nadrzędna dla wewnętrznej struktury samego systemu. Jednym z wewnętrznych aspektów najmniejszego uprzywilejowania jest konstruowanie modułów w taki sposób, aby tylko elementy hermetyzowane przez moduł były bezpośrednio obsługiwane przez funkcje działające w module. Elementy zewnętrzne w stosunku do modułu, na które może mieć wpływ działanie modułu, są pośrednio dostępne poprzez interakcję (np. poprzez wywołanie funkcji) z modułem, który zawiera te elementy. Innym aspektem wewnętrznego najmniejszego uprzywilejowania jest fakt, że zakres danego modułu lub komponentu obejmuje tylko te elementy systemu, które są niezbędne dla jego funkcjonalności, a tryby dostępu do elementów (np. odczyt, zapis) są zminimalizowane.

Zabezpieczenia powiązane: AC-6, CM-7.

(15) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | PREDYKAT ZEZWOLEŃ

Wdrożenie zasady projektowania bezpieczeństwa opartej na predykacie zezwoleń w [***Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację***]**.**

Omówienie: Zasada uprawnień predykatowych stwierdza, że projektanci systemów rozważają wymaganie od wielu uprawnionych podmiotów dostarczenia zgody przed wykonaniem wysoce krytycznej operacji lub uzyskaniem dostępu do wysoce wrażliwych danych, informacji lub zasobów. [SALTZER75] oryginalnie nazwał predykat zezwolenia separacją przywilejów. Jest to również odpowiednik separacji obowiązków. Podział przywilejów pomiędzy wiele stron zmniejsza prawdopodobieństwo nadużyć i stanowi zabezpieczenie, że żaden pojedynczy wypadek, oszustwo lub naruszenie zaufania nie jest wystarczające, aby umożliwić nieodwracalne działanie, które może prowadzić do znacząco szkodliwych skutków. Warianty konstrukcyjne takiego mechanizmu mogą wymagać równoczesnego działania (np. odpalenie broni jądrowej wymaga, aby dwie odmienne upoważnione osoby wydały prawidłowe polecenie w niewielkim odstępie czasu) lub sekwencji operacji, w której każde kolejne działanie jest umożliwione przez jakieś wcześniejsze działanie, ale żadna osoba nie jest w stanie umożliwić więcej niż jednego działania.

Zabezpieczenia powiązane: AC-5.

(16) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | SAMOISTNA WIARYGODNOŚĆ

Wdrożenie zasady projektowania bezpieczeństwa polegającej na samoistnej wiarygodności w [***Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację***]**.**

Omówienie: Zasada samoistnej wiarygodności stanowi, że systemy minimalizują zależność od innych systemów pod względem własnej wiarygodności. System jest

domyślnie wiarygodny, a każde połączenie z podmiotem zewnętrznym jest wykorzystywane do uzupełnienia jego funkcji. Gdyby od systemu wymagano utrzymywania połączenia z innym podmiotem zewnętrznym w celu utrzymania jego wiarygodności, system ten byłby podatny na szkodliwe i nieszkodliwe zagrożenia, które mogłyby doprowadzić do utraty lub pogorszenia tego połączenia. Korzyścią wynikającą z zasady samoistnej wiarygodności jest to, że izolacja systemu sprawi, że będzie on mniej podatny na atak. Konsekwencja tej zasady odnosi się do zdolności systemu (lub komponentu systemu) do działania w izolacji, a następnie do resynchronizacji z innymi komponentami, gdy jest z nimi połączony.

Zabezpieczenia powiązane: Brak.

(17) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | BEZPIECZNY SKŁAD ROZPROSZONY

Wdrożenie zasady projektowania bezpieczeństwa opartej na bezpiecznej kompozycji rozproszonej w [***Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację***]**.**

Omówienie: Zasada bezpiecznego składu rozproszonego stanowi, że kompozycja elementów rozproszonych, które egzekwują tę samą politykę bezpieczeństwa systemu, powoduje powstanie systemu, który egzekwuje tę politykę co najmniej tak samo jak poszczególne elementy. Wiele z zasad projektowania bezpiecznych systemów dotyczy tego, w jaki sposób komponenty mogą lub powinny ze sobą współdziałać. Potrzeba stworzenia lub umożliwienia możliwości wynikających ze składu komponentów rozproszonych może zwiększyć znaczenie tych zasad. W szczególności, przełożenie polityki bezpieczeństwa z systemu autonomicznego (*ang. stand-alone system*) na system rozproszony (*ang. distributed system*) lub zbiór systemów (*ang. system-of-systems – SoS*), może mieć nieoczekiwane lub nowo powstałe rezultaty. Protokoły komunikacyjne i mechanizmy spójności danych rozproszonych pomagają zapewnić spójne egzekwowanie polityki w całym

systemie rozproszonym. Aby zapewnić ogólnosystemowy poziom pewności właściwego egzekwowania polityki, dokładnie analizowana jest architektura bezpieczeństwa rozproszonego systemu złożonego.

Zabezpieczenia powiązane: Brak.

(18) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | ZAUFANE KANAŁY KOMUNIKACJI

Wdrożenie zasady projektowania bezpieczeństwa opartej na zaufanych kanałach komunikacyjnych w [***Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację***]**.**

Omówienie: Zasada zaufanych kanałów komunikacyjnych stanowi, że przy twozreniu systemu, w którym istnieje potencjalne zagrożenie dla komunikacji między komponentami (tj. połączeń między komponentami), każdy kanał komunikacyjny jest godny zaufania do poziomu współmiernego do obsługiwanych przez niego zależności bezpieczeństwa (tj. w jaki stopniu inne komponenty ufają mu w wykonywaniu jego funkcji bezpieczeństwa). Zaufane kanały komunikacyjne uzyskuje się poprzez kombinację ograniczania dostępu do kanału komunikacyjnego (w celu zapewnienia akceptowalnego dopasowania wiarygodności punktów końcowych zaangażowanych w komunikację) i stosowania zabezpieczeń typu "end-to-end" dla danych przekazywanych przez kanał komunikacyjny (w celu ochrony przed przechwyceniem i modyfikacją oraz dalszego zwiększenia pewności prawidłowej komunikacji typu "end-to-end").

Zabezpieczenia powiązane: SC-8, SC-12, SC-13.

(19) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | CIĄGŁA OCHRONA

Wdrożenie zasady projektowania bezpieczeństwa opartej na ciągłej ochronie [***Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację***]**.**

Omówienie: Zasada ciągłej ochrony stanowi, że komponenty i dane wykorzystywane do egzekwowania polityki bezpieczeństwa mają nieprzerwaną ochronę, która jest zgodna z polityką bezpieczeństwa i założeniami architektury bezpieczeństwa. Nie można zagwarantować, że system może zapewnić poufność, integralność, dostępność i ochronę prywatności w odniesieniu do jego możliwości projektowych, jeśli istnieją luki w ochronie. Wszelkie zapewnienia dotyczące możliwości zabezpieczenia dostarczanej funkcjonalności wymagają, aby dane i informacje były stale chronione. Oznacza to, że nie ma okresów, w których dane i informacje pozostają bez ochrony, gdy znajdują się pod kontrolą systemu (tj. podczas tworzenia, przechowywania, przetwarzania lub przekazywania danych i informacji, jak również podczas inicjowania, działania, awarii, zakłóceń i zamykania systemu). Ciągła ochrona wymaga przestrzegania zasad koncepcji monitora referencyjnego (tj. każde żądanie jest zatwierdzane przez monitor referencyjny; monitor referencyjny jest w stanie chronić się przed ingerencją osób niepowołanych; a wystarczającą pewność co do poprawności i kompletności mechanizmu można ustalić na podstawie analizy i testowania) oraz zasady bezpiecznej awarii i odzyskiwania (tj. zachowanie bezpiecznego stanu podczas błędu, usterki, awarii i udanego ataku; zachowanie bezpiecznego stanu podczas powrotu do normalnego, ograniczonego lub alternatywnego trybu pracy).

Ciągła ochrona dotyczy również systemów zaprojektowanych do pracy w różnych konfiguracjach, w tym takich, które zapewniają pełną zdolność operacyjną oraz konfiguracji w trybie awaryjnym, które zapewniają częściową zdolność operacyjną. Zasada ciągłej ochrony wymaga, aby zmiany w polityce bezpieczeństwa systemu były możliwe do prześledzenia pod kątem potrzeby

operacyjnej, która determinuje konfigurację i były możliwe do zweryfikowania (tzn. aby można było sprawdzić, czy proponowane zmiany nie spowodują, że system znajdzie się w stanie niezabezpieczonym). Niedostateczna identyfikowalność i weryfikacja mogą prowadzić do niespójnych stanów lub nieciągłości ochrony ze względu na złożony lub niedookreślony charakter problemu. Zastosowanie wstępnie zweryfikowanych definicji konfiguracji, które odzwierciedlają nową politykę bezpieczeństwa, umożliwia analizę w celu ustalenia, czy przejście ze starej do nowej polityki ma zasadniczo charakter niepodzielny i czy gwarantuje się, że wszelkie pozostałe skutki wynikające ze starej polityki nie będą sprzeczne z nową polityką. Zdolność do wykazania ciągłej ochrony ma swoje źródło w wyraźnym określeniu potrzeb w zakresie ochrony cyklu życia jako wymogów bezpieczeństwa zainteresowanych stron.

Zabezpieczenia powiązane: AC-25.

(20) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | BEZPIECZNE ZARZĄDZANIE METADANYMI

Wdrożenie zasady projektowania bezpieczeństwa opartej na bezpiecznym zarządzaniu metadanymi w [***Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację***]**.**

Omówienie: Zasada bezpiecznego zarządzania metadanymi stanowi, że metadane są obiektami "pierwszej klasy" w kontekście polityki bezpieczeństwa, o ile polityka ta wymaga albo pełnej ochrony informacji, albo samoochrony podsystemu bezpieczeństwa. Zasada bezpiecznego zarządzania metadanymi wynika z ustalenia, że system, podsystem lub komponent nie może osiągnąć samoochrony, jeśli nie chroni danych, na których opiera się jego prawidłowe działanie. Dane na ogół nie są interpretowane przez system, który je przechowuje. Mogą one mieć wartość semantyczną (tj. zawierać informacje) dla użytkowników i programów, które przetwarzają dane. Z kolei metadane to informacje o danych, takie jak nazwa pliku lub data jego utworzenia. Metadane są

związane z danymi docelowymi, które określają w sposób umożliwiający systemowi ich interpretację, ale nie muszą być przechowywane wewnątrz lub w pobliżu danych docelowych. Mogą istnieć metadane, których celem są same metadane (np. poziom klasyfikacji lub poziom wpływu nazwy pliku), w tym metadane samoreferencyjne.

Pozornie drugorzędny charakter metadanych może prowadzić do pominięcia ich uzasadnionej potrzeby ochrony, co skutkuje naruszeniem polityki bezpieczeństwa obejmującym eksfiltrację informacji. Szczególny problem związany z niewystarczającą ochroną metadanych dotyczy systemów wielopoziomowych (*ang. multilevel secure system - MLS*). Systemy MLS pośredniczą w dostępie podmiotu do obiektu w oparciu o względne poziomy wrażliwości. Wynika z tego, że wszystkie podmioty i obiekty znajdujące się w zakresie kontroli systemu MLS są albo bezpośrednio oznakowane, albo pośrednio przypisane do poziomów wrażliwości. Następstwem oznakowanych metadanych dla systemów MLS jest stwierdzenie, że obiekty zawierające metadane są oznakowane. Podobnie jak w przypadku oceny potrzeb w zakresie ochrony danych, zwraca się uwagę na to, aby ochrona poufności i integralności była indywidualnie oceniana, określana i przydzielana metadanym, podobnie jak w przypadku misji, danych biznesowych i systemowych..

Zabezpieczenia powiązane: Brak.

(21) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | SAMOANALIZY

Wdrożenie zasady projektowania bezpieczeństwa opartej na samoanalizie w [***Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację***]**.**

Omówienie: Zasada samoanalizy stanowi, że komponent systemu jest w stanie ocenić swój stan wewnętrzny i funkcjonalność w ograniczonym zakresie na różnych etapach realizacji, a ta zdolność samoanalizy jest współmierna do poziomu wiarygodności pokładanego w system. Na poziomie systemu,

samoanaliza może być osiągnięta poprzez hierarchiczne oceny wiarygodności ustalone w sposób oddolny. W ramach tego podejścia komponenty niższego szczebla sprawdzają integralność danych i prawidłową funkcjonalność (w ograniczonym zakresie) komponentów wyższego szczebla. Na przykład zaufane sekwencje rozruchowe obejmują zaufany komponent niższego poziomu, który poświadcza wiarygodność kolejnych komponentów wyższego poziomu, dzięki czemu możliwe jest ustanowienie przejściowego łańcucha zaufania. Na samym początku komponent poświadcza sam siebie, co zazwyczaj wiąże się z aksjomatycznym lub narzuconym ze środowiskowego punktu widzenia założeniem dotyczącym jego integralności. Wyniki samoanalizy mogą być wykorzystane do ochrony przed błędami spowodowanymi przez czynniki zewnętrzne, wewnętrznymi nieprawidłowościami w funkcjonowaniu lub przejściowymi błędami. Stosując się do tej zasady, można wykryć pewne proste usterki lub błędy, nie dopuszczając do tego, aby skutki błędu lub nieprawidłowego działania rozprzestrzeniały się na zewnątrz elementu. Ponadto, autotest może być wykorzystany do potwierdzenia konfiguracji komponentu, wykrywając wszelkie potencjalne konflikty w konfiguracji w odniesieniu do oczekiwanej konfiguracji.

Zabezpieczenia powiązane: CA-7.

(22) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI I OCHRONY PRYWATNOŚCI | ROZLICZALNOŚĆ I IDENTYFIKOWALNOŚĆ

Wdrożenie zasady projektowania bezpieczeństwa opartej na rozliczalności i identyfikowalności w [***Realizacja: systemy lub komponenty systemu określone przez organizację***]**.**

Omówienie: Zasada rozliczalności i identyfikowalności stanowi, że możliwe jest śledzenie działań związanych z bezpieczeństwem (tj. interakcji podmiot - przedmiot) podmiotu, w imieniu którego działania są podejmowane. Zasada rozliczalności i identyfikowalności wymaga wiarygodnej infrastruktury, która może rejestrować szczegóły dotyczące działań mających wpływ na bezpieczeństwo

systemu (np. podsystem audytu). W celu zarejestrowania szczegółów działań, system jest w stanie jednoznacznie zidentyfikować podmiot, w imieniu którego podejmowane są działania, a także zarejestrować odpowiednią sekwencję działań, które są przeprowadzane. Polityka rozliczalności wymaga również, aby sama ścieżka audytu była chroniona przed nieautoryzowanym dostępem i modyfikacjami. Zasada jak najmniejszego uprzywilejowania pomaga w śledzeniu działań do poszczególnych podmiotów, ponieważ zwiększa szczegółowość rozliczalności. Powiązanie określonych działań z podmiotami systemu, a docelowo z użytkownikami, oraz zabezpieczenie ścieżki audytu przed nieautoryzowanym dostępem i modyfikacjami zapewnia niezaprzeczalność, ponieważ po zarejestrowaniu działania nie ma możliwości zmiany ścieżki audytu. Inną ważną funkcją, jaką pełni rozliczalność i identyfikowalność, jest rutynowa i kryminalistyczna analiza zdarzeń związanych z naruszeniem polityki bezpieczeństwa. Analiza dzienników audytów może dostarczyć dodatkowych informacji, które mogą być pomocne w określeniu ścieżki lub komponentu, który pozwolił na naruszenie polityki bezpieczeństwa oraz działań osób związanych z naruszeniem polityki bezpieczeństwa.

Zabezpieczenia powiązane: AC-6, AU-2, AU-3, AU-6, AU-9, AU-10, AU-12, IA-2, IR-4.

(23) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | ZABEZPIECZENIA DOMYŚLNE

Wdrożenie zasady projektowania bezpieczeństwa opartej na zabezpieczeniach domyślnych w [***Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację***]**.**

Omówienie: Zgodnie z zasadą zabezpieczeń domyślnych (*ang. secure defaults*) domyślna konfiguracja systemu (w tym jego podsystemów, komponentów i mechanizmów) odzwierciedla restrykcyjne i konserwatywne egzekwowanie polityki bezpieczeństwa. Zasada zabezpieczeń domyślnych odnosi się do początkowej (tzn. domyślnej) konfiguracji systemu, jak również do inżynierii

bezpieczeństwa i projektowania kontroli dostępu oraz innych funkcji bezpieczeństwa, które są zgodne ze strategią "odmowa, chyba że jest to wyraźnie dozwolone". Wstępny aspekt konfiguracji tej zasady wymaga, aby każda konfiguracja systemu, podsystemu lub komponentu systemu "w stanie, w jakim został on dostarczony" nie pomagała w naruszeniu polityki bezpieczeństwa i mogła uniemożliwić działanie systemu w konfiguracji domyślnej w przypadkach, gdy sama polityka bezpieczeństwa wymaga konfiguracji przez użytkownika systemu operacyjnego.

Restrykcyjne ustawienia domyślne oznaczają, że system będzie działał "w stanie gotowym do użycia" z odpowiednią samoochroną i będzie w stanie zapobiegać naruszeniom bezpieczeństwa przed ustanowieniem zamierzonej polityki bezpieczeństwa i konfiguracji systemu. W przypadkach, gdy ochrona zapewniana przez produkt "w stanie gotowym do użycia" jest nieodpowiednia, interesariusze oceniają ryzyko jego użycia przed ustanowieniem bezpiecznego stanu początkowego. Przestrzeganie zasady zabezpieczeń domyślnych gwarantuje, że system jest ustanawiany w bezpiecznym stanie po pomyślnym zakończeniu inicjalizacji. W sytuacjach, gdy system nie zakończy inicjalizacji, albo wykona żądaną operację z wykorzystaniem bezpiecznych ustawień domyślnych, albo nie wykona tej operacji. Należy odnieść się do zasad ciągłej ochrony oraz bezpiecznej awarii i odzyskiwania, które są równoległe do tej zasady, aby zapewnić możliwość wykrywania i odzyskiwania po awarii.

Podejście inżynierii bezpieczeństwa do tej zasady mówi, że mechanizmy bezpieczeństwa odrzucają żądania, chyba że okaże się, że żądanie jest dobrze sformowane i zgodne z polityką bezpieczeństwa. Niebezpieczną alternatywą jest zezwolenie na żądanie, chyba że okaże się, że jest ono niezgodne z polityką bezpieczeństwa. W rozległym systemie, warunki, które są spełnione, aby zaakceptować żądanie, które jest domyślnie odrzucane, są często o wiele bardziej kompaktowe i kompletne niż te, które musiałyby być sprawdzone w celu odrzucenia żądania, które jest domyślnie przyznawane.

Zabezpieczenia powiązane: CM-2, CM-6, SA-4.

(24) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | BEZPIECZNA AWARIA I ODZYSKIWANIE DANYCH

Wdrożenie zasady projektowania bezpieczeństwa opartej na bezpiecznej awarii i odzyskiwaniu danych w [***Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację***]**.**

Omówienie: Zasada bezpiecznej awarii i odzyskiwania danych stanowi, że ani awaria funkcji lub mechanizmu systemu, ani żadne działania naprawcze w odpowiedzi na awarię nie prowadzą do naruszenia polityki bezpieczeństwa. Zasada bezpiecznej awarii i odzyskiwania danych jest zbieżna z zasadą ciągłej ochrony w celu zapewnienia, że system jest w stanie wykryć (w określonych granicach) aktualną i zbliżającą się awarię na każdym etapie jego działania (tj. inicjalizacji, normalnego działania, wyłączenia i konserwacji) oraz podjąć odpowiednie kroki w celu zapewnienia, że polityka bezpieczeństwa nie zostanie naruszona. Ponadto, gdy jest to określone, system jest w stanie powrócić do normalnego, ograniczonego lub alternatywnego bezpiecznego działania po zbliżającej się lub rzeczywistej awarii, zapewniając jednocześnie utrzymanie bezpiecznego stanu tak, aby polityki bezpieczeństwa nie były naruszane.

Awaria to stan, w którym zachowanie komponentu odbiega od określonego lub oczekiwanego zachowania przy jednoznacznie udokumentowanych danych źródłowych. Po wykryciu awarii funkcji bezpieczeństwa, system może dokonać rekonfiguracji w celu obejścia uszkodzonego komponentu przy jednoczesnym zachowaniu bezpieczeństwa i zapewnieniu wszystkich lub części funkcji oryginalnego systemu lub może całkowicie się wyłączyć, aby zapobiec dalszemu naruszaniu zasad bezpieczeństwa. Funkcje rekonfiguracji systemu są tak zaprojektowane, aby zapewnić ciągłe egzekwowanie polityki bezpieczeństwa podczas różnych faz rekonfiguracji.

Inną techniką, która może być zastosowana w celu przywrócenia do stanu bezpiecznego (który może być stanem początkowym), jest powrót do stanu bezpiecznego, a następnie wyłączenie lub zastąpienie usługi lub komponentu, który uległ awarii, tak aby bezpieczne operacje mogły zostać wznowione. Awaria komponentu może, ale nie musi być wykrywalna przez komponenty z nim współpracujące. Zasada bezpiecznej awarii wskazuje, że komponenty ulegają awarii w stanie, który raczej odmawia niż przyznaje dostęp. Na przykład, nominalnie "niepodzielna" operacja przerwana przed zakończeniem nie narusza polityki bezpieczeństwa i jest zaprojektowana do obsługi zdarzeń przerwania poprzez zastosowanie mechanizmów wyższego poziomu niepodzielności i przywracania (np. transakcji). Jeśli wykorzystywana jest usługa, jej właściwości niepodzielności są odpowiednio udokumentowane i scharakteryzowane, tak aby komponent korzystający z tej usługi mógł odpowiednio wykrywać i obsługiwać zdarzenia przerwania. Na przykład, system jest zaprojektowany tak, aby z należytym wyczuciem reagował na rozłączenie i wspierał resynchronizację oraz spójność danych po rozłączeniu.

Strategie ochrony przed awariami, które wykorzystują replikację mechanizmów egzekwowania polityk, nazywane czasami obroną w głąb (ang. defense in depth), mogą pozwolić systemowi na kontynuowanie pracy w bezpiecznym stanie nawet wtedy, gdy jeden z mechanizmów nie zdołał ochronić systemu. Jeśli jednak mechanizmy są podobne, dodatkowa ochrona może być złudna, ponieważ przeciwnik może po prostu atakować seriami. Podobnie, w systemie sieciowym, przełamanie zabezpieczeń jednego systemu lub usługi może umożliwić atakującemu wykonanie tego samego na innych, podobnych, replikowanych systemach i usługach. Dzięki zastosowaniu wielu mechanizmów ochrony, których cechy są znacząco różne, można ograniczyć możliwość replikacji lub powtarzania ataków. Prowadzone są analizy mające na celu rozważenie kosztów i korzyści wynikających z zastosowania takich technik redundancji w kontekście zwiększonego wykorzystania zasobów i niekorzystnego wpływu na ogólną

wydajność systemu. Dodatkowe analizy przeprowadzane są w miarę wzrostu złożoności tych mechanizmów, co może mieć miejsce w przypadku zachowań dynamicznych. Zwiększona złożoność generalnie zmniejsza wiarygodność. Jeśli zasób nie może być stale chroniony, krytyczne jest wykrycie i naprawienie wszelkich naruszeń bezpieczeństwa, zanim zasób zostanie ponownie wykorzystany w bezpiecznym kontekście.

Zabezpieczenia powiązane: CP-10, CP-12, SC-7, SC-8, SC-24, SI-13.

(25) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | BEZPIECZEŃSTWO EKONOMICZNE

Wdrożenie zasady projektowania bezpieczeństwa opartej na bezpieczeństwie ekonomicznym w [***Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację***]**.**

Omówienie: Zasada bezpieczeństwa ekonomicznego stanowi, że mechanizmy bezpieczeństwa nie są bardziej kosztowne niż potencjalne szkody, które mogłyby powstać w wyniku naruszenia bezpieczeństwa. Jest to istotna z punktu widzenia bezpieczeństwa forma analizy kosztów i korzyści stosowana w zarządzaniu ryzykiem. Założenia kosztowe analizy kosztów i korzyści uniemożliwiają projektantowi systemu wprowadzenie mechanizmów bezpieczeństwa o większej sile niż jest to konieczne, przy czym siła mechanizmu jest proporcjonalna do kosztów. Zasada bezpieczeństwa ekonomicznego wymaga również analizy korzyści wynikających z zapewnienia wiarygodności w stosunku do kosztów tego zapewnienia pod względem wysiłku włożonego w uzyskanie odpowiednich i wiarygodnych dowodów, jak również niezbędnych analiz umożliwiających ocenę i wyciągnięcie z nich wniosków dotyczących wiarygodności i ryzyka.

Zabezpieczenia powiązane: RA-3.

(26) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | PEWNOŚĆ DZIAŁANIA

Wdrożenie zasady projektowania bezpieczeństwa opartej na pewności działania w [***Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację***]**.**

Omówienie: Zasada pewności działania stanowi, że mechanizmy bezpieczeństwa są tak skonstruowane, aby nie wpływały nadmiernie na obniżenie wydajności systemu. Wymagania zainteresowanych stron i konstrukcyjne systemu dotyczące wydajności i bezpieczeństwa są precyzyjnie sformułowane i hierarchizowane. W celu spełnienia przez implementację systemu wymagań projektowych i uznania jej za możliwą do zaakceptowania przez interesariuszy (tj. weryfikacja względem wymagań interesariuszy), projektanci stosują się do określonych ograniczeń, które wymagania dotyczące wydajności zdolności systemu nakładają na kwestie ochrony. Ogólny wpływ usług bezpieczeństwa wymagających dużych mocy obliczeniowych (np. kryptografii) jest oceniany i wykazywany jako nie mający znaczącego wpływu na kwestie wydajności mające wyższy priorytet lub jako zapewniający akceptowalny kompromis pomiędzy wydajnością, a godną zaufania ochroną. Rozważania kompromisowe obejmują mniej wymagające obliczeniowo usługi bezpieczeństwa, o ile nie są one niedostępne lub niewystarczające. Niewystarczalność usługi bezpieczeństwa jest określana na podstawie zdolności funkcjonalnej i siły mechanizmu. Siła mechanizmu jest wybierana w odniesieniu do wymagań bezpieczeństwa krytycznych dla wydajności, kwestii ogólnych (np. zarządzanie kluczami kryptograficznymi) oraz oceny możliwości zagrożenia.

Zasada bezpieczeństwa wydajnościowego prowadzi do włączania funkcji, które pomagają w egzekwowaniu polityki bezpieczeństwa, ale mają minimalny narzut, takich jak niskopoziomowe mechanizmy sprzętowe, na których można budować usługi wyższego poziomu. Takie niskopoziomowe mechanizmy są zazwyczaj bardzo precyzyjne, mają bardzo ograniczoną funkcjonalność i są zoptymalizowane pod kątem wydajności. Na przykład, po przyznaniu praw dostępu do części pamięci, wiele systemów wykorzystuje mechanizmy sprzętowe, aby zapewnić, że wszystkie dalsze dostępy dotyczą właściwego adresu pamięci i trybu dostępu.

Zastosowanie tej zasady wymusza konieczność projektowania bezpieczeństwa w systemie od podstaw i włączania prostych mechanizmów w niższych warstwach, które mogą być wykorzystane jako bloki konstrukcyjne dla mechanizmów wyższego poziomu.

Zabezpieczenia powiązane: SC-12, SC-13, SI-2, SI-7.

(27) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | BEZPIECZEŃSTWO UWZGLĘDNIAJĄCE CZYNNIK LUDZKI

Wdrożenie zasady projektowania bezpieczeństwa polegającej na uwzględnianiu czynnika ludzkiego w [***Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację***]**.**

Omówienie: Zasada bezpieczeństwa uwzględniająca czynnik ludzki stanowi, że interfejs użytkownika stosowany dla funkcji bezpieczeństwa i usług wspierających jest intuicyjny, przyjazny dla użytkownika i zapewnia informacje zwrotne dla działań użytkownika, które mają wpływ na realizację polityki bezpieczeństwa i jej egzekwowanie. Mechanizmy egzekwujące politykę bezpieczeństwa nie są inwazyjne dla użytkownika i są zaprojektowane tak, aby nie obniżać wydajności pracy użytkownika. Mechanizmy egzekwowania polityki bezpieczeństwa dostarczają również użytkownikowi znaczących, jasnych i istotnych informacji zwrotnych oraz ostrzeżeń w przypadku dokonywania wyborów niezgodnych z zasadami bezpieczeństwa. Szczególną uwagę zwraca się na interfejsy, za pomocą których personel odpowiedzialny za administrowanie i funkcjonowanie systemu konfiguruje i ustawia polityki bezpieczeństwa. W idealnym przypadku personel ten jest w stanie zrozumieć wpływ dokonywanych przez siebie wyborów. Personel odpowiedzialny za administrowanie i funkcjonowanie systemu jest w stanie konfigurować systemy przed ich uruchomieniem i zarządzać nimi w czasie działania mając pewność, że jego intencje są prawidłowo odwzorowane w mechanizmach systemu. Usługi, funkcje i mechanizmy bezpieczeństwa nie utrudniają, ani nie powodują niepotrzebnych komplikacji

w obsłudze systemu. Istnieje kompromis pomiędzy użytecznością systemu, a restrykcyjnością egzekwowania polityki bezpieczeństwa. Jeżeli mechanizmy bezpieczeństwa są frustrujące lub trudne w użyciu, wówczas użytkownicy mogą je wyłączyć, omijać lub używać ich w sposób niezgodny z wymaganiami bezpieczeństwa i potrzebami ochrony, dla zaspokojenia których mechanizmy te zostały zaprojektowane.

Zabezpieczenia powiązane: Brak.

(28) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | AKCEPTOWALNY POZIOM BEZPIECZEŃSTWA

Wdrożenie zasady projektowania bezpieczeństwa ustanawiającej akceptowalny poziom bezpieczeństwa w [***Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację***]**.**

Omówienie: Zasada akceptowalnego poziomu bezpieczeństwa wymaga, aby poziom ochrony prywatności i wydajności, jaki zapewnia system, był zgodny z oczekiwaniami użytkowników. Postrzeganie prywatności może wpływać na zachowanie użytkowników, ich morale i skuteczność. W oparciu o organizacyjną politykę prywatności i konstrukcje systemu, użytkownicy powinni mieć możliwość ograniczania swoich działań w celu ochrony swojej prywatności. Jeżeli systemy nie zapewniają intuicyjnych interfejsów lub nie spełniają oczekiwań w zakresie prywatności i wydajności, użytkownicy mogą zdecydować się na całkowite unikanie korzystania z systemu lub wykorzystywać go w sposób, który może być nieefektywny lub nawet niebezpieczny.

Zabezpieczenia powiązane: Brak.

(29) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | POWTARZALNE I UDOKUMENTOWANE PROCEDURY

Wdrożenie zasady projektowania bezpieczeństwa opartej na powtarzalnych i udokumentowanych procedurach w [***Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację***]**.**

Omówienie: Zasada powtarzalnych i udokumentowanych procedur stanowi, że techniki i metody zastosowane do skonstruowania komponentu systemu pozwalają na całkowitą i poprawną rekonstrukcję tego samego komponentu w późniejszym czasie. Powtarzalne i udokumentowane procedury wspomagają rozwój komponentu, który jest identyczny z komponentem stworzonym wcześniej, a który może być powszechnie stosowany. W przypadku innych artefaktów systemu (np. dokumentacja i wyniki testów), powtarzalność wspiera spójność i możliwość kontroli artefaktów. Powtarzalne i udokumentowane procedury mogą być wprowadzane na różnych etapach cyklu życia systemu i przyczyniają się do zwiększenia zdolności oceny roszczeń dotyczących wiarygodności systemu. Przykłady obejmują systematyczne procedury rozwoju i przeglądu kodu, procedury zarządzania konfiguracją narzędzi rozwojowych i artefaktów systemu oraz procedury dostawy systemu.

Zabezpieczenia powiązane: CM-1, SA-1, SA-10, SA-11, SA-15, SA-17, SC-1, SI-1.

(30) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | RYGOR PROCEDURALNY

Wdrożenie zasady projektowania bezpieczeństwa opartej na rygorze proceduralnym w [***Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację***]**.**

Omówienie: Zasada rygoru proceduralnego stanowi, że rygor procesu cyklu życia systemu jest współmierny do jego zamierzonej wiarygodności. Rygor proceduralny określa skalę, głębokość i szczegółowość procedur cyklu życia systemu. Rygorystyczne procedury cyklu życia systemu przyczyniają się do zapewnienia, że system jest poprawny i wolny od niezamierzonej funkcjonalności na kilka sposobów. Po pierwsze, procedury narzucają kontrolę i równoważenie

procesu cyklu życia w taki sposób, że zapobiega się wprowadzaniu niesprecyzowanej funkcjonalności. Po drugie, rygorystyczne procedury stosowane w działaniach inżynierii bezpieczeństwa systemów, które tworzą specyfikacje i inne dokumenty projektowe systemu, przyczyniają się do zdolności zrozumienia systemu w takiej postaci, w jakiej został on zbudowany, zamiast ufać, że komponent, jako zaimplementowany, jest miarodajną (i potencjalnie mylącą) specyfikacją. Wreszcie, modyfikacje istniejącego komponentu systemu są łatwiejsze, gdy istnieją szczegółowe specyfikacje opisujące jego aktualną konstrukcję, zamiast studiowania kodu źródłowego lub schematów w celu próby zrozumienia, jak on działa. Rygory proceduralne pomagają zapewnić, że wymagania funkcjonalne i bezpieczeństwa zostały spełnione, a także przyczyniają się do stworzenia bardziej świadomej podstawy do określania wiarygodności i podejścia do ryzyka. Rygory proceduralne są współmierne do stopnia pewności pożądanego dla systemu. Jeżeli wymagana wiarygodność systemu jest niska, wysoki poziom rygoru proceduralnego może niepotrzebnie zwiększyć koszty, natomiast gdy wysoka wiarygodność jest krytyczna, koszt wysokiego rygoru proceduralnego jest uzasadniony.

Zabezpieczenia powiązane: Brak.

(31) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | BEZPIECZNA MODYFIKACJA SYSTEMU

Wdrożenie zasady projektowania bezpieczeństwa opartej na bezpiecznej modyfikacji [***Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację***]**.**

Omówienie: Zasada bezpiecznej modyfikacji systemu stanowi, że modyfikacja systemu zachowuje bezpieczeństwo systemu w odniesieniu do wymagań bezpieczeństwa i tolerancji ryzyka interesariuszy. Aktualizacje lub modyfikacje systemów mogą przekształcić bezpieczne systemy w systemy, które nie gwarantują bezpieczeństwa. Procedury modyfikacji systemu zapewniają, że jeżeli

system ma zachować swoją wiarygodność, to do wszelkich zmian w systemie stosuje się ten sam rygor, który został zastosowany podczas jego pierwotnego rozwoju. Ponieważ modyfikacje mogą mieć wpływ na zdolność systemu do utrzymania bezpiecznego stanu, przed ich wprowadzeniem i wdrożeniem konieczna jest dokładna analiza bezpieczeństwa tych modyfikacji. Zasada ta jest analogiczna do zasady bezpiecznej ewolucyjności.

Zabezpieczenia powiązane: CM-3, CM-4.

(32) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | NIEZBĘDNA DOKUMENTACJA

Wdrożenie zasady projektowania bezpieczeństwa opartej na zapewnieniu niezbędnej dokumentacji [***Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację***]**.**

Omówienie: Zasada niezbędnej dokumentacji stanowi, że personel organizacyjny odpowiedzialny za interakcję z systemem otrzymuje odpowiednią dokumentację i inne informacje, które przyczyniają się do bezpieczeństwa systemu, a nie go zakłócają. Pomimo prób przestrzegania takich zasad, jak bezpieczeństwo oparte na czynnikach ludzkich i bezpieczeństwo akceptowalne, systemy są z natury rzeczy złożone, a intencje projektowe dotyczące wykorzystania mechanizmów bezpieczeństwa i konsekwencje ich niewłaściwego wykorzystania lub błędnej konfiguracji nie zawsze są intuicyjnie oczywiste. Niedoinformowani i niedostatecznie przeszkoleni użytkownicy mogą wprowadzić podatność na zagrożenia z powodu błędów wynikających z zaniechania lub działania z własnej winy. Dostępność dokumentacji i szkoleń może pomóc w zapewnieniu kompetentnego personelu, z którego każdy ma krytyczną rolę w osiągnięciu zasad takich jak ciągła ochrona. Dokumentacja musi być napisana w sposób jasny i poparta szkoleniami, uświadamiającymi kwestie bezpieczeństwa i pozwalającymi zrozumieć obowiązki związane z bezpieczeństwem.

Zabezpieczenia powiązane: NA 2, NA 3, SA-5.

(33) ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | ZASADA MINIMALIZACJI

Wdrożenie zasady ochrony prywatności opartej na minimalizacji [***Realizacja: przy użyciu procesów zdefiniowanych przez organizację***]**.**

Omówienie: Zasada minimalizacji stanowi, że organizacje powinny przetwarzać tylko te dane osobowe, które są bezpośrednio istotne i niezbędne do osiągnięcia uprawnionego celu i powinny przechowywać dane osobowe tylko tak długo, jak jest to konieczne do osiągnięcia tego celu. Organizacje stosują procesy określone obowiązującym prawem i przyjętą polityką organizacji, w celu wdrożenia zasady minimalizacji.

Zabezpieczenia powiązane: PE-8, PM-25, SC-42, SI-12.

Referencje: [PRIVACT], [0MB A-130], [FIPS 199], [FIPS 200], [NIST SP 800-37], [NIST SP 800-53A], [NIST SP 800- 60-1], [NIST SP 800-60-2], [NIST SP 800-160-1], [IR 8062].

SA-9 USŁUGI SYSTEMU ZEWNĘTRZNEGO

Zabezpieczenie podstawowe:

a. Wymaganie, aby dostawcy zewnętrznych usług systemowych przestrzegali organizacyjnych wymogów bezpieczeństwa i ochrony prywatności oraz stosowali następujące zabezpieczenia: [*Realizacja: zabezpieczenia określone przez organizację*];

b. Określanie i dokumentowanie nadzoru organizacyjnego oraz ról i obowiązków użytkowników w odniesieniu do zewnętrznych usług systemowych; oraz

c. Stosowanie następujących procesów, metod i technik w celu bieżącego monitorowania zgodności zabezpieczeń wykorzystywanych przez zewnętrznych dostawców usług: [*Realizacja: procesy, metody i techniki zdefiniowane przez organizację*].

Omówienie: Zewnętrzne usługi systemowe są świadczone przez zewnętrznego dostawcę, a organizacja nie ma bezpośredniej kontroli nad wdrożeniem wymaganych zabezpieczeń lub oceną skuteczności zabezpieczeń. Organizacje nawiązują relacje z zewnętrznymi dostawcami usług na różne sposoby, w tym poprzez partnerstwa biznesowe, umowy, porozumienia międzyorganizacyjne, porozumienia branżowe, umowy licencyjne, wspólne przedsięwzięcia oraz wymiany w ramach łańcucha dostaw. Odpowiedzialność za zarządzanie ryzykiem wynikającym z korzystania z zewnętrznych usług systemowych spoczywa na osobach autoryzujących (*ang. authorizing official – AO*)[96]. W przypadku usług świadczonych na zewnątrz organizacji, łańcuch zaufania wymaga, aby organizacje ustanowiły i utrzymały pewien poziom zaufania, zgodnie z którym każdy usługodawca w relacji konsument-usługodawca zapewnia odpowiednią ochronę świadczonych usług. Zakres i charakter tego łańcucha zaufania różni się w zależności od relacji pomiędzy

[96] Patrz: NSC 800-37; NSC 7298.

organizacjami, a zewnętrznymi dostawcami. Organizacje dokumentują podstawy relacji zaufania, co pozwala na monitorowanie tych relacji. Dokumentacja zewnętrznych usług systemowych obejmuje administrację rządową, dostawców usług, role i obowiązki użytkownika końcowego w zakresie bezpieczeństwa oraz umowy o gwarantowanym poziomie usług (ang. service-level agreement - SLA). Umowy SLA określają oczekiwania dotyczące wydajności wdrożonych zabezpieczeń, opisują mierzalne wyniki oraz określają środki zaradcze i wymagania dotyczące reakcji na zidentyfikowane przypadki niezgodności.

Zabezpieczenia powiązane: AC-20, CA-3, CP-2, IR-4, IR-7, PL-10, PL-11, PS-7, SA-2, SA-4, SR-3, SR-5.

Zabezpieczenia rozszerzone:

(1) USŁUGI SYSTEMU ZEWNĘTRZNEGO | OCENA RYZYKA / ZATWIERDZENIA ORGANIZACYJNE

(a) Przeprowadzanie oceny ryzyka organizacyjnego przed nabyciem lub zleceniem wykonania dedykowanych usług bezpieczeństwa informacji; oraz

(b) Sprawdzanie, czy nabycie lub zlecenie wykonania dedykowanych usług bezpieczeństwa informacji jest zatwierdzone przez [***Realizacja: personel lub role określone przez organizację***]**.**

Omówienie: Usługi w zakresie bezpieczeństwa informacji obejmują obsługę urządzeń zabezpieczających, takich jak zapory ogniowe lub usługi zarządzania kluczami, a także monitorowanie, analizę i reagowanie na incydenty. Oceniane ryzyko może obejmować ryzyko związane z systemem, misją lub działalnością, bezpieczeństwem, prywatnością lub łańcuchem dostaw.

Zabezpieczenia powiązane: CA-6, RA-3, RA-8.

(2) USŁUGI SYSTEMU ZEWNĘTRZNEGO | IDENTYFIKACJA FUNKCJI, PORTÓW, PROTOKOŁÓW I USŁUG

Wymaganie od dostawców usług zapewnienia [*Realizacja: określone przez organizację usługi systemu zewnętrznego*] do zidentyfikowania funkcji, portów, protokołów i innych usług wymaganych do korzystania z takich usług.

Omówienie: Informacje od zewnętrznych dostawców usług dotyczące poszczególnych funkcji, portów, protokołów i usług wykorzystywanych przy świadczeniu takich usług mogą być przydatne, gdy pojawia się potrzeba zrozumienia zależności związanych z ograniczeniem pewnych funkcji i usług lub zablokowaniem konkretnych portów i protokołów.

Zabezpieczenia powiązane: CM-6, CM-7.

(3) USŁUGI SYSTEMU ZEWNĘTRZNEGO | TWORZENIE / UTRZYMANIE RELACJI ZAUFANIA Z DOSTAWCAMI

Ustanowienie, udokumentowanie i utrzymanie relacji zaufania z zewnętrznymi dostawcami usług w oparciu o następujące wymagania, właściwości, czynniki lub warunki: [***Realizacja: określone przez organizację wymagania dotyczące bezpieczeństwa i ochrony prywatności, właściwości, czynników lub warunków określających dopuszczalne relacje oparte na zaufaniu***]**.**

Omówienie: Relacje oparte na zaufaniu pomiędzy organizacjami i zewnętrznymi dostawcami usług odzwierciedlają stopień pewności, że ryzyko związane z korzystaniem z usług zewnętrznych jest na akceptowalnym poziomie. Relacje oparte na zaufaniu mogą pomóc organizacjom uzyskać wyższy poziom pewności, że dostawcy usług zapewniają odpowiednią ochronę świadczonych usług, a także mogą być przydatne podczas reagowania na incydenty lub podczas planowania aktualizacji lub wycofywania usług z użycia. Relacje oparte na zaufaniu mogą być skomplikowane ze względu na potencjalnie dużą liczbę podmiotów uczestniczących w interakcjach między konsumentem a usługodawcą, relacje podrzędne i poziomy zaufania oraz rodzaje interakcji między stronami.

W niektórych przypadkach stopień zaufania opiera się na poziomie kontroli, jaką organizacje mogą sprawować nad zewnętrznymi dostawcami usług w zakresie zabezpieczeń niezbędnych do ochrony usług, informacji lub prywatności osób oraz na przedstawionych dowodach skuteczności wdrożonych zabezpieczeń. Poziom kontroli jest ustalony przez warunki kontraktów lub umów ogwarancji świadczenia usług (SLA).

Zabezpieczenia powiązane: SR-2.

(4) USŁUGI SYSTEMU ZEWNĘTRZNEGO | ZGODNOŚĆ INTERESÓW KONSUMENTÓW I DOSTAWCÓW

Podejmowanie następujących działań mających na celu sprawdzenia, czy interesy [*Realizacja: zewnętrzni dostawcy usług zdefiniowani przez organizację*] są zgodne i odzwierciedlają interesy organizacyjne [Realizacja: *działania określone przez organizację*].

Omówienie: Ponieważ organizacje coraz częściej korzystają z usług zewnętrznych dostawców usług możliwe jest, że interesy dostawców usług mogą być rozbieżne z interesami organizacji. W takich sytuacjach samo wprowadzenie wymaganych zabezpieczeń technicznych, administracyjnych lub operacyjnych może okazać się niewystarczające, jeśli dostawcy, którzy wdrażają te zabezpieczenia i zarządzają nimi, nie działają w sposób zgodny z interesami organizacji korzystających z tego rodzaju usług. Działania, które organizacje podejmują w celu wyeliminowania takich wątpliwości, obejmują wymóg sprawdzania pochodzenia wybranych pracowników dostawców usług, sprawdzanie rejestrów własności, korzystanie wyłącznie z usług dostawców godnych zaufania, takich jak dostawcy, z którymi organizacje nawiązały udane relacje oparte na zaufaniu, oraz przeprowadzanie rutynowych, okresowych, niezaplanowanych wizyt w obiektach dostawców usług.

Zabezpieczenia powiązane: Brak.

(5) USŁUGI SYSTEMU ZEWNĘTRZNEGO | OBSZAR PROCESOWANIA, PRZECHOWYWANIA I OBSŁUGI TECHNICZNEJ

Ograniczenie lokalizacji [*Wybór (jeden lub więcej): przetwarzanie informacji; informacje lub dane; usługi systemowe*] do [Realizacja: *lokalizacje określone przez organizację*] *w* oparciu o [Realizacja: *wymagania lub warunki określone przez organizację*].

Omówienie: Miejsce przetwarzania informacji, przechowywania informacji i danych lub usług systemowych może mieć bezpośredni wpływ na zdolność organizacji do skutecznej realizacji ich misji i funkcji biznesowych. Wpływ ten ma miejsce, gdy zewnętrzni dostawcy zabezpieczają lokalizację przetwarzania, przechowywania lub usług. Kryteria, które zewnętrzni dostawcy stosują przy wyborze lokalizacji przetwarzania, przechowywania lub świadczenia usług, mogą różnić się od kryteriów, które stosują organizacje. Na przykład, organizacje mogą chcieć, aby lokalizacje przechowywania danych lub informacji były ograniczone do określonych lokalizacji, aby ułatwić reagowanie na incydenty w przypadku naruszenia bezpieczeństwa informacji lub prywatności. Na działania związane z reagowaniem na incydenty, w tym analizy kryminalistyczne i badania powykonawcze, mogą mieć negatywny wpływ obowiązujące przepisy, zasady lub protokoły w miejscach, w których odbywa się przetwarzanie i przechowywanie i/lub w miejscach, z których pochodzą usługi systemu.

Zabezpieczenia powiązane: SA-5, SR-4.

(6) USŁUGI SYSTEMU ZEWNĘTRZNEGO | NADZOROWANIE ZARZĄDZANIA KLUCZAMI KRYPTOGRAFICZNYMI PRZEZ ORGANIZACJĘ

Utrzymywanie wyłącznej kontroli nad kluczami kryptograficznymi odnoszącymi się do zaszyfrowanych materiałów przechowywanych lub przesyłanych przez system zewnętrzny.

Omówienie: Utrzymywanie wyłącznej kontroli nad kluczami kryptograficznymi w systemie zewnętrznym zapobiega odszyfrowywaniu danych organizacyjnych przez personel systemu zewnętrznego. Organizacyjna kontrola kluczy kryptograficznych może być realizowana przez szyfrowanie i odszyfrowywanie

danych wewnątrz organizacji, gdy dane są wysyłane do i odbierane z systemu zewnętrznego lub przez zastosowanie komponentu, który pozwala na lokalne wykonywanie funkcji szyfrowania i odszyfrowywania w systemie zewnętrznym, ale pozwala wyłącznie organizacji na dostęp do kluczy szyfrujących.

Zabezpieczenia powiązane: SC-12, SC-13, SI-4.

(7) USŁUGI SYSTEMU ZEWNĘTRZNEGO | ORGANIZACYJNIE KONTROLOWANE ZABEZPIECZENIA INTEGRALNOŚCI

Zapewnienie możliwości sprawdzania integralności informacji znajdujących się w systemie zewnętrznym..

Omówienie: Przechowywanie informacji organizacyjnych w systemie zewnętrznym może ograniczać kontrolę nad stanem bezpieczeństwa danych. Zdolność organizacji do weryfikacji i zatwierdzania integralności przechowywanych danych bez przenoszenia ich z systemu zewnętrznego zapewnia taką dostępność.

Zabezpieczenia powiązane: SI-7.

(8) USŁUGI SYSTEMU ZEWNĘTRZNEGO | LOKALIZACJA PRZETWARZANIA I PRZECHOWYWANIA - JURYSDYKCJA KRAJOWA

Ograniczanie położenia geograficznego przetwarzania i przechowywania informacji do obiektów znajdujących się w granicach jurysdykcji prawnej Państwa.

Omówienie: Lokalizacja geograficzna przetwarzania informacji i przechowywania danych może mieć bezpośredni wpływ na zdolność organizacji do skutecznej realizacji ich misji i funkcji biznesowych. Kompromitacja lub naruszenie informacji i systemów o wysokim poziomie wpływu może mieć poważne lub katastrofalne skutki dla aktywów i działań organizacji, osób, innych organizacji i Państwa. Ograniczenie przetwarzania i przechowywania informacji o wysokim poziomie

wpływu do obiektów znajdujących się w granicach jurysdykcji prawnej Państwa zapewnia zwiększoną kontrolę nad procesem przetwarzania i przechowywania.

Zabezpieczenia powiązane: SA-5, SR-4.

Referencje: [OMB A-130], [NIST SP 800-35], [NIST SP 800-160-1], [NIST SP 800-161], [NIST SP 800-171].

SA-10 ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA

Zabezpieczenie podstawowe: Wymaganie od producenta systemu, komponentu systemu lub usługi systemu:

a. Zarządzania konfiguracją systemu, komponentu lub usługi podczas [*Wybór (jeden lub więcej): projektowanie, opracowanie, wdrożenie, obsługa, utylizacja*];

b. Dokumentowania, zarządzania i kontroli integralności zmian w [*Realizacja: zdefiniowane przez organizację elementy konfiguracji w ramach zarządzania konfiguracją*];

c. Wdrażania tylko zatwierdzonych przez organizację zmian w systemie, komponencie lub usłudze;

d. Dokumentowania zatwierdzonych zmian w systemie, komponencie lub usłudze oraz potencjalnego wpływu takich zmian na bezpieczeństwo i prywatność; oraz

e. Śledzenie luk w zabezpieczeniach i ich usuwanie w obrębie systemu, komponentu lub usługi oraz przekazywanie wyników do [*Realizacja: personel określony przez organizację*].

Omówienie: Organizacje uznają jakość i kompletność działań związanych z zarządzaniem konfiguracją prowadzonych przez programistów za bezpośredni dowód stosowania skutecznych środków bezpieczeństwa. Zabezpieczenia te obejmują ochronę kopii źródłowych materiałów używanych do generowania istotnych z punktu widzenia bezpieczeństwa elementów sprzętu, aplikacji i oprogramowania układowego systemu przed nieuprawnioną modyfikacją lub zniszczeniem. Utrzymanie integralności zmian w systemie, komponencie systemu lub usłudze systemowej wymaga ścisłej kontroli konfiguracji w całym cyklu życia systemu w celu śledzenia autoryzowanych zmian i zapobiegania zmianom nieautoryzowanym.

Elementy konfiguracji, które są włączone do zarządzania konfiguracją, obejmują model formalny; specyfikacje funkcjonalne wysokopoziomowe i niskopoziomowe projektu; inne dane projektowe; dokumentację implementacyjną; kod źródłowy

i schematy sprzętu; bieżącą działającą wersję kodu obiektowego; narzędzia do porównywania nowych wersji istotnych z punktu widzenia bezpieczeństwa opisów sprzętu i kodu źródłowego z poprzednimi wersjami; oraz oprzyrządowanie i dokumentację testową. W zależności od misji i potrzeb biznesowych organizacji oraz charakteru istniejących relacji kontraktowych, deweloperzy mogą zapewnić wsparcie w zakresie zarządzania konfiguracją na etapie eksploatacji i utrzymania cyklu życia systemu.

Zabezpieczenia powiązane: CM-2, CM-3, CM-4, CM-7, CM-9, SA-4, SA-5, SA-8, SA-15, SI-2, SR-3, SR-4, SR-5, SR-6.

Zabezpieczenia rozszerzone:

(1) ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA | WERYFIKACJA INTEGRALNOŚCI PROGRAMÓW I OPROGRAMOWANIA UKŁADOWEGO

Wymaganie od producenta systemu, komponentu systemu lub usługi systemowej, aby umożliwiał weryfikację integralności komponentów aplikacji i oprogramowania sprzętowego.

Omówienie: Weryfikacja integralności aplikacji i oprogramowania układowego pozwala organizacjom na wykrycie nieautoryzowanych zmian w oprogramowaniu i komponentach firmware'u przy użyciu narzędzi, technik i mechanizmów dostarczonych przez dewelopera. Mechanizmy weryfikacji integralności mogą również przeciwdziałać podrabianiu oprogramowania i składników firmware'u. Organizacje weryfikują integralność komponentów oprogramowania i firmware'u, na przykład za pomocą bezpiecznych, jednokierunkowych haszy (skrótów) dostarczanych przez deweloperów. Dostarczane elementy oprogramowania i firmware'u zawierają również wszelkie aktualizacje takich elementów.

Zabezpieczenia powiązane: SI-7, SR-11.

(2) ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA | ALTERNATYWNE PROCESY ZARZĄDZANIA KONFIGURACJĄ

Zapewnienie alternatywnego procesu zarządzania konfiguracją z wykorzystaniem personelu organizacyjnego w przypadku braku dedykowanego zespołu programistów zarządzających konfiguracją.

Omówienie: Alternatywne procesy zarządzania konfiguracją mogą być wymagane w przypadku korzystania przez organizacje z komercyjnych, gotowych produktów informatycznych. Alternatywne procesy zarządzania konfiguracją obejmują personel organizacyjny, który dokonuje przeglądu i zatwierdza proponowane zmiany w systemach, komponentach systemu i usługach systemowych oraz przeprowadza analizy wpływu na bezpieczeństwo i prywatność przed wprowadzeniem zmian w systemach, komponentach lub usługach.

Zabezpieczenia powiązane: Brak.

(3) ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA | WERYFIKACJA INTEGRALNOŚCI SPRZĘTU

Wymaganie od twórcy systemu, komponentu systemu lub usługi systemowej umożliwienia weryfikacji integralności komponentów sprzętowych.

Omówienie: Weryfikacja integralności sprzętowej pozwala organizacjom na wykrycie nieautoryzowanych zmian w komponentach sprzętowych przy użyciu narzędzi, technik, metod i mechanizmów dostarczonych przez dewelopera. Organizacje mogą weryfikować integralność komponentów sprzętowych za pomocą trudnych do skopiowania etykiet, możliwych do zweryfikowania numerów seryjnych dostarczonych przez deweloperów oraz poprzez wymaganie stosowania technologii zabezpieczających przed manipulacją. Dostarczone komponenty sprzętowe zawierają również aktualizacje sprzętu i oprogramowania układowego takich komponentów.

Zabezpieczenia powiązane: SI-7.

(4) ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA | ZAUFANA GENERACJA

Żądanie od twórcy systemu, komponentu systemu lub usługi systemowej stosowania narzędzi do porównywania nowo wygenerowanych wersji opisów sprzętu istotnych z punktu widzenia bezpieczeństwa, kodu źródłowego i kodu obiektu z poprzednimi wersjami.

Omówienie: Zaufane generowanie opisów, kodu źródłowego i kodu obiektowego dotyczy autoryzowanych zmian w komponentach sprzętu, oprogramowania i oprogramowania układowego między kolejnymi wersjami w ramach rozwoju oprogramowania. Główny nacisk kładziony jest na skuteczność procesu zarządzania konfiguracją przez dewelopera w celu zapewnienia, że nowo wygenerowane wersje istotnych dla bezpieczeństwa opisów sprzętu, kodu źródłowego i kodu obiektowego nadal egzekwują politykę bezpieczeństwa systemu, komponentu systemu lub usługi systemowej. Z kolei zabezpieczenia SA-10(1) i SA-10(3) pozwalają organizacjom na wykrywanie nieautoryzowanych zmian w sprzęcie, oprogramowaniu i komponentach firmware'u przy użyciu narzędzi, technik lub mechanizmów dostarczonych przez twórców oprogramowania.

Zabezpieczenia powiązane: Brak.

(5) ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA | INTEGRALNOŚĆ MAPOWANIA KONTROLI WERSJI

Wymaganie od twórcy systemu, komponentu systemu lub usługi systemowej zachowania integralności mapowania między danymi kompilacji głównej (sprzęt, aplikacje, oprogramowanie układowe) opisującymi aktualną wersję istotnego dla bezpieczeństwa sprzętu, aplikacji i oprogramowania układowego oraz zaktualizowaną kopią głównej wersji danych.

Omówienie: Integralność mapowania kontroli wersji odnosi się do zmian w komponentach sprzętu, aplikacjach i oprogramowaniu układowym zarówno na etapie przygotowania, jak i w trakcie aktualizowania w cyklu życia systemu.

Utrzymanie integralności pomiędzy kopiami wzorcowymi sprzętu, aplikacji i firmware'u o istotnym znaczeniu dla bezpieczeństwa (w tym projektów, rysunków sprzętu, kodu źródłowego), a równoważnymi danymi w kopiach wzorcowych w środowiskach operacyjnych jest niezbędne do zapewnienia dostępności systemów organizacyjnych, które wspierają krytyczne misje i funkcje biznesowe.

Zabezpieczenia powiązane: Brak.

(6) ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA | ZAUFANA DYSTRYBUCJA

Wymaganie od twórcy systemu, komponentu systemu lub usługi systemowej wykonania procedur mających na celu zapewnienie, że istotne dla bezpieczeństwa sprzętu, oprogramowania i oprogramowania układowego aktualizacje dystrybuowane do organizacji są dokładnie takie, jak podano we wzorcach tych aktualizacji.

Omówienie: Zaufana dystrybucja aktualizacji istotnych dla bezpieczeństwa sprzętu, aplikacji i oprogramowania układowego pomaga zapewnić, że aktualizacje są poprawną reprezentacją kopii wzorcowych utrzymywanych przez dewelopera i nie zostały naruszone podczas dystrybucji.

Zabezpieczenia powiązane: Brak.

(7) ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA | PERSONEL BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Wymaganie , aby [*Realizacja: zdefiniowani przez organizację* przedstawiciele ds. bezpieczeństwa i ochrony prywatności] byli włączeni do [*Realizacja: zdefiniowany przez organizację proces zarządzania zmianą konfiguracji i zabezpieczeń*].

Omówienie: W skład przedstawicieli ds. bezpieczeństwa informacji i prywatności mogą wchodzić SSO, SAISO, SAOP i SPO.[97] Uczestnictwo w procesie zarządzania zmianami konfiguracji i zabezpieczeń personelu posiadającego wiedzę z zakresu bezpieczeństwa informacji i ochrony prywatności jest istotne, ponieważ zmiany konfiguracji systemu mogą mieć niezamierzone skutki uboczne, z których niektóre mogą mieć znaczenie dla bezpieczeństwa lub ochrony prywatności. Wykrycie takich zmian we wczesnym etapie procesu może pomóc w uniknięciu niezamierzonych, negatywnych konsekwencji, które mogłyby ostatecznie wpłynąć na bezpieczeństwo i prywatność systemów. Proces zarządzania zmianami konfiguracji i zabezpieczeń wymagany przez zabezpieczenie rozszerzone SA-10(7) odnosi się do procesu zarządzania określonego przez organizacje w zabezpieczeniu podstawowym SA-10b.

Zabezpieczenia powiązane: Brak.

Referencje: [FIPS 140-3], [FIPS 180-4], [FIPS 202], [NIST SP 800-128], [NIST SP 800-160-1].

[97] Patrz: NSC 800-37; NSC 7298.

SA-11 TESTOWANIE I OCENA PRZEZ DEWELOPERA

Zabezpieczenie podstawowe: Wymaganie, aby twórca systemu, komponentu systemu lub usługi systemowej, realizujący wszystkie etapy powykonawcze w cyklu życia systemu, był zobowiązany do:

a. Opracowania i wdrożenia planu bieżącej oceny bezpieczeństwa i ochrony prywatności;

b. Wykonania [*Wybór (jeden lub więcej): jednostkowe; integracyjne; systemowe; regresyjne*] testowania/oceny z [Realizacja: *częstotliwość zdefiniowana przez organizację*] w [*Realizacja: wielostopniowość i zakres zdefiniowane przez organizację*];

c. Przedstawienia dowodów wykonania planu oceny oraz wyniki przeprowadzonych badań i ocen;

d. Wdrożenia możliwego do zweryfikowania procesu usuwania zagrożeń; oraz

e. Poprawienia błędów wykrytych podczas badań i oceny.

Omówienie: Testy rozwojowe i ocena potwierdzają, że wymagane zabezpieczenia są wdrażane prawidłowo, działają zgodnie z założeniami, egzekwując pożądaną politykę bezpieczeństwa i ochrony prywatności oraz spełniając ustalone wymogi bezpieczeństwa i ochrony prywatności. Wzajemne połączenie elementów systemu lub zmiany w tych elementach mogą mieć wpływ na bezpieczeństwo i prywatność osób. Wzajemne połączenia lub zmiany - w tym modernizacja lub wymiana aplikacji, systemów operacyjnych i oprogramowania układowego - mogą mieć negatywny wpływ na wcześniej wdrożone zabezpieczenia. Prowadzenie bieżącej oceny w procesie rozwoju pozwala na przeprowadzanie dodatkowych rodzajów testów i ocen, które twórcy oprogramowania mogą wykonywać w celu ograniczenia lub wyeliminowania potencjalnych wad. Testowanie aplikacji oprogramowania niestandardowego może wymagać takich metod, jak ręczny przegląd kodu, przegląd

architektury bezpieczeństwa i testy penetracyjne, a także analiza statyczna, dynamiczna, binarna lub hybrydowa tych trzech metod analizy.

Deweloperzy mogą stosować podejścia analityczne, wraz z wykorzystaniem oprzyrządowania bezpieczeństwa i testowaniem odporności na błędne dane (*ang. fuzzing*), przy użyciu różnych narzędzi i podczas przeglądów kodu źródłowego. Plany oceny bezpieczeństwa i ochrony prywatności obejmują określone działania, które deweloperzy planują przeprowadzić, w tym rodzaje analiz, testowania, oceny i przeglądów komponentów oprogramowania i oprogramowania układowego; stopień rygoru, jaki ma być zastosowany; częstotliwość bieżącego testowania i oceny; oraz rodzaje artefaktów wytworzonych podczas tych procesów. Szczegółowość testowania i oceny odnosi się do rygoru i poziomu szczegółowości związanego z procesem oceny. Zakres testowania i oceny odnosi się do zakresu (tj. liczby i rodzaju) artefaktów uwzględnionych w procesie oceny. Umowy określają kryteria akceptacji dla planów oceny bezpieczeństwa i prywatności, procesy usuwania wad oraz dowody na to, że plany i procesy zostały sumiennie zrealizowane. Metody przeglądu i ochrony planów oceny, dowodów i dokumentacji są współmierne do kategorii bezpieczeństwa lub poziomu klauzuli niejawności systemu. Umowy mogą określać wymagania dotyczące ochrony dokumentacji.

Zabezpieczenia powiązane: CA-2, CA-7, CM-4, SA-3, SA-4, SA-5, SA-8, SA-15, SA-17, SI-2, SR-5, SR-6, SR-7.

Zabezpieczenia rozszerzone:

(1) TESTOWANIE I OCENA PRZEZ DEWELOPERA | ANALIZA KODU STATYCZNEGO

Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej zastosowania narzędzi do analizy kodu statycznego w celu zidentyfikowania typowych błędów i udokumentowania wyników analizy.

Omówienie: Statyczna analiza kodu wykorzystuje technologię i metodologię przeglądów bezpieczeństwa i obejmuje sprawdzanie błędów w kodzie, jak również włączanie bibliotek lub innego kodu ze znanymi podatnościami lub

takiego, który jest przestarzały i niewspierany. Statyczna analiza kodu może być używana do identyfikacji podatności i egzekwowania praktyk bezpiecznego kodowania. Jest ona najbardziej efektywna, gdy jest stosowana we wczesnym etapie rozwoju oprogramowania, kiedy każda zmiana kodu może być automatycznie skanowana w poszukiwaniu potencjalnych niedoskonałości. Statyczna analiza kodu może dostarczyć czytelnych wskazówek naprawczych i zidentyfikować defekty, które programiści muszą naprawić. Dowodem na prawidłowe wdrożenie analizy statycznej może być zagregowana liczebność defektów dla krytycznych typów błędów, dowody na to, że błędy zostały sprawdzone przez deweloperów lub profesjonalistów ds. bezpieczeństwa oraz dowody na to, że błędy zostały naprawione. Wysoka gęstość zignorowanych wyników, powszechnie określanych jako fałszywie pozytywne, wskazuje na potencjalny problem z procesem analizy lub narzędziem analitycznym. W takich przypadkach, organizacje poddają analizie ważność dowodów w odniesieniu do dowodów pochodzących z innych źródeł.

Zabezpieczenia powiązane: Brak.

(2) TESTOWANIE I OCENA PRZEZ DEWELOPERA | MODELOWANIE ZAGROŻEŃ I ANALIZA PODATNOŚCI

Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej przeprowadzenia modelowania zagrożeń i analiz podatności na zagrożenia w trakcie opracowywania systemu, a następnie testowania i oceny wykonanego systemu, komponentu lub usługi:

(a) Wykorzystując następujące informacje kontekstowe: [***Realizacja: określone przez organizację informacje dotyczące wpływu, środowiska działania, znanych lub zakładanych zagrożeń oraz dopuszczalnych poziomów ryzyka***]**;**

(b) Stosując następujące narzędzia i metody: [***Realizacja: narzędzia i metody zdefiniowane przez organizację***]**;**

(c) Przeprowadzając modelowanie i analizy na następującym poziomie rygoru: [***Realizacja: określony przez organizację zakres i głębokość modelowania i analiz***]***;*** **oraz**

(d) Przedstawiając dowody, które spełniają następujące kryteria akceptacji: [***Realizacja: określone przez organizację kryteria akceptacji***]**.**

Omówienie: Systemy, komponenty systemu i usługi systemowe mogą znacznie odbiegać od specyfikacji funkcjonalnych i projektowych stworzonych w trakcie wymagań i etapów projektowania cyklu życia systemu. Dlatego też aktualizacje modelowania zagrożeń i analizy podatności tych systemów, komponentów systemu i usług systemowych w trakcie rozwoju i przed dostawą, mają kluczowe znaczenie dla efektywnego działania tych systemów, komponentów i usług. Modelowanie zagrożeń i analizy podatności na tym etapie cyklu życia systemu zapewniają, że zmiany w projekcie i wdrożeniu zostały uwzględnione oraz, że podatności powstałe w wyniku tych zmian zostały poddane przeglądowi i złagodzone.

Zabezpieczenia powiązane: PM-15, RA-3, RA-5.

(3) TESTOWANIE I OCENA PRZEZ DEWELOPERA | NIEZALEŻNA WERYFIKACJA PLANÓW OCENY / EWIDENCJA

a) Wymaganie, aby niezależny organ spełniający [*Realizacja: kryteria niezależności określone przez organizację*] zweryfikował prawidłowe wdrożenie przez dewelopera planów oceny bezpieczeństwa i ochrony prywatności oraz dowodów przedstawionych podczas testów i oceny; oraz

b) Sprawdzanie, czy niezależny organ uzyskał wystarczające informacje do zakończenia procesu weryfikacji lub udzielono mu upoważnienia do uzyskania takich informacji.

Omówienie: Niezależne organy posiadają kwalifikacje - w tym wiedzę fachową, umiejętności, szkolenia, certyfikaty i doświadczenie - pozwalające na weryfikację

prawidłowego wdrożenia przez deweloperów planów oceny bezpieczeństwa i ochrony prywatności.

Zabezpieczenia powiązane: AT-3, RA-5.

(4) TESTOWANIE I OCENA PRZEZ DEWELOPERA | MANUALNY PRZEGLĄD KODU

Wymaganie, aby deweloper systemu, komponentu systemu lub usługi systemowej wykonał ręczny przegląd kodu [***Realizacja: specyficzny kod zdefiniowany przez organizację***] **przy użyciu następujących procesów, procedur i/lub technik:** [***Realizacja: zdefiniowane przez organizację procesy, procedury i/lub techniki***]**.**

Omówienie: Ręczne przeglądy kodu są zazwyczaj zarezerwowane dla krytycznych komponentów oprogramowania i firmware'u systemów. Ręczne przeglądy kodu skutecznie identyfikują słabe punkty, które wymagają znajomości wymagań aplikacji lub kontekstu, który w większości przypadków jest niedostępny dla automatycznych narzędzi i technik analitycznych, takich jak analiza statyczna i dynamiczna. Korzyści płynące z ręcznego przeglądu kodu obejmują możliwość weryfikacji matryc kontroli dostępu w odniesieniu do zabezpieczeń aplikacji oraz przegląd szczegółowych aspektów wdrożeń i zabezpieczeń kryptograficznych.

Zabezpieczenia powiązane: Brak.

(5) TESTOWANIE I OCENA PRZEZ DEWELOPERA | TESTOWANIE PENETRACYJNE

Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej przeprowadzenia testów penetracyjnych:

(a) Na poniższym poziomie rygoru: [***Realizacja: określony przez organizację zakres i głębokość badania***]**; oraz**

(b) Pod następującymi warunkami: [***Realizacja: ograniczenia zdefiniowane przez organizację***]**.**

Omówienie: Testy penetracyjne to metodologia oceny, w której osoby oceniające, wykorzystując całą dostępną dokumentację produktów lub systemów

informatycznych i pracując w określonych warunkach, próbują obejść wdrożone zabezpieczenia i środki ochrony prywatności produktów i systemów informatycznych. Informacje przydatne dla osób oceniających, które przeprowadzają testy penetracyjne, obejmują specyfikacje projektu produktu i systemu, kod źródłowy oraz instrukcje dla administratora i operatora. Testy penetracyjne mogą obejmować testy *white-box, gray-box lub black-box* z analizami przeprowadzanymi przez wykwalifikowanych specjalistów, którzy symulują działania przeciwników. Celem testów penetracyjnych jest wykrycie luk w systemach, komponentach systemu i usługach, które wynikają z błędów wdrożeniowych, błędów w konfiguracji lub innych podatności lub braków operacyjnych. Testy penetracyjne mogą być wykonywane w połączeniu ze zautomatyzowanymi i ręcznymi przeglądami kodu w celu zapewnienia wyższego poziomu analizy niż jest to zazwyczaj możliwe. W przypadku pozyskiwania lub utrwalania podczas testów penetracyjnych informacji o sesji użytkownika oraz innych informacji umożliwiających identyfikację osoby, informacje te są odpowiednio traktowane w celu zapewnienia ochrony prywatności.

Zabezpieczenia powiązane: CA-8, PM-14, PM-25, PT-2, SA-3 , SI-6.

(6) TESTOWANIE I OCENA PRZEZ DEWELOPERA | PRZEGLĄD PŁASZCZYZNY ATAKU

Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej wykonania przeglądu płaszczyzny ataku.

Omówienie: Powierzchnie ataku systemów i ich komponentów to eksponowane obszary, które czynią te systemy bardziej podatnymi na ataki. Powierzchnie ataku obejmują wszelkie dostępne obszary, w których błędy lub braki w sprzęcie, oprogramowaniu i komponentach firmware'u dają przeciwnikom możliwość wykorzystania podatności. Przeglądy powierzchni ataku zapewniają, że deweloperzy analizują zmiany projektowe i implementacyjne w systemach i łagodzą wektory ataków powstałe w wyniku tych zmian. Korekta zidentyfikowanych błędów obejmuje eliminację niebezpiecznych funkcji.

Zabezpieczenia powiązane: SA-15.

(7) TESTOWANIE I OCENA PRZEZ DEWELOPERA | WERYFIKACJA ZAKRESU TESTU / OCENA

Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej sprawdzenia, czy zakres testów i oceny obejmuje wszystkie wymagane zabezpieczenia na następującym poziomie rygoru: [***Realizacja: określony przez organizację zakres i głębokość testów i oceny***]**.**

Omówienie: W celu sprawdzenia, czy testowanie i ocena obejmują wszystkie wymagane zabezpieczenia, można zastosować różne techniki analityczne, od nieformalnych po formalne. Każda z tych technik zapewnia coraz wyższy poziom pewności, który odpowiada poziomowi formalności analizy. Rygorystyczne zademonstrowanie pokrycia zabezpieczeń na najwyższych poziomach pewności może być osiągnięte przy użyciu technik formalnego modelowania i analizy, w tym korelacji pomiędzy implementacją zabezpieczeń i odpowiadającymi im przypadkami testowymi.

Zabezpieczenia powiązane: SA-15.

(8) TESTOWANIE I OCENA PRZEZ DEWELOPERA | DYNAMICZNA ANALIZA KODU

Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej zastosowania narzędzi dynamicznej analizy kodu w celu zidentyfikowania wspólnych błędów i udokumentowania wyników analizy.

Omówienie: Dynamiczna analiza kodu umożliwia weryfikację działania programów przy użyciu narzędzi pozwalających na monitorowanie programów pod kątem uszkodzeń pamięci, problemów z uprawnieniami użytkowników i innych potencjalnych problemów z bezpieczeństwem. Dynamiczna analiza kodu wykorzystuje narzędzia uruchomieniowe (*ang. run-time*) w celu zapewnienia, że funkcjonalność bezpieczeństwa działa w sposób, w jaki została zaprojektowana. Rodzaj dynamicznej analizy, znany jako testowanie odporności na błędne dane

(*ang. fuzz testing*), powoduje awarie programów poprzez celowe wprowadzanie do programów zniekształconych lub przypadkowych danych. Strategie *fuzz testing* pochodzą z zamierzonego wykorzystania aplikacji oraz specyfikacji funkcjonalnych i projektowych aplikacji. W celu zrozumienia zakresu dynamicznej analizy kodu i udzielanej gwarancji, organizacje mogą również rozważyć przeprowadzenie analizy pokrycia kodu (tj. sprawdzenie stopnia, w jakim kod został przetestowany przy użyciu metryki takiej jak procent testowanych podprogramów lub procent deklaracji programu wywołanych podczas wykonywania pakietu testowego) i/lub analizy zgodności (tj. sprawdzenie, czy w kodzie oprogramowania nie ma słów, które są nie na swoim miejscu, takich jak słowa w języku innym niż angielski lub terminy obraźliwe).

Zabezpieczenia powiązane: Brak.

(9) TESTOWANIE I OCENA PRZEZ DEWELOPERA | INTERAKTYWNE TESTOWANIE BEZPIECZEŃSTWA APLIKACJI

Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej zastosowania interaktywnych narzędzi do testowania bezpieczeństwa aplikacji w celu zidentyfikowania wad i udokumentowania wyników.

Omówienie: Interaktywne (znane również jako oparte na oprzyrządowaniu) testowanie bezpieczeństwa aplikacji jest metodą wykrywania podatności poprzez obserwację aplikacji w trakcie jej działania podczas testów. Wykorzystanie oprzyrządowania opiera się na bezpośrednich pomiarach faktycznie działających aplikacji i wykorzystuje dostęp do kodu, interakcji użytkownika, bibliotek, struktur, połączeń wstecznych i konfiguracji, aby bezpośrednio zmierzyć skuteczność zabezpieczeń. W połączeniu z technikami analizy, interaktywne testowanie bezpieczeństwa aplikacji może zidentyfikować szeroki zakres potencjalnych podatności i potwierdzić skuteczność zabezpieczeń. Testy oparte

na oprzyrządowaniu działają w czasie rzeczywistym i mogą być stosowane w sposób ciągły przez cały cykl życia systemu.

Zabezpieczenia powiązane: Brak.

Referencje: [ISO 15408-3], [NIST SP 800-30], [NIST SP 800-53A], [NIST SP 800-154], [NIST SP 800-160-1].

SA-12 BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW

[Wycofane: Włączone do: Kategoria SR].

Zabezpieczenia rozszerzone:

(1) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | STRATEGIE ZAKUPÓW, NARZĘDZIA, METODY

[Wycofane: Włączone do SR-5].

(2) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | PRZEGLĄD DOSTAWCÓW

[Wycofane: Włączone do SR-6].

(3) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | ZAUFANA WYSYŁKA I MAGAZYNOWANIE

[Wycofane: Włączone do SR-3].

(4) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | DYWERSYFIKACJA DOSTAWCÓW

[Wycofane: Włączone do SR-3(1)].

(5) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | OGRANICZENIE SZKODY

[Wycofane: Włączone do SR-3(2)].

(6) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | MINIMALIZACJA CZASU ZAMÓWIENIA

[Wycofane: Włączone do SR-5(1)].

(7) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | OCENY PRZED WYBOREM / ODBIOREM / AKTUALIZACJĄ

[Wycofane: Włączone do SR-5(2)].

(8) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | POZYSKIWANIE INFORMACJI Z WSZYSTKICH DOSTĘPNYCH ŹRÓDEŁ

[Wycofane: Włączone do RA-3(2)].

(9) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | BEZPIECZEŃSTWO OPERACYJNE

[Wycofane: Włączone do SR-7].

(10) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | OCENA ORYGINALNOŚCI I NIEZMIENNOŚCI

[Wycofane: Włączone do SR-4(3)].

(11) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | TESTOWANIE PENETRACYJNE / ANALIZA ELEMENTÓW, PROCESÓW I WYKONAWCÓW

[Wycofane: Włączone do SR-6(1)].

(12) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | UMOWY MIĘDZYORGANIZACYJNE

[Wycofane: Włączone do SR-8].

(13) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | KOMPONENTY KRYTYCZNE SYSTEMU INFORMATYCZNEGO

[Wycofane: Włączone do MA-6 i RA-9].

(14) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | IDENTYFIKACJA I ŚLEDZENIE

[Wycofane: Włączone do SR-4(1) i SR-4(2).

(15) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | MECHANIZMY ADRESOWANIA SŁABYCH STRON LUB WAD

[Wycofane: Włączone do SR-3].

SA-13 WIARYGODNOŚĆ

[Wycofane: Włączone do SA-8].

SA-14 ANALIZA KRYTYCZNOŚCI

[Wycofane: Włączone do RA-9].

Zabezpieczenia rozszerzone:

(1) ANALIZA KRYTYCZNOŚCI | KRYTYCZNE KOMPONENTY POZBAWIONE ALTERNATYWNEGO ŹRÓDŁA ZAOPATRZENIA

[Wycofane: Włączone do SA-20].

SA-15 PROCES ROZWOJU, STANDARDY I NARZĘDZIA

Zabezpieczenie podstawowe:

a. Wymaganie, aby deweloper systemu, komponentu systemu lub usługi systemowej przestrzegał udokumentowanego procesu rozwoju, który:

   1. Jednoznacznie odnosi się do wymogów bezpieczeństwa i ochrony prywatności;
   2. Określa standardy i narzędzia wykorzystywane w procesie rozwoju;
   3. Dokumentuje szczegółowe opcje i konfiguracje narzędzi używane w procesie rozwoju; oraz
   4. Dokumentuje, zarządza i zapewnia integralność zmian w procesie i/lub narzędziach wykorzystywanych w rozwoju; oraz

b. Przegląd procesu rozwoju, standardów, narzędzi, opcji narzędziowych oraz konfiguracji narzędzi [*Realizacja: częstotliwość zdefiniowana przez organizację*] w celu określenia czy wybrany i zastosowany proces, standardy, narzędzia, opcje narzędziowe oraz konfiguracje narzędziowe spełnią następujące wymagania dotyczące bezpieczeństwa i ochrony prywatności: [*Realizacja: zdefiniowane przez organizację wymagania dotyczące bezpieczeństwa i ochrony prywatności*].

Omówienie: Narzędzia deweloperskie obejmują języki programowania i wspomagane komputerowo systemy projektowania. Przeglądy procesów deweloperskich obejmują wykorzystanie modeli dojrzałości do określenia potencjalnej skuteczności takich procesów. Utrzymanie integralności zmian w narzędziach i procesach ułatwia skuteczną ocenę i ograniczanie ryzyka w łańcuchu dostaw. Integralność taka wymaga kontroli konfiguracji w całym cyklu życia systemu w celu śledzenia autoryzowanych zmian i zapobiegania nieautoryzowanym zmianom.

Zabezpieczenia powiązane: MA-6, SA-3, SA-4, SA-8, SA-10, SA-11, SR-3, SR-4, SR-5, SR-6, SR-9.

Zabezpieczenia rozszerzone:

(1) PROCES ROZWOJU, STANDARDY I NARZĘDZIA | METRYKI JAKOŚCI

Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej:

(a) Zdefiniowania wskaźników jakości na początku procesu rozwoju; oraz

(b) Przedstawienia dowodów potwierdzających spełnienie kryteriów jakości [***Wybór (jeden lub więcej)***]***:*** [***Realizacja: częstotliwość zdefiniowana przez organizację***]***;*** [***Realizacja: etapy przeglądu (kamienie milowe) programu zdefiniowane przez organizację***]***; po dostarczeniu***].

Omówienie: Organizacje wykorzystują metryki jakości w celu ustalenia akceptowalnych poziomów jakości systemu. Metryki mogą obejmować wskaźniki jakości, które są zbiorem kryteriów wykonania lub standardów wystarczalności, które reprezentują zadowalające wykonanie określonych faz projektu rozwoju systemu. Na przykład, wskaźnik jakości może wymagać wyeliminowania wszystkich ostrzeżeń kompilatora lub stwierdzenia, że takie ostrzeżenia nie mają wpływu na skuteczność wymaganych zdolności w zakresie bezpieczeństwa lub ochrony prywatności. W fazach realizacji projektów rozwojowych wskaźniki jakości dostarczają jasnych, jednoznacznych informacji o postępach. Inne metryki odnoszą się do całego projektu rozwojowego. Metryki mogą obejmować definiowanie progów istotności podatności zgodnie z tolerancją ryzyka organizacyjnego, np. wymóg braku znanych podatności w dostarczonym systemie o istotności średniej lub wysokiej według Common Vulnerability Scoring System (CVSS).

Zabezpieczenia powiązane: Brak.

(2) PROCES ROZWOJU, STANDARDY I NARZĘDZIA | NARZĘDZIA DO MONITOROWANIA BEZPIECZEŃSTWA I PRYWATNOŚCI

Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej wybrania i zastosowania narzędzia do śledzenia bezpieczeństwa i ochrony prywatności używanego podczas procesu programowania.

Omówienie: Zespoły zajmujące się rozwojem systemu wybierają i wdrażają narzędzia do śledzenia bezpieczeństwa i prywatności, w tym systemy śledzenia podatności lub elementów pracy ułatwiających przydzielanie, sortowanie, filtrowanie i śledzenie wykonanych elementów pracy lub zadań związanych z procesami rozwoju.

Zabezpieczenia powiązane: SA-11.

(3) PROCES ROZWOJU, STANDARDY I NARZĘDZIA | ANALIZA KRYTYCZNOŚCI

Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej przeprowadzenia analizy krytyczności:

(a) W poniższych punktach decyzyjnych w cyklu życia systemu: [***Realizacja: określone przez organizację punkty decyzyjne w cyklu życia systemu***]**; oraz**

(b) Na poniższym poziomie rygoru: [***Realizacja: zdefiniowany zakres organizacji i głębokość analizy krytyczności***]**.**

Omówienie: Analiza krytyczności przeprowadzona przez dewelopera stanowi wkład w analizę krytyczności przeprowadzaną przez organizacje. Wkład dewelopera jest niezbędny do analizy krytyczności organizacji, ponieważ organizacje mogą nie mieć dostępu do szczegółowej dokumentacji projektowej komponentów systemu, które są opracowywane jako produkty dostępne w sprzedaży komercyjnej. Taka dokumentacja projektowa zawiera specyfikacje funkcjonalne, projekty wysokiego poziomu, projekty niskiego poziomu, kod źródłowy i schematy sprzętowe. Analiza krytyczności jest ważna dla systemów organizacyjnych, które są oznaczone jako aktywa o wysokiej wartości. Aktywa

o wysokiej wartości mogą być systemami o umiarkowanym lub dużym wpływie podatności ze względu na zwiększone zainteresowanie przeciwników lub potencjalne negatywne skutki dla przedsiębiorstwa. Wkład dewelopera jest szczególnie ważny, gdy organizacje przeprowadzają analizy krytyczności łańcucha dostaw.

Zabezpieczenia powiązane: RA-9.

(4) PROCES ROZWOJU, STANDARDY I NARZĘDZIA | MODELOWANIE ZAGROŻEŃ / ANALIZA PODATNOŚCI

[Wycofane: Włączone do SA-11(2)].

(5) PROCES ROZWOJU, STANDARDY I NARZĘDZIA | OGRANICZANIE PŁASZCZYZNY ATAKU

Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej zmniejszenia powierzchni ataku do [***Realizacja: progi zdefiniowane przez organizację***]**.**

Omówienie: Redukcja powierzchni ataku jest ściśle powiązana z analizami zagrożeń i podatności oraz architekturą i projektowaniem systemu. Redukcja powierzchni ataku jest sposobem na zmniejszenie ryzyka dla organizacji poprzez zmniejszenie możliwości wykorzystania przez atakujących błędów i niedociągnięć (tj. potencjalnych podatności) w systemach, komponentach i usługach systemowych. Redukcja powierzchni ataku obejmuje wdrożenie koncepcji obrony warstwowej, stosowanie zasad najmniejszego przywileju i najmniejszej funkcjonalności, stosowanie bezpiecznych praktyk tworzenia oprogramowania, usuwanie niebezpiecznych funkcji, redukcję punktów dostępowych umożliwiających ich wykorzystanie przez nieuprawnionych użytkowników, redukcję ilości wykonywanego kodu oraz eliminację interfejsów programowania aplikacji (API), które są podatne na ataki.

Zabezpieczenia powiązane: AC-6, CM-7, RA-3, SA-11.

(6) PROCES ROZWOJU, STANDARDY I NARZĘDZIA | CIĄGŁE DOSKONALENIE

Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej wdrożenia jasno sprecyzowanego mechanizmu ciągłego doskonalenia procesu rozwoju.

Omówienie: Deweloperzy systemów, komponentów systemów i usług systemowych rozważają skuteczność i wydajność wdrażanych procesów rozwojowych pod kątem spełniania celów jakościowych oraz możliwości zapewnienia bezpieczeństwa i ochrony prywatności w aktualnych środowiskach zagrożeń.

Zabezpieczenia powiązane: Brak.

(7) PROCES ROZWOJU, STANDARDY I NARZĘDZIA | AUTOMATYCZNA ANALIZA PODATNOŚCI

Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej [***Realizacja: częstotliwość określona przez organizację***]**:**

(a) Przeprowadzania automatycznej analizy podatności przy użyciu [***Realizacja: narzędzia zdefiniowane przez organizację***]***;***

(b) Określania potencjału wykorzystania zidentyfikowanych podatnosci;

(c) Określania potencjalnych środków ograniczających ryzyko związane z wykrytymi podatnościami; oraz

(d) Dostarczania danych wyjściowych z narzędzi i wyników analizy do [***Realizacja: personel lub role zdefiniowane przez organizację***]**.**

Omówienie: Zautomatyzowane narzędzia mogą być bardziej skuteczne w analizowaniu możliwych do wykorzystania podatności lub braków w dużych i złożonych systemach, nadawaniu priorytetu podatnościom według ich wagi oraz dostarczaniu zaleceń dotyczących ograniczania ryzyka.

Zabezpieczenia powiązane: RA-5, SA-11.

(8) PROCES ROZWOJU, STANDARDY I NARZĘDZIA | PONOWNIE UŻYCIE INFORMACJI O ZAGROŻENIACH I PODATNOŚCI

Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej wykorzystywania modelowania zagrożeń i analizy podatności z adekwatnych systemów, komponentów lub usług do informowania o bieżącym procesie rozwoju.

Omówienie: Analiza podatności wykrytych w adekwatnych aplikacjach może stanowić źródło informacji na temat potencjalnych problemów projektowych i wdrożeniowych opracowywanych systemów. Podobne systemy lub elementy systemu mogą istnieć w organizacjach deweloperskich. Informacje o podatnościach są dostępne w różnych źródłach sektora publicznego i prywatnego, w tym np. w NIST National Vulnerability Database.

Zabezpieczenia powiązane: Brak.

(9) PROCES ROZWOJU, STANDARDY I NARZĘDZIA | KREATYWNE WYKORZYSTANIE DANYCH

[Wycofane: Włączone do SA-3(2)].

(10) PROCES ROZWOJU, STANDARDY I NARZĘDZIA | PLAN ODPOWIEDZI NA INCYDENT

Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej dostarczenia, wdrożenia i przetestowania planu reagowania na incydenty.

Omówienie: Plan reagowania na incydenty przekazany przez deweloperów może dostarczać informacje, które nie są łatwo dostępne dla organizacji i być włączony do organizacyjnych planów reagowania na incydenty. Informacje te mogą być również niezwykle pomocne, np. gdy organizacje podejmują działania w związku z podatnościami występującymi w dostępnych produktach komercyjnych.

Zabezpieczenia powiązane: IR-8.

(11) PROCES ROZWOJU, STANDARDY I NARZĘDZIA | ARCHIWIZACJA SYSTEMU LUB KOMPONENTU

Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej dokonania archiwizacji wydanego / dostarczonego systemu lub komponentu wraz z odpowiednimi dowodami wskazującymi na przeprowadzenie końcowego przeglądu bezpieczeństwa i ochrony prywatności.

Omówienie: Archiwizacja systemu lub komponentów systemu wymaga od dewelopera zachowania kluczowych artefaktów rozwojowych, w tym specyfikacji sprzętowej, kodu źródłowego, kodu obiektu oraz odpowiedniej dokumentacji z procesu rozwoju, która może dostarczyć łatwo dostępną bazę konfiguracji do aktualizacji lub modyfikacji systemu i komponentów.

Zabezpieczenia powiązane: CM-2.

(12) PROCES ROZWOJU, STANDARDY I NARZĘDZIA | MINIMALIZACJA INFORMACJI UMOŻLIWIAJĄCYCH IDENTYFIKACJĘ OSOBY

Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej, aby zminimalizował wykorzystywanie danych osobowych w środowiskach rozwojowych i testowych.

Omówienie: Organizacje mogą zminimalizować zagrożenie prywatności osób poprzez zastosowanie technik anonimizacji danych, takich jak deidentyfikacja lub dane syntetyczne. Ograniczenie wykorzystania informacji umożliwiających identyfikację osób w środowiskach rozwojowych i testowych pomaga zmniejszyć poziom zagrożenia prywatności stwarzanego przez system.

Zabezpieczenia powiązane: PM-25, SA-3, SA-8.

Referencje: [NIST SP 800-160-1], [IR 8179].

SA-16 SZKOLENIA PROWADZONE PRZEZ DEWELOPERA

Zabezpieczenie podstawowe: Wymaganie od deweloperów systemu, komponentu systemu lub usługi systemowej przeprowadzenia następującego szkolenia w zakresie właściwego użytkowania i obsługi wdrożonych, zabezpieczeń i/lub mechanizmów funkcji bezpieczeństwa i ochrony prywatności: [*Realizacja: szkolenie określone przez organizację*].

Omówienie: Szkolenie dla deweloperów zewnętrznych i wewnętrznych. Szkolenie personelu jest niezbędne do zapewnienia skuteczności zabezpieczeń realizowanych w ramach systemów organizacyjnych. Rodzaje szkoleń obejmują szkolenia internetowe i komputerowe, szkolenia w salach wykładowych oraz szkolenia praktyczne (w tym mikroszkolenia). Organizacje mogą również zamówić materiały szkoleniowe od deweloperów w celu przeprowadzenia szkoleń wewnętrznych lub zaoferować personelowi organizacji samodzielne szkolenia. Organizacje określają rodzaj niezbędnych szkoleń i mogą wymagać różnych rodzajów szkoleń w zakresie różnych funkcji, zabezpieczeń i mechanizmów bezpieczeństwa i ochrony prywatności.

Zabezpieczenia powiązane: AT-2, AT-3, PE-3, SA-4, SA-5.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

SA-17 ARCHITEKTURA ORAZ PROJEKT BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI DEWELOPERA

Zabezpieczenie podstawowe: Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej opracowania specyfikacji projektu oraz architektury J i ochrony prywatności, która:

a. Jest zgodna z architekturą bezpieczeństwa i ochrony prywatności organizacji stanowiącą integralną część jej architektury korporacyjnej;

b. Dokładnie i wyczerpująco opisuje wymagane funkcje bezpieczeństwa i ochrony prywatności oraz podział zabezpieczeń pomiędzy elementami fizycznymi i logicznymi; oraz

c. Wyraża, w jaki sposób poszczególne funkcje, mechanizmy i usługi w zakresie bezpieczeństwa i ochrony prywatności współdziałają ze sobą w celu zapewnienia wymaganych zdolności w zakresie bezpieczeństwa i ochrony prywatności oraz jednolitego podejścia do ochrony.

Omówienie: Architektura i projekt bezpieczeństwa i ochrony prywatności deweloperów są skierowane do deweloperów zewnętrznych, choć mogą być również stosowane do rozwoju wewnętrznego. Natomiast zabezpieczenie PL-8 jest skierowane do deweloperów wewnętrznych, aby zapewnić, że organizacje opracowują architekturę bezpieczeństwa i ochrony prywatności, która jest zintegrowana z architekturą korporacyjną. Rozróżnienie pomiędzy zabezpieczeniami SA-17 i PL-8 jest szczególnie ważne, gdy organizacje zlecają na zewnątrz rozwój systemów, komponentów systemu lub usług systemowych oraz gdy istnieje wymóg wykazania zgodności z architekturą korporacyjną oraz architekturą bezpieczeństwa i ochrony prywatności organizacji. [ISO 15408-2], [ISO 15408-3], oraz [NIST SP 800-160-1] dostarczają informacji na temat architektury bezpieczeństwa i projektowania, w tym formalnych modeli polityki, komponentów istotnych dla bezpieczeństwa, formalnej i nieformalnej korespondencji, koncepcyjnie prostego projektowania oraz strukturyzacji w celu zapewnienia jak najmniejszego uprzywilejowania i testowania.

Zabezpieczenia powiązane: PL-2, PL-8, PM-7, SA-3, SA-4, SA-8, SC-7.

Zabezpieczenia rozszerzone:

(1) ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | FORMALNY MODEL POLITYKI

Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej:

(a) Opracowania, jako integralnej części procesu rozwoju, formalnego modelu polityki opisującego [***Realizacja: zdefiniowane przez organizację elementy polityki bezpieczeństwa i ochrony prywatności***]**, które mają być egzekwowane; oraz**

(b) Wykazanie, że formalny model polityki jest wewnętrznie spójny i wystarczający do egzekwowania określonych elementów polityki bezpieczeństwa i ochrony prywatności organizacji po zakończeniu wdrożenia.

Omówienie: Modele formalne opisują poszczególne zachowania lub zasady bezpieczeństwa i ochrony prywatności przy użyciu sformalizowanych języków, umożliwiając w ten sposób oficjalne potwierdzenie poprawności tych zachowań i zasad. Nie wszystkie komponenty systemów mogą być modelowane. Generalnie, formalne specyfikacje są ograniczone do zachowań lub polityk będących przedmiotem zainteresowania, takich jak niedyskrecjonalne polityki kontroli dostępu. Organizacje wybierają język modelowania formalnego i podejście oparte na naturze zachowań i zasad, które mają być opisane oraz na dostępnych narzędziach.

Zabezpieczenia powiązane: AC-3, AC-4, AC-25.

(2) ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | BAZOWE ELEMENTY BEZPIECZEŃSTWA

Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej:

(a) Zdefiniowania sprzętu, aplikacji i oprogramowania układowego istotnego dla bezpieczeństwa; oraz

(b) Przedstawienie uzasadnienia, że zdefiniowany sprzętu, aplikacje i oprogramowanie układowe mające znaczenie dla bezpieczeństwa jest kompletne.

Omówienie: Sprzęt, oprogramowanie i oprogramowanie układowe istotne z punktu widzenia bezpieczeństwa stanowią te składniki systemu, komponentu lub usługi, którym można zaufać, że działają prawidłowo w celu zachowania wymaganych właściwości bezpieczeństwa.

Zabezpieczenia powiązane: AC-25, SA-5.

(3) ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | FORMALNA SPECYFIKACJA

Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej:

(a) Opracowania, jako integralnej części procesu rozwoju systemu, formalnej specyfikacji najwyższego poziomu, która określa interfejsy do sprzętu, aplikacji i oprogramowania układowego istotne z punktu widzenia bezpieczeństwa powiązane merytorycznie z wyjątkami, komunikatami o błędach i skutkami;

(b) Wykazania za pomocą możliwego do przeprowadzenia dowodu, a w razie potrzeby dodatkowo z nieformalną prezentacją, że istniejąca specyfikacja najwyższego poziomu jest zgodna z formalnym modelem polityki;

(c) Wykazania poprzez nieformalną prezentację, że formalna specyfikacja najwyższego poziomu obejmuje interfejsy z istotnym dla bezpieczeństwa sprzętem, aplikacjami i oprogramowaniem układowym;

(d) Wykazania, że formalna specyfikacja najwyższego poziomu jest dokładnym opisem zaimplementowanego, związanego z bezpieczeństwem sprzętu, aplikacji i oprogramowania układowego; oraz

(e) Opisania mechanizmów związanych z bezpieczeństwem sprzętu, aplikacji i oprogramowania układowego, które nie zostały uwzględnione w formalnej specyfikacji najwyższego poziomu, ale ściśle dotyczą sprzętu, aplikacji i oprogramowania układowego związanego z bezpieczeństwem.

Omówienie: Zgodność jest istotną częścią pewności uzyskanej poprzez modelowanie. Wykazuje ona, że implementacja jest dokładnym przekształceniem modelu, oraz że każdy dodatkowy kod lub szczegóły implementacji, które są dostępne, nie mają wpływu na modelowane zachowania lub polityki. Metody formalne mogą być wykorzystane do wykazania, że właściwości bezpieczeństwa wysokiego poziomu są spełnione przez formalny opis systemu, oraz że formalny opis systemu jest poprawnie zaimplementowany przez charakterystykę niższego poziomu, w tym opis sprzętu. Spójność między formalną specyfikacją najwyższego poziomu, a formalnymi modelami polityki nie jest na ogół możliwa do pełnego udowodnienia. Dlatego do wykazania takiej spójności może być potrzebne połączenie metod formalnych i nieformalnych. Spójność między formalną specyfikacją głównego poziomu, a rzeczywistym wdrożeniem może wymagać użycia nieformalnej demonstracji wynikającej z ograniczeń w stosowalności metod formalnych w celu udowodnienia, że specyfikacja dokladnie odzwierciedla wdrożenie. Mechanizmy sprzętowe, softwarowe i firmware'owe występujące wewnątrz komponentów istotnych z punktu widzenia bezpieczeństwa obejmują rejestry odwzorowujące oraz bezpośrednie wejście i wyjście z pamięci.

Zabezpieczenia powiązane: AC-3, AC-4, AC-25, SA-4, SA-5.

(4) ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | NIEFORMALNE SPECYFIKACJE

Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej:

(a) Opracowania, jako integralnej części procesu rozwoju, nieformalnej opisowej specyfikacji najwyższego poziomu, która określa interfejsy sprzętowe istotne z punktu widzenia bezpieczeństwa, aplikacje oraz oprogramowanie układowe powiązane merytorycznie z wyjątkami, komunikatami o błędach i skutkami;

(b) Wykazania poprzez [*Realizacja: nieformalna prezentacja, przekonujący argument metodami formalnymi, jeśli jest to wykonalne*], że opisowa specyfikacja najwyższego poziomu jest zgodna z formalnym modelem polityki;

(c) Wykazania że opisowa specyfikacja najwyższego poziomu obejmuje interfejsy z istotnym dla bezpieczeństwa sprzętem, aplikacjami i oprogramowaniem układowym; oraz

(d) Opisania mechanizmów związanych z bezpieczeństwem sprzętu, aplikacji i oprogramowania układowego, które nie zostały wykazane w opisowej specyfikacji najwyższego poziomu, ale ściśle dotyczą sprzętu, oprogramowania i oprogramowania układowego związanego z bezpieczeństwem.

Omówienie: Zgodność jest ważną częścią pewności uzyskanej poprzez modelowanie. Wykazuje ona, że implementacja jest dokładnym przekształceniem modelu oraz, że dodatkowy kod lub szczegóły implementacji nie mają wpływu na modelowane zachowania lub polityki. Spójność pomiędzy opisową specyfikacją najwyższego poziomu (tj. projekt wysokiego/niskiego poziomu), a formalnym modelem polityki nie jest zazwyczaj możliwa do pełnego udowodnienia. Dlatego do wykazania takiej spójności może być potrzebne połączenie metod formalnych i

nieformalnych. Mechanizmy sprzętowe, software'owe i firmware'owe, pozostające w ścisłym związku ze sprzętem, oprogramowaniem i firmware'em mającym znaczenie dla bezpieczeństwa, obejmują rejestry odwzorowujące oraz bezpośrednie wejście i wyjście z pamięci.

Zabezpieczenia powiązane: AC-3, AC-4, AC-25, SA-4, SA-5.

(5) ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | PROJEKT PROSTY KONCEPCYJNIE

Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej:

(a) Projektowania i konstruowania istotnego dla bezpieczeństwa sprzętu, aplikacji i oprogramowania układowego w celu wykorzystania kompletnego, koncepcyjnie prostego mechanizmu ochrony z precyzyjnie zdefiniowaną semantyką; oraz

(b) Ustrukturyzowania wewnętrznie istotnego dla bezpieczeństwa sprzętu, aplikacji i oprogramowania układowego, ze szczególnym uwzględnieniem tego mechanizmu.

Omówienie: Zasada zredukowanej złożoności mówi, że projekt systemu jest tak prosty i minimalny, jak to tylko możliwe (patrz zabezpieczenie SA-8(7)). Taki projekt jest łatwiejszy do zrozumienia i analizy, a także jest mniej podatny na błędy (patrz zabezpieczenia AC-25, SA-8(13)). Zasada zredukowanej złożoności odnosi się do każdego aspektu systemu, ale ma szczególne znaczenie dla bezpieczeństwa ze względu na różne analizy wykonywane w celu uzyskania dowodów na temat występujących właściwości bezpieczeństwa systemu. Aby takie analizy były skuteczne, niezbędny jest minimalny i prosty projekt. Zastosowanie zasady zredukowanej złożoności przyczynia się do zwiększenia zdolności deweloperów systemów do zrozumienia poprawności i kompletności funkcji bezpieczeństwa systemu oraz ułatwia identyfikację potencjalnych podatności. Następstwo zasady zredukowanej złożoności mówi, że prostota

systemu jest bezpośrednio związana z liczbą podatności, które będzie on zawierał. Oznacza to, że prostsze systemy zawierają mniej podatności. Ważną korzyścią wynikającą ze zredukowanej złożoności jest to, że łatwiej jest zrozumieć, czy polityka bezpieczeństwa została uwzględniona w projekcie systemu oraz, że mniej podatności zostanie prawdopodobnie wprowadzonych podczas opracowywania systemu. Dodatkową korzyścią jest to, że każdy taki wniosek dotyczący poprawności, kompletności i istnienia podatności może być wyciągnięty z większym stopniem pewności w przeciwieństwie do wniosków wyciągniętych w sytuacjach, gdy projekt systemu jest z natury bardziej złożony.

Zabezpieczenia powiązane: AC-25, SA-8, SC-3.

(6) ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | STRUKTURA DO TESTOWANIA

Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej aby ustrukturyzowała sprzęt, aplikacje i oprogramowanie układowe istotne dla bezpieczeństwa w celu ułatwienia testowania.

Omówienie: Stosowanie zasad projektowania bezpieczeństwa zawartych w publikacji [NIST SP 800-160-1] promuje pełne, spójne i kompleksowe testowanie i ocenę systemów, komponentów systemów i usług. Szczegółowość takiego testowania przyczynia się do uzyskania dowodów, które pozwalają na wygenerowanie skutecznego poświadczenia lub argumentu co do wiarygodności systemu, komponentu systemu lub usługi..

Zabezpieczenia powiązane: SA-5, SA-11.

(7) ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | STRUKTURA NAJNIŻSZYCH UPRAWNIEŃ

Wymaganie od dewelopera systemu, komponentu systemu lub usługi systemowej stworzenia struktury sprzętu, aplikacji i oprogramowania

układowego istotnego dla bezpieczeństwa w celu ułatwienia kontroli dostępu z jak najmniejszymi uprawnieniami.

Omówienie: Zasada najmniejszych uprawnień stanowi, że każdemu komponentowi przydzielane są uprawnienia wystarczające do realizacji jego określonych funkcji, jednakże nie wykraczające poza nie (patrz SA-8(14)). Stosowanie zasady najmniejszych uprawnień ogranicza zakres działań komponentu, co ma dwa pożądane efekty. Po pierwsze, wpływ awarii, uszkodzenia lub niewłaściwego użycia komponentu systemu na bezpieczeństwo jest zminimalizowany. Po drugie, analiza bezpieczeństwa komponentu jest uproszczona. Najniższe uprawnienia są wszechobecną zasadą, która jest odzwierciedlona we wszystkich aspektach projektowania bezpiecznego systemu. Interfejsy wykorzystywane do uruchamiania funkcjonalności komponentu są dostępne tylko dla określonych podzbiorów populacji użytkowników, a konstrukcja komponentu wspiera wystarczająco drobną granulację rozkładu uprawnień. Na przykład, w przypadku mechanizmu audytu, może istnieć interfejs dla menedżera audytu, który konfiguruje ustawienia audytu; interfejs dla operatora audytu, który zapewnia, że dane audytu są bezpiecznie gromadzone i przechowywane; i wreszcie jeszcze jeden interfejs dla recenzenta audytu, który ma jedynie potrzebę przeglądania danych audytu, które zostały zgromadzone, ale nie ma potrzeby wykonywania operacji na tych danych.

Oprócz widocznych przejawów na interfejsie systemu, zasada najmniejszego uprawnienia może być wykorzystywana jako zasada przewodnia dla wewnętrznej struktury samego systemu. Jednym z aspektów wewnętrznego najmniejszego przywileju jest konstruowanie modułów w taki sposób, aby tylko elementy hermetyzowane przez moduł były bezpośrednio obsługiwane przez funkcje wewnątrz modułu. Elementy zewnętrzne w stosunku do modułu, na które może mieć wpływ działanie modułu, są pośrednio dostępne poprzez interakcję (np. poprzez wywołanie funkcji) z modułem, który zawiera te elementy. Innym aspektem wewnętrznego najmniejszego uprawnienia jest to, że zakres danego

modułu lub komponentu obejmuje tylko te elementy systemu, które są niezbędne dla jego funkcjonalności, a tryby dostępu do elementów (np. odczyt, zapis) są zminimalizowane.

Zabezpieczenia powiązane: AC-5, AC-6, SA-8.

(8) ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | ARANŻACJA (ORKIESTRACJA)

Projektowanie [***Realizacja: zdefiniowane przez organizację systemy krytyczne lub komponenty systemu***] **oparte na skoordynowanym zachowaniu w celu wdrożenia następujących możliwości:** [***Realizacja: zdefiniowane przez organizację możliwości, według systemu lub komponentu***]**.**

Omówienie: Zasoby bezpieczeństwa, które są umieszczone w różnych warstwach lub w różnych elementach systemu, lub są zaimplementowane w celu wspierania różnych aspektów wiarygodności, mogą oddziaływać na siebie w nieprzewidziany lub nieprawidłowy sposób. Niekorzystne konsekwencje mogą obejmować awarie kaskadowe, interferencje lub luki w działaniu. Koordynacja zachowania zasobów bezpieczeństwa (np. poprzez zapewnienie, że jedna poprawka jest zainstalowana we wszystkich zasobach przed dokonaniem zmiany konfiguracji, która zakłada, że poprawka jest rozpowszechniana) może zapobiec takim negatywnym interakcjom.

Zabezpieczenia powiązane: Brak.

(9) ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | ROZPROSZENIE PROJEKTOWANIA

Stosowanie różnych projektów do realizacji [***Realizacja: zdefiniowane przez organizację systemy krytyczne lub komponenty systemu***] **w celu spełnienia wspólnego zestawu wymagań lub zapewnienia równoważnej funkcjonalności.**

Omówienie: Rozproszone projektowanie jest osiągane poprzez dostarczenie tej samej specyfikacji wymagań wielu deweloperom, z których każdy jest

odpowiedzialny za stworzenie wariantu systemu lub komponentu systemu spełniającego te wymagania. Można tworzyć warianty w projekcie oprogramowania, w projekcie sprzętu, lub zarówno w projekcie sprzętu jak i oprogramowania. Różnice w wariantach projektowych mogą wynikać z doświadczenia dewelopera (np. wcześniejsze użycie wzorca projektowego), stylu projektowego (np. podczas rozkładania wymaganej funkcjonalności na mniejsze zadania, określenie co stanowi oddzielne zadanie i jak dalece rozkładać zadania na podzadania), wyboru bibliotek do włączenia do wariantu oraz środowiska programistycznego (np. różne narzędzia projektowe sprawiają, że niektóre wzorce projektowe są łatwiejsze do wizualizacji). Rozproszone projektowanie sprzętu obejmuje podejmowanie różnych decyzji dotyczących tego, jakie informacje zachować w postaci analogowej, a jakie przekształcić na postać cyfrową, przekazywanie tych samych informacji w różnym czasie oraz wprowadzanie opóźnień w próbkowaniu (różnorodność czasowa). Rozproszone projektowanie jest powszechnie wykorzystywana do wspierania odporności na błędy.

Zabezpieczenia powiązane: Brak.

Referencje: [ISO 15408-2], [ISO 15408-3], [SP. 800-160-1].

SA-18 ODPORNOŚĆ NA SABOTAŻ I WYKRYWANIE MANIPULACJI

[Wycofane: Włączone do SR-9].

Zabezpieczenia rozszerzone:

(1) OPORNOŚĆ NA SABOTAŻ I WYKRYWANIE MANIPULACJI | WIELOFAZOWOŚĆ CYKLU ŻYCIA SYSTEMU

[Wycofane: Włączone do SR-9(1)].

(2) OPORNOŚĆ NA SABOTAŻ I WYKRYWANIE MANIPULACJI | KONTROLA SYSTEMÓW INFORMATYCZNYCH, KOMPONENTÓW LUB URZĄDZEŃ

[Wycofane: Włączone do SR-10].

SA-19 AUTENTYCZNOŚĆ KOMPONENTÓW

[Wycofane: Włączone do SR-11].

Zabezpieczenia rozszerzone:

(1) AUTENTYCZNOŚĆ KOMPONENTÓW SZKOLENIE / ROZPOZNAWANIE AUTENTYCZNOŚCI

[Wycofane: Włączone do SR-11(1)].

(2) AUTENTYCZNOŚĆ KOMPONENTÓW | KONTROLA KONFIGURACJI NA POTRZEBY SERWISOWANIA / NAPRAWY KOMPONENTÓW

[Wycofane: Włączone do SR-11(2)].

(3) AUTENTYCZNOŚĆ KOMPONENTÓW | UTYLIZACJA KOMPONENTÓW

[Wycofane: Włączone do SR-12].

(4) AUTENTYCZNOŚĆ KOMPONENTÓW | SKANOWANIE AUTENTYCZNOŚCI

[Wycofane: Włączone do SR-11(3)].

SA-20 NIESTANDARDOWA (NA ZAMÓWIENIE) ROZBUDOWA KOMPONENTÓW KRYTYCZNYCH

Zabezpieczenie podstawowe: Ponowne wdrożenie lub opracowanie na zamówienie następujących krytycznych komponentów systemu: [*Realizacja: zdefiniowane przez organizację krytyczne komponenty systemu*].

Omówienie: Organizacje określają, że pewnym komponentom systemu prawdopodobnie nie można ufać ze względu na konkretne zagrożenia i podatności tych komponentów, które nie zostały poddane skutecznym zabezpieczeniom w celu odpowiedniego zmniejszenia ryzyka. Reimplementacja lub opracowanie takich komponentów na specjalne zamówienie może spełnić wymagania dotyczące wyższego stopnia pewności i jest przeprowadzane poprzez inicjowanie zmian w komponentach systemu (w tym w sprzęcie, aplikacjach i oprogramowaniu układowym), dzięki którym prawdopodobieństwo powodzenia standardowych ataków przeciwników jest mniejsze. W sytuacjach, w których alternatywne źródła zaopatrzenia nie są dostępne, a organizacje nie decydują się na ponowne wdrożenie lub opracowanie na zamówienie krytycznych komponentów systemu, można zastosować dodatkowe zabezpieczenia. Obejmują one rozszerzony audyt, ograniczenia dostępu do kodu źródłowego i narzędzi systemowych oraz ochronę przed usuwaniem plików systemowych i aplikacji.

Zabezpieczenia powiązane: CP-2, RA-9, SA-8.

Zabezpieczenia rozszerzone: Brak.

Referencje: [NIST SP 800-160-1].

SA-21 DOBÓR DEWELOPERÓW

Zabezpieczenie podstawowe: Wymaganie od dewelopera [*Realizacja: system zdefiniowany przez organizację, komponent systemu lub usługa systemowa*]*:*

a. Posiadania odpowiedniego uprawnienia dostępu zgodnie z przypisanymi [Realizacja: zdefiniowane przez organizację oficjalne obowiązki wynikające z pełnionej funkcji]; oraz

b. Spełniania następujących dodatkowych kryteriów weryfikacji personelu: [*Realizacja: zdefiniowane przez organizację dodatkowe kryteria weryfikacji*].

Omówienie: Postępowanie sprawdzające wobec deweloperów jest skierowane do deweloperów zewnętrznych. Wewnętrzne postępowanie sprawdzające programistów jest omówione w zabezpieczeniu PS-3. Ponieważ system, komponent systemu lub usługa systemowa mogą być wykorzystywane w działaniach krytycznych, istotnych z punktu widzenia interesów bezpieczeństwa narodowego lub ekonomicznego Państwa, w interesie organizacji leży zapewnienie, aby programiści byli godni zaufania. Stopień zaufania wymagany od deweloperów może być spójny ze stopniem zaufania osób, które uzyskują dostęp do systemów, komponentów systemu lub usług systemowych po ich wdrożeniu. Kryteria upoważniania i sprawdzania personelu obejmują poświadczenia bezpieczeństwa, sprawdzanie przeszłości, obywatelstwo i narodowość. Wiarygodność dewelopera może również obejmować przegląd i analizę struktury własności firmy oraz relacji, jakie firma ma z podmiotami, które mogą potencjalnie wpłynąć na jakość i niezawodność opracowywanych systemów, komponentów lub usług. Spełnienie wymaganych kryteriów autoryzacji dostępu i sprawdzania personelu obejmuje dostarczenie listy wszystkich osób, które są upoważnione do wykonywania czynności rozwojowych w wybranym systemie, komponencie systemu lub usłudze systemowej, tak aby organizacje mogły sprawdzić, czy deweloper spełnił kryteria autoryzacji i weryfikacji.

Zabezpieczenia powiązane: PS-2, PS-3, PS-6, PS-7, SA-4, SR-6.

Zabezpieczenia rozszerzone:

(1) DOBÓR DEWELOPERÓW | OCENA PRZEGLĄDU

[Wycofane: Włączone do SA-21].

Referencje: Brak.

SA-22 KOMPONENTY SYSTEMU BEZ WSPARCIA

Zabezpieczenie podstawowe:

a. Zastępowanie komponentów systemu, gdy wsparcie dla tych komponentów nie jest już zapewniane przez dewelopera, dostawcę lub producenta; lub

b. Dostarczanie uzasadnienia i dokumentów potwierdzających dalsze używanie nieobsługiwanych komponentów systemu wymaganych do spełnienia wymagań biznesowych poprzez [*Wybór (jeden lub więcej): wsparcie wewnętrzne;* [*Realizacja: zdefiniowane przez organizację wsparcie zapewniane przez zewnętrznych dostawców*]].

Omówienie: Wsparcie dla komponentów systemu obejmuje poprawki aplikacji, aktualizacje oprogramowania sprzętowego, części zamienne i umowy serwisowe. Przykładem nieobsługiwania komponentów jest sytuacja, gdy dostawcy nie udostępniają już krytycznych poprawek oprogramowania lub aktualizacji produktu, co może prowadzić do wykorzystania przez przeciwników podatności zainstalowanych komponentów. Wyjątki od konieczności wymiany niewspieranych komponentów systemu obejmują systemy, które zapewniają krytyczne funkcje lub działania biznesowe, dla których nowsze technologie nie są dostępne lub które są tak odizolowane, że instalacja komponentów zamiennych nie jest możliwa.

Alternatywne źródła wsparcia odnoszą się do potrzeby zapewnienia ciągłości obsługi komponentów systemu, które nie są już wspierane przez pierwotnych producentów, deweloperów lub sprzedawców, jeżeli takie komponenty pozostają kluczowe dla misji i funkcji biznesowych organizacji. W razie potrzeby organizacje mogą ustanowić wewnętrzne wsparcie poprzez opracowywanie dostosowanych nakładek na krytyczne komponenty oprogramowania lub, alternatywnie, skorzystać z usług zewnętrznych dostawców, którzy zapewnią stałe wsparcie niewspieranych komponentów na podstawie umów. Takie stosunki umowne mogą obejmować sprzedawców oprogramowania open source z wartością dodaną. Zwiększone ryzyko korzystania z niewspieranych komponentów systemu można ograniczyć na przykład

poprzez zakaz podłączania takich komponentów do sieci publicznych lub niekontrolowanych albo poprzez wdrożenie innych form izolacji.

Zabezpieczenia powiązane: PL-2, SA-3.

Zabezpieczenia rozszerzone:

(1) KOMPONENTY SYSTEMU BEZ WSPARCIA | ALTERNATYWNE ŹRÓDŁA STAŁEGO WSPARCIA

[Wycofane: Włączone do SA-22].

Referencje: Brak.

SA-23 SPECJALIZACJA

Zabezpieczenie podstawowe: Zastosowanie [*Wybór (jeden lub więcej): projektowanie; modyfikacja; rozbudowa; rekonfiguracja*] wspierających podstawowe usługi lub funkcje [*Realizacja: zdefiniowane przez organizację systemy lub komponenty systemu*] w celu zwiększenia wiarygodności tych systemów lub komponentów.

Omówienie: Niejednokrotnie konieczne jest, aby system lub komponent systemu, który wspiera usługi lub funkcje istotne dla misji, został usprawniony w celu zmaksymalizowania wiarygodności zasobu. Czasami takie rozszerzenie jest dokonywane na poziomie projektu. W innych przypadkach jest ono dokonywane po zaprojektowaniu, poprzez modyfikację danego systemu lub poprzez rozszerzenie systemu o dodatkowe komponenty. Na przykład, dodatkowe funkcje uwierzytelniania lub niezaprzeczalności mogą być dodane do systemu celem rozszerzenia identyfikacji zasobów krytycznych dla innych zasobów, które zależą od zasobów zdefiniowanych przez organizację.

Zabezpieczenia powiązane: RA-9, SA-8.

Zabezpieczenia rozszerzone: Brak.

Referencje: [NIST SP 800-160-1], [NIST SP 800-160-2]

KATEGORIA SC – OCHRONA SYSTEMÓW I SIECI TELEKOMUNIKACYJNYCH

SC-1 POLITYKA I PROCEDURY

Zabezpieczenie podstawowe:

a. Opracowywanie, dokumentowanie i rozpowszechnianie wśród [Realizacja: *personel lub role określone przez organizację*]:

   1. [*Wybór (jeden lub więcej): poziom organizacji; poziom misji/procesu biznesowego; poziom systemu*] polityki ochrony systemów i sieci telekomunikacyjnych, która:

      (a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność zprzepisami; oraz

      (b) Jest zgodna z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi; oraz

   2. Procedur ułatwiających wdrożenie polityki polityki ochrony systemów i sieci telekomunikacyjnych oraz powiązanych zabezpieczeń w zakresie polityki ochrony systemów i sieci telekomunikacyjnych;

b. Wyznaczanie [Realizacja: *osoba wyznaczona przez organizację*] do zarządzania rozwojem, dokumentacją i rozpowszechnianiem polityki i procedur polityki ochrony systemów i sieci telekomunikacyjnych; oraz

c. Przeglądanie i aktualizacja bieżącej:

   1. Polityki polityki ochrony systemów i sieci telekomunikacyjnych z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*]; oraz

   2. Procedur polityki ochrony systemów i sieci telekomunikacyjnych z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*].

Omówienie: Polityka i procedury w zakresie ochrony systemów i sieci telekomunikacyjnych dotyczą zabezpieczeń w kategorii *Ochrona systemów i sieci telekomunikacyjnych* (SC), które są wdrażane w ramach systemów i organizacji. Strategia zarządzania ryzykiem jest ważnym czynnikiem przy tworzeniu takich polityk i procedur. Polityki i procedury przyczyniają się do zapewnienia bezpieczeństwa i ochrony prywatności. Dlatego ważne jest, aby programy bezpieczeństwa i ochrony prywatności były opracowywane wspólnie przy kształtowaniu polityki i procedur ochrony systemów i sieci telekomunikacyjnych. Polityki i procedury dotyczące programów bezpieczeństwa i ochrony prywatności na poziomie organizacji są ogólnie rzecz biorąc preferowane i mogą eliminować potrzeby tworzenia polityk i procedur specyficznych dla danej misji lub systemu. Polityka może być włączona jako część ogólnej polityki bezpieczeństwa i ochrony prywatności lub reprezentowana przez wiele polityk odzwierciedlających złożony charakter organizacji. Procedury mogą być ustanowione dla programów bezpieczeństwa i ochrony prywatności, dla misji lub procesów biznesowych oraz dla systemów, jeśli to konieczne. Procedury opisują sposób wdrażania zasad lub zabezpieczeń i mogą być skierowane do osoby lub roli, która jest przedmiotem procedury. Procedury mogą być udokumentowane w planach bezpieczeństwa i ochrony prywatności systemu w jednym lub kilku oddzielnych dokumentach.

Zdarzenia, które mogą spowodować konieczność aktualizacji polityki i procedur ochrony systemów i sieci telekomunikacyjnych, obejmują wyniki oceny lub audytu, incydenty lub naruszenia bezpieczeństwa, lub zmiany w przepisach prawa, zarządzeniach, dyrektywach, rozporządzeniach, zasadach, standardach i wytycznych.

Oświadczenie o wprowadzeniu zabezpieczeń nie jest równoznaczne z ustanowieniem polityki lub procedury organizacyjnej.

Zabezpieczenia powiązane: PM-9, PS-8, SA-8, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [NIST SP 800-12], [NIST SP 800-100].

SC-2 ROZDZIELENIE FUNKCJONALNOŚCI SYSTEMU I UŻYTKOWNIKA

Zabezpieczenie podstawowe: Oddzielenie funkcji użytkownika, w tym usług interfejsu użytkownika, od funkcji zarządzania systemem.

Omówienie: Funkcja zarządzania systemem obejmuje funkcje niezbędne do administrowania bazami danych, komponentami sieci, stacjami roboczymi lub serwerami. Funkcje te zazwyczaj wymagają uprzywilejowanego dostępu użytkownika. Oddzielenie funkcji użytkownika od funkcji zarządzania systemem dokonywane jest fizyczne lub logiczne. Organizacje mogą oddzielić funkcje zarządzania systemem od funkcji użytkownika poprzez wykorzystanie różnych komputerów, instancji systemów operacyjnych, jednostek centralnych lub adresów sieciowych; poprzez zastosowanie technik wirtualizacji; lub poprzez kombinacje tych lub innych metod. Oddzielenie funkcji zarządzania systemem od funkcji użytkownika obejmuje sieciowe (webowe) interfejsy administracyjne, które wykorzystują oddzielne metody uwierzytelniania wobec użytkowników wszelkich innych zasobów systemowych. Oddzielenie funkcji systemu od funkcji użytkownika może obejmować oddzielenie interfejsów administracyjnych w różnych domenach i przy zastosowaniu dodatkowych kontroli dostępu. Oddzielenie funkcji systemu od funkcji użytkownika można osiągnąć poprzez zastosowanie zasad projektowania inżynierii bezpieczeństwa systemów zawartych w zabezpieczeniu podstawowym SA-8, w tym w zabezpieczeniach rozszerzonych SA-8(1), SA-8(3), SA-8(4), SA-8(10), SA-8(12), SA-8(13), SA-8(14) i SA-8(18).

Zabezpieczenia powiązane: AC-6, SA-4, SA-8, SC-3, SC-7, SC-22, SC-32, SC-39.

Zabezpieczenia rozszerzone:

(1) ROZDZIELENIE FUNKCJONALNOŚCI SYSTEMU I UŻYTKOWNIKA | INTERFEJSY DLA UŻYTKOWNIKÓW NIEUPRZYWILEJOWANYCH

Zapobieganie prezentacji funkcji zarządzania systemem na interfejsach dedykowanych użytkownikom nieuprzywilejowanym.

Omówienie: Zapobieganie prezentacji funkcjonalności zarządzania systemem na interfejsach dla użytkowników nieuprzywilejowanych zapewnia, że opcje zarządzania systemem, w tym uprawnienia administratora, nie są dostępne dla ogółu populacji użytkowników. Ograniczenie dostępu użytkownika zabrania również korzystania z opcji „wyszarzenia" (zaciemniania), powszechnie stosowanej w celu wyeliminowania dostępu do takich informacji. Jednym z potencjalnych rozwiązań jest zablokowanie możliwości administrowania systemem do czasu ustanowienia przez użytkowników sesji z uprawnieniami administratora

Zabezpieczenia powiązane: AC-3.

(2) ROZDZIELENIE FUNKCJONALNOŚCI SYSTEMU I UŻYTKOWNIKA | NIEPOŁĄCZALNOŚĆ (DEZASOCJACJA)

Oddzielnie przechowywanych informacji o statusie aplikacji i oprogramowania.

Omówienie: W przypadku kompromitacji systemu, przechowywanie aplikacji i oprogramowania oddzielnie od informacji dotyczących stanu interakcji użytkowników z aplikacją może skuteczniej chronić prywatność osób.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

SC-3 IZOLACJA FUNKCJI BEZPIECZEŃSTWA

Zabezpieczenie podstawowe: Oddzielenie funkcji bezpieczeństwa od funkcji nie związanych z bezpieczeństwem.

Omówienie: Funkcje bezpieczeństwa są odizolowane od funkcji niezwiązanych z bezpieczeństwem za pomocą granicy izolacji wdrożonej w systemie za pośrednictwem partycji i domen. Granica izolacji kontroluje dostęp i chroni integralność sprzętu, oprogramowania i oprogramowania układowego, które realizują funkcje bezpieczeństwa systemu. Systemy realizują separację kodu na wiele sposobów, np. poprzez dostarczanie jąder bezpieczeństwa za pośrednictwem pierścieni procesora lub trybów procesora. W przypadku kodu niebędącego jądrem, izolacja funkcji bezpieczeństwa jest często osiągana poprzez zabezpieczenia systemu plików, które chronią kod na dysku, oraz zabezpieczenia przestrzeni adresowej, które chronią wykonywany kod. Systemy mogą ograniczać dostęp do funkcji bezpieczeństwa za pomocą mechanizmów kontroli dostępu oraz poprzez implementację funkcji najmniejszych uprawnień. Chociaż ideałem jest, aby cały kod w obrębie zdefiniowanej granicy izolacji funkcji bezpieczeństwa zawierał tylko kod istotny dla bezpieczeństwa, to jednak czasami konieczne jest uwzględnienie funkcji niezwiązanych z bezpieczeństwem jako wyjątku. Izolacja funkcji bezpieczeństwa od funkcji nie związanych z bezpieczeństwem może być osiągnięta poprzez zastosowanie zasad projektowania inżynierii bezpieczeństwa systemów zawartych w zabezpieczeniu podstawowym SA-8, w tym w zabezpieczeniach rozszerzonych SA-8(1), SA-8(3), SA-8(4), SA-8(10), SA-8(12), SA-8(13), SA-8(14) oraz SA-8(18).

Zabezpieczenia powiązane: AC-3, AC-6, AC-25, CM-2, CM-4, SA-4, SA-5, SA-8, SA-15, SA-17, SC-2, SC-7, SC- 32, SC-39, SI-16.

Zabezpieczenia rozszerzone:

(1) IZOLACJA FUNKCJI BEZPIECZEŃSTWA | SEPARACJA SPRZĘTOWA

Zastosowanie mechanizmów separacji sprzętowej w celu wdrożenia izolacji funkcji bezpieczeństwa.

Omówienie: Mechanizmy separacji sprzętowej obejmują architektury pierścieni sprzętowych, które są zaimplementowane w ramach mikroprocesorów oraz wymuszoną sprzętowo segmentację adresów używaną do obsługi logicznie odrębnych obiektów pamięci masowej z odrębnymi atrybutami (tj. możliwymi do odczytu, zapisywalnymi).

Powiązane elementy kontrolne: Brak.

(2) IZOLACJA FUNKCJI BEZPIECZEŃSTWA | FUNKCJE KONTROLI DOSTĘPU I PRZEPŁYWU

Oddzielenie funkcji bezpieczeństwa wymuszających kontrolę dostępu i przepływu informacji od funkcji nie związanych z bezpieczeństwem oraz od innych funkcji bezpieczeństwa.

Omówienie: Izolacja funkcji bezpieczeństwa występuje podczas implementacji. Funkcje te nadal mogą być skanowane i monitorowane. Funkcje bezpieczeństwa, które są potencjalnie odizolowane od funkcji egzekwowania kontroli dostępu i przepływu, obejmują funkcje audytu, wykrywania włamań i ochrony przed złośliwym kodem.

Zabezpieczenia powiązane: Brak.

(3) IZOLACJA FUNKCJI BEZPIECZEŃSTWA | MINIMALIZACJA FUNKCJI NIE ZWIĄZANYCH Z BEZPIECZEŃSTWEM

Minimalizowanie liczby funkcji niezwiązanych z bezpieczeństwem zawartych w granicach izolacji zawierających funkcje bezpieczeństwa.

Omówienie: Tam, gdzie nie jest możliwe osiągnięcie ścisłej izolacji funkcji nie związanych z bezpieczeństwem od funkcji bezpieczeństwa, konieczne jest podjęcie działań w celu zminimalizowania funkcji niemających znaczenia dla bezpieczeństwa w granicach funkcji bezpieczeństwa. Funkcje nie związane z bezpieczeństwem zawarte w granicach izolacji uważa się za mające znaczenie dla bezpieczeństwa, ponieważ błędy lub złośliwe kody w oprogramowaniu mogą mieć bezpośredni wpływ na funkcje bezpieczeństwa systemów. Podstawowym celem projektu jest to, aby poszczególne części systemów, które zapewniają bezpieczeństwo informacji, miały minimalny rozmiar i złożoność. Zminimalizowanie liczby funkcji niezwiązanych z bezpieczeństwem w komponentach systemu istotnych z punktu widzenia bezpieczeństwa, pozwala projektantom i wykonawcom skoncentrować się wyłącznie na tych funkcjach, które są niezbędne do zapewnienia pożądanych możliwości w zakresie bezpieczeństwa (zazwyczaj egzekwowania dostępu). Minimalizując funkcje niezwiązane z bezpieczeństwem w granicach izolacji, znacznie zmniejsza się objętość kodu, który jest zaufany do egzekwowania polityk bezpieczeństwa, przyczyniając się w ten sposób do zwiększenia jego zrozumiałości.

Zabezpieczenia powiązane: Brak.

(4) IZOLACJA FUNKCJI BEZPIECZEŃSTWA | MODUŁ SPRZĘŻENIA I SPÓJNOŚCI

Wdrożanie funkcji bezpieczeństwa jako wysoce niezależnych modułów, które maksymalizują wewnętrzną spójność w obrębie modułów i minimalizują sprzężenie między modułami.

Omówienie: Redukcja interakcji międzymodułowych pomaga w ograniczaniu funkcji bezpieczeństwa i zarządzaniu złożonością. Pojęcia sprzężenia i spójności są istotne w odniesieniu do modularności w projektowaniu oprogramowania. Sprzężenie odnosi się do zależności, jakie dany moduł wykazuje w stosunku do innych modułów. Spójność odnosi się do relacji pomiędzy funkcjami w obrębie modułu. Najlepsze praktyki w inżynierii oprogramowania i inżynierii

bezpieczeństwa systemów opierają się na warstwowości, minimalizacji i modułowej dekompozycji w celu zmniejszenia i zarządzania złożonością. W ten sposób powstają moduły oprogramowania, które są wysoce spójne i jednocześnie luźno sprzężone.

Zabezpieczenia powiązane: Brak.

(5) IZOLACJA FUNKCJI BEZPIECZEŃSTWA | STRUKTURY WARSTWOWE

Zaimplementowanie funkcji bezpieczeństwa jako struktury warstwowej, minimalizując interakcje między warstwami projektu i unikając uzależnienia niższych warstw od funkcjonalności lub poprawności wyższych warstw.

Omówienie: Implementacja struktur warstwowych o zminimalizowanych interakcjach pomiędzy funkcjami bezpieczeństwa i nie zapętlających się warstwach (tzn. funkcje niższej warstwy nie zależą od funkcji wyższej warstwy) umożliwia izolację funkcji bezpieczeństwa i zarządzanie złożonością.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

SC-4 INFORMACJE NA WSPÓŁDZIELONYCH ZASOBACH SYSTEMOWYCH

Zabezpieczenie podstawowe: Zapobieganie nieautoryzowanemu i niezamierzonemu przekazywaniu informacji za pośrednictwem współdzielonych zasobów systemowych.

Omówienie: Zapobieganie nieautoryzowanemu i niezamierzonemu przekazywaniu informacji za pośrednictwem współdzielonych zasobów systemowych powoduje, że informacje wytworzone przez działania poprzednich użytkowników lub ról (lub działania procesów działających w imieniu poprzednich użytkowników lub ról) nie są dostępne dla obecnych użytkowników lub ról (lub bieżących procesów działających w imieniu obecnych użytkowników lub ról), którzy uzyskują dostęp do współdzielonych zasobów systemowych po ich ponownym udostępnieniu do systemu. Informacje we współdzielonych zasobach systemu dotyczą również zaszyfrowanych reprezentacji informacji. W innych kontekstach zabezpieczenie informacji we wspólnych zasobach systemowych określana jest jako ponowne wykorzystanie obiektu i ochrona informacji szczątkowych. Informacje we wspólnych zasobach systemowych nie dotyczą remanencji informacji, która odnosi się do reprezentacji szczątkowej danych, które zostały nominalnie usunięte; ukrytych kanałów (w tym kanałów przechowywania i synchronizacji), w których współdzielone zasoby systemowe są manipulowane w celu naruszenia ograniczeń w przepływie informacji; lub komponentów w ramach systemów, dla których istnieją tylko pojedynczy użytkownicy lub role.

Zabezpieczenia powiązane: AC-3, AC-4, SA-8.

Zabezpieczenia rozszerzone:

(1) INFORMACJE NA WSPÓŁDZIELONYCH ZASOBACH SYSTEMOWYCH | POZIOMY BEZPIECZEŃSTWA

[Wycofane: Włączone do SC-4].

(2) INFORMACJE NA WSPÓŁDZIELONYCH ZASOBACH SYSTEMOWYCH | PRZETWARZANIE WIELOPOZIOMOWE LUB OKRESOWE

Zapobieganie nieautoryzowanemu przekazywaniu informacji za pośrednictwem współdzielonych zasobów zgodnie z [***Realizacja: procedury określone przez organizację***]**, gdy system procesujący przełącza się między różnymi poziomami klasyfikacji informacji lub kategoriami bezpieczeństwa.**

Omówienie: Zmiany w poziomach przetwarzania mogą wystąpić podczas wielopoziomowego lub okresowego przetwarzania informacji o różnych poziomach klasyfikacji lub kategoriach bezpieczeństwa. Mogą one również wystąpić podczas szeregowego ponownego wykorzystywania komponentów sprzętowych na różnych poziomach klasyfikacji. Procedury określone przez organizację mogą obejmować zatwierdzone procesy sanityzacji informacji przechowywanych elektronicznie.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

SC-5 OCHRONA PRZED BLOKADĄ USŁUG (DoS)

Zabezpieczenie podstawowe:

a. [*Wybór: Chronienie przed; Ograniczanie*] skutki następujących rodzajów ataków typu „blokada usługi": [*Realizacja: określone przez organizację rodzaje zdarzeń związanych z odmową obsługi*]; oraz

b. Stosowanie następujących zabezpieczeń dla osiągnięcia celu ochrony przed blokadą usługi: [*Realizacja: środki bezpieczeństwa określone przez organizację według typu zdarzenia DoS*].

Omówienie: Zdarzenia związane z ochroną przed blokadą usługi (*ang. denial-of-service – DoS*) mogą wystąpić z różnych przyczyn wewnętrznych i zewnętrznych, takich jak atak przeciwnika lub brak planowania w celu wsparcia potrzeb organizacyjnych w zakresie przepustowości i szerokości pasma. Takie ataki mogą wystąpić poprzez szeroki zakres protokołów sieciowych (np. IPv4, IPv6). Dostępne są różne technologie ograniczające lub eliminujące powstawanie i skutki ataków typu DoS. Na przykład, urządzenia ochrony brzegowej mogą filtrować określone typy pakietów w celu ochrony komponentów systemu w sieciach wewnętrznych przed bezpośrednim wpływem lub źródłem ataków typu DoS. Zastosowanie zwiększonej pojemności i przepustowości sieci w połączeniu z redundancją usług również zmniejsza podatność na zdarzenia typu DoS.

Zabezpieczenia powiązane: CP-2, IR-4, SC-6, SC-7, SC-40.

Zabezpieczenia rozszerzone:

(1) OCHRONA PRZED BLOKADĄ USŁUG (DoS) | OGRANICZENIE MOŻLIWOŚCI ATAKOWANIA INNYCH SYSTEMÓW

Ograniczanie jednostkom możliwości przeprowadzania następujących ataków typu DoS na systemy: [***Realizacja: ataki typu DoS zdefiniowane przez organizację***]**.**

Omówienie: Ograniczanie zdolności jednostek do przeprowadzania ataków typu DoS wymaga niedostępności powszechnie wykorzystywanych do takich ataków instrumentów. Do jednostek, które stanowią zagrożenie, zalicza się wrogie osoby wewnątrz organizacji lub zewnętrznych przeciwników, którzy naruszyli lub skompromitowali system i wykorzystują go do przeprowadzenia ataku typu DoS. Organizacje mogą ograniczyć zdolność jednostek do łączenia się i przekazywania dowolnych informacji na medium transportowym (tj. sieci przewodowe, sieci bezprzewodowe, spreparowane pakiety protokołu internetowego). Organizacje mogą również ograniczać możliwość korzystania przez jednostki z nadmiarowych zasobów systemowych. Ochrona przed jednostkami zdolnymi do przeprowadzania ataków typu DoS może być wdrożona w określonych systemach lub urządzeniach brzegowych, które uniemożliwiają dostęp do systemów będących potencjalnym celem ataku.

Zabezpieczenia powiązane: Brak.

(2) OCHRONA PRZED BLOKADĄ USŁUG (DoS) | PRZEPUSTOWOŚĆ, SZEROKOŚĆ PASMA I NADMIAROWOŚĆ

Zarządzanie przepustowością, szerokością pasma lub nadmiarowością w celu ograniczenia skutków ataków typu „blokada usługi" DoS.

Omówienie: Zarządzanie przepustowością zapewnia, że dostępna jest wystarczająca przepustowość do przeciwdziałania atakom typu "przepełnienie" (*ang. flooding attacks*). Zarządzanie szerokością pasma obejmuje ustanowienie wybranych priorytetów użytkowania, limitów, partycjonowania lub równoważenia obciążenia..

Zabezpieczenia powiązane: Brak.

(3) OCHRONA PRZED BLOKADĄ USŁUG (DoS) | WYKRYWANIE I MONITOROWANIE

(a) Zastosowanie następujących narzędzi monitorujących w celu wykrycia wskaźników ataków typu DoS skierowanych na systemi lub

uruchamianych z systemu: [***Realizacja: narzędzia monitoringu zdefiniowane przez organizację***]**; oraz**

(b) Monitorowanie następujących zasobów systemowych w celu ustalenia, czy istnieją wystarczające zasoby do zapobiegania skutecznym atakom typu DoS: [***Realizacja: zasoby systemowe zdefiniowane przez organizację***]**.**

Omówienie: Organizacje biorą pod uwagę wykorzystanie i pojemność zasobów systemowych przy zarządzaniu ryzykiem związanym z blokadą usług w związku ze złośliwymi atakami. Ataki typu DoS mogą pochodzić z zewnętrznych lub wewnętrznych źródeł. Zasoby systemowe, które są wrażliwe na blokadę usługi, obejmują fizyczną pamięć dyskową, pamięć i cykle procesora. Techniki wykorzystywane do zapobiegania atakom typu DoS związanym z wykorzystaniem pamięci masowej i jej przepustowości obejmują ustanawianie limitów pojemności dysków, konfigurowanie systemów w celu automatycznego ostrzegania administratorów o osiągnięciu określonych progów pojemności, wykorzystywanie technologii kompresji plików w celu maksymalizacji dostępnej przestrzeni dyskowej oraz narzucanie oddzielnych partycji dla danych systemowych i danych użytkowników.

Zabezpieczenia powiązane: CA-7, SI-4.

Referencje: [NIST SP 800-189].

SC-6 DOSTĘPNOŚĆ ZASOBÓW

Zabezpieczenie podstawowe: Ochrona dostępności zasobów poprzez przydzielenie [Realizacja: *zasoby zdefiniowane przez organizację*] i stosowanie [*Wybór (jeden lub więcej): priorytet; przydział;* [*Realizacja: zabezpieczenia zdefiniowane przez organizację*]].

Omówienie: Ochrona priorytetów zapobiega opóźnieniom lub zakłóceniom procesów o niższym priorytecie w systemie obsługujących procesy o wyższym priorytecie. Przydziały zasobów uniemożliwiają użytkownikom lub procesom uzyskanie większych niż z góry ustalone ilości zasobów.

Zabezpieczenia powiązane: SC-5.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB M-08-05], [DHS TIC].

SC-7 OCHRONA POŁĄCZEŃ BRZEGOWYCH

Zabezpieczenie podstawowe:

a. Monitorowanie i kontrolowanie komunikacji na zewnętrznych zarządzanych interfejsach systemu oraz na kluczowych wewnętrznych zarządzanych interfejsach tego systemu;

b. Wdrożenie podsieci dla publicznie dostępnych komponentów systemu, które są [Realizacja: fizycznie; logicznie] oddzielone od wewnętrznych sieci organizacyjnych; oraz

c. Podłączenie do zewnętrznych sieci lub systemów wyłącznie poprzez zarządzane interfejsy składające się z urządzeń ochrony brzegowej rozmieszczonych zgodnie z organizacyjną architekturą bezpieczeństwa i ochrony prywatności..

Omówienie: Zarządzane interfejsy obejmują bramy, routery, zapory ogniowe, osłony, sieciową analizę złośliwego kodu, systemy wirtualizacji lub szyfrowane tunele wdrożone w ramach architektury bezpieczeństwa. Podsieci, które są fizycznie lub logicznie oddzielone od sieci wewnętrznych, nazywane są strefami zdemilitaryzowanymi lub DMZ. Ograniczanie lub zakazywanie używania interfejsów w systemach organizacyjnych obejmuje ograniczanie zewnętrznego ruchu sieciowego do wyznaczonych serwerów sieciowych w obrębie zarządzanych interfejsów, zakazanie ruchu zewnętrznego, który wygląda na spoofing adresów wewnętrznych, oraz zakazanie ruchu wewnętrznego, który wygląda na spoofing adresów zewnętrznych. Publikacja [SP 800-189] dostarcza dodatkowych informacji na temat technik walidacji adresów źródłowych, pozwalających zapobiegać wprowadzaniu i wyprowadzaniu ruchu z fałszywymi adresami. Komercyjne usługi telekomunikacyjne są świadczone przez komponenty sieciowe i skonsolidowane systemy zarządzania współdzielone przez klientów. Usługi te mogą również obejmować linie dostępowe dostarczane przez strony trzecie oraz inne elementy usługowe. Takie usługi mogą stanowić źródła zwiększonego ryzyka pomimo postanowień dotyczących

bezpieczeństwa zawartych w umowie. Ochrona obszarów może zostać wdrożona jako wspólne zabezpieczenie dla całej sieci organizacyjnej lub jej części w taki sposób, że chroniona granica jest większa niż granica specyficzna dla danego systemu (np. granica autoryzacji).

Zabezpieczenia powiązane: AC-4, AC-17, AC-18, AC-19, AC-20, AU-13, CA-3, CM-2, CM-4, CM-7, CM-10, CP- 8, CP-10, IR-4, MA-4, PE-3, PL-8, PM-12, SA-8, SA-17, SC-5, SC-26, SC-32, SC-35, SC-43.

Zabezpieczenia rozszerzone:

(1) OCHRONA POŁĄCZEŃ BRZEGOWYCH | FIZYCZNIE ODDZIELONE PODSIECI

[Wycofane: Włączone do SC-7].

(2) OCHRONA POŁĄCZEŃ BRZEGOWYCH | DOSTĘP PUBLICZNY

[Wycofane: Włączone do SC-7].

(3) OCHRONA POŁĄCZEŃ BRZEGOWYCH | PUNKTY DOSTĘPOWE

Ograniczanie liczby zewnętrznych połączeń sieciowych do systemu.

Omówienie: Ograniczenie liczby zewnętrznych połączeń sieciowych ułatwia monitorowanie ruchu w komunikacji przychodzącej i wychodzącej. Inicjatywa Trusted Internet Connection [DHS TIC] jest przykładem wytycznych, które wymagają ograniczenia liczby zewnętrznych połączeń sieciowych. Ograniczenie liczby zewnętrznych połączeń sieciowych do systemu jest szczególnie ważne w okresach przejściowych od starszych do nowszych technologii (np. przejście od protokołów sieciowych IPv4 do IPv6). Taka transformacja może wymagać jednoczesnego wdrożenia starszych i nowszych technologii w okresie przejściowym, a tym samym zwiększenia liczby punktów dostępowych do systemu.

Zabezpieczenia powiązane: Brak.

(4) OCHRONA POŁĄCZEŃ BRZEGOWYCH | ZEWNĘTRZNE USŁUGI TELEKOMUNIKACYJNE

(a) Wdrożenie zarządzanego interfejsu dla każdej zewnętrznej usługi telekomunikacyjnej;

(b) Ustalenie polityki przepływu ruchu dla każdego zarządzanego interfejsu;

(c) Chronienie poufności i integralności informacji przekazywanych za pośrednictwem każdego interfejsu;

(d) Dokumentowanie każdego wyjątku od polityki przepływu ruchu wraz z misją lub potrzebą biznesową i czasem trwania tego wyjątku;

(e) Przeglądanie wyjątków w polityce przepływu ruchu [***Realizacja: częstotliwość określona przez organizację***] **i usuwanie wyjątków, które nie są już wymagane przez określoną misję lub potrzebę biznesową;**

(f) Zapobieganie nieuprawnionej wymianie ruchu w obrębie płaszczyzny sterowania z sieciami zewnętrznymi;

(g) Publikowanie informacji umożliwiających zdalnym sieciom wykrywanie nieautoryzowanego ruchu w płaszczyźnie sterowania z sieci wewnętrznych; oraz

(h) Filtrowanie nieautoryzowanego ruchu w płaszczyźnie sterowania z sieci zewnętrznych..

Omówienie: Zewnętrzne usługi telekomunikacyjne mogą świadczyć usługi w zakresie przesyłania danych i/lub głosu. Przykłady ruchu w płaszczyźnie sterowania obejmują Border Gateway Protocol (BGP) routing, system nazw domen (DNS) i zarządzanie ptotokołami.

Dodatkowe informacje na temat wykorzystania zasobów infrastruktury klucza publicznego (*ang. resource public key infrastructure - RPKI*) do ochrony tras BGP i wykrywania nieautoryzowanych rozgłoszeń BGP, zawarte są w publikacji [NIST SP 800-189].

Zabezpieczenia powiązane: AC-3, SC-8, SC-20, SC-21 i SC-22.

(5) OCHRONA POŁĄCZEŃ BRZEGOWYCH | ODRZUĆ DOMYŚLNIE / POZWÓL NA WYJĄTEK

Domyślnie odmawia się dostępu do komunikacji sieciowej i zezwala na komunikację sieciową w drodze wyjątku [***Wybór (jeden lub więcej): na zarządzanych interfejsach; dla*** [***Realizacja: systemy zdefiniowane przez organizację***]]**.**

Omówienie: Domyślne odmawianie i zezwalanie na podstawie wyjątków dotyczy przychodzącego i wychodzącego ruchu telekomunikacyjnego w sieci. Polityka ruchu sieciowego typu "odmawiaj wszystkim, zezwalaj na wyjątki" zapewnia, że dozwolone są tylko te połączenia systemowe, które są niezbędne i zatwierdzone. Domyślne blokowanie i zezwalanie na podstawie wyjątków dotyczy również systemu, który jest połączony z systemem zewnętrznym.

Zabezpieczenia powiązane: Brak.

(6) OCHRONA POŁĄCZEŃ BRZEGOWYCH | ODPOWIEDŹ NA ROZPOZNANE AWARIE

[Wycofane: Włączone do SC-7(18)].

(7) OCHRONA POŁĄCZEŃ BRZEGOWYCH | DZIELONE TUNELOWANIE URZĄDZEŃ ZDALNYCH

Zapobieganie dzieleniu tuneli pomiędzy urządzeniami zdalnymi łączącymi się z systemami organizacyjnymi, chyba że tunel dzielony jest bezpiecznie udostępniony przy użyciu [*Realizacja: zabezpieczenia zdefiniowane przez organizację*].

Omówienie: Tunelowanie dzielone to proces umożliwiający zdalnemu użytkownikowi (*ang. remote user*) lub urządzeniu (*ang. remote device)*

zestawienie połączenia z systemem w sposób inny niż zdalny[98] (*ang. non-remote connection*) i jednoczesne komunikowanie się za pomocą innego połączenia z zasobem w sieci zewnętrznej. Ta metoda dostępu do sieci umożliwia użytkownikowi dostęp do zdalnych urządzeń i jednocześnie dostęp do niekontrolowanych sieci. Tunelowanie dzielone może być wykorzystywane przez użytkowników zdalnych do komunikowania się z lokalnymi zasobami systemowymi, takimi jak drukarki lub serwery plików. Jednakże, dzielenie tunelowania może ułatwić nieautoryzowane połączenia zewnętrzne, czyniąc system podatnym na ataki i eksfiltrację informacji organizacyjnych. Tunelowaniu dzielonemu można zapobiegać poprzez wyłączanie ustawień konfiguracyjnych, które umożliwiają takie możliwości w urządzeniach zdalnych oraz uniemożliwienie konfigurowania tych ustawień przez użytkowników. Zapobieganie można również osiągnąć poprzez wykrywanie tunelowania dzielonego (lub ustawień konfiguracyjnych, które umożliwiają tunelowanie dzielone) w urządzeniu zdalnym oraz poprzez zakazanie połączenia, jeżeli urządzenie zdalne korzysta z tunelowania dzielonego. Do bezpiecznego udostępniania tunelu dzielonego można użyć wirtualnej sieci prywatnej (VPN). Bezpiecznie udostępniona sieć VPN obejmuje blokowanie komunikacji z wykluczonym, zarządzanym i znanym środowiskiem lub z określonym zestawem wstępnie zatwierdzonych adresów bez kontroli użytkownika.

Zabezpieczenia powiązane: Brak.

(8) OCHRONA POŁĄCZEŃ BRZEGOWYCH | RUCH TELEKOMUNIKACYJNY DO AUTORYZOWANYCH SERWERÓW PROXY

[98] Przykładem ścieżki komunikacyjnej z urządzenia zdalnego, nie będącej ścieżką zdalną, jest wirtualna sieć prywatna.

Kierowanie [***Realizacja: zdefiniowany przez organizację wewnętrzny ruch telekomunikacyjny***] **do** [***Realizacja: zdefiniowane przez organizację sieci zewnętrzne***] **poprzez zarządzane interfejsy uwierzytelnionych serwerów proxy.**

Omówienie: Sieci zewnętrzne to sieci pozostające poza kontrolą organizacyjną. Serwer proxy to serwer (tzn. system lub aplikacja), który działa jako pośrednik dla klientów żądających zasobów systemowych od nieorganizacyjnych lub innych serwerów organizacyjnych. Zasoby systemowe, które mogą być wymagane, obejmują pliki, połączenia, strony internetowe lub usługi. Ocenia się, że żądania klientów powstałe w wyniku połączenia z serwerem proxy mają na celu zarządzanie złożonością i zapewnienie dodatkowej ochrony poprzez ograniczenie bezpośredniego połączenia. Urządzenia filtrujące zawartość stron internetowych są jednymi z najbardziej popularnych serwerów proxy, które zapewniają dostęp do Internetu. Serwery proxy mogą obsługiwać rejestrowanie sesji protokołów kontroli transmisji (*ang. Transmission Control Protocol – TCP*) i blokowanie określonych ujednoliconych formatów adresowania (*ang. Uniform Resource Locators – URL*), adresów protokołu internetowego (*ang. Internet protocol – IP*) i nazw domen. Serwery proxy mogą być konfigurowane za pomocą zdefiniowanych organizacyjnie list autoryzowanych i nieautoryzowanych stron internetowych. Należy pamiętać, że serwery proxy mogą blokować korzystanie z wirtualnych sieci prywatnych (VPN) i stwarzać możliwość ataków "man-in-the-middle" (w zależności od implementacji).

Zabezpieczenia powiązane: AC-3.

(9) OCHRONA POŁĄCZEŃ BRZEGOWYCH | OGRANICZENIE ZAGROŻEŃ WYJŚCIOWEGO RUCHU TELEKOMUNIKACYJNEGO

(a) Wykrywanie i odrzucanie ruchu wychodzącego stanowiącego zagrożenie dla systemów zewnętrznych; oraz

(b) Kontrolowanie tożsamości użytkowników wewnętrznych związanych z odmową komunikacji.

Omówienie: Wykrywanie wychodzącego ruchu komunikacyjnego powstającego w wyniku działań wewnętrznych, który może stanowić zagrożenie dla systemów zewnętrznych, znane jest jako wykrywanie wyprowadzania danych (ang. extrusion detection). Jest realizowane wewnątrz systemu na zarządzanych interfejsach. Obejmuje analizę przychodzącego i wychodzącego ruchu komunikacyjnego w poszukiwaniu oznak wewnętrznych zagrożeń pod kątem bezpieczeństwa systemów zewnętrznych. Wewnętrzne zagrożenia dla systemów zewnętrznych obejmują ruch wskazujący na ataki typu "blokada usług" (*ang. denial-of-service - DoS*), ruch ze sfałszowanymi adresami źródłowymi oraz ruch zawierający złośliwy kod. Organizacje posiadają kryteria określania, aktualizacji i zarządzania zidentyfikowanymi zagrożeniami związanymi z wykrywaniem eksfiltracji.

Zabezpieczenia powiązane: AU-2, AU-6, SC-5, SC-38, SC-44, SI-3, SI-4.

(10) OCHRONA POŁĄCZEŃ BRZEGOWYCH | ZAPOBIEGANIE EKSFILTRACJI

(a) Zapobieganie eksfiltracji informacji; oraz

(b) Przeprowadzanie testów eksfiltracyjnych [***Realizacja: częstotliwość określona przez organizację***]**.**

Omówienie: Zapobieganie eksfiltracji dotyczy zarówno umyślnej, jak i niezamierzonej eksfiltracji informacji. Techniki stosowane w celu zapobiegania eksfiltracji informacji z systemów mogą być wdrażane na wewnętrznych punktach końcowych, granicach zewnętrznych oraz w obrębie zarządzanych interfejsów i obejmują przestrzeganie formatów protokołów, monitorowanie działań sygnalizacyjnych pochodzących z systemów, odłączanie zewnętrznych interfejsów sieciowych (chyba, że jest to bezwzględnie konieczne), stosowanie analizy profilu ruchu w celu wykrywania odchyleń od oczekiwanego natężenia i rodzaju ruchu, oddzwanianie do centrów zarządzania i kontroli, przeprowadzanie testów penetracyjnych, monitorowanie steganografii, dezasemblację i ponowną asemblację nagłówków pakietów oraz stosowanie narzędzi zapobiegających

utracie i wyciekowi danych. Do urządzeń wymuszających ścisłe przestrzeganie formatów protokołów należą firewalle z funkcją głębokiej inspekcji pakietów oraz bramy uniwersalnego języka znaczników (ang. Extensible Markup Language - XML). Urządzenia te weryfikują zgodność z formatami i specyfikacjami protokołów w warstwie aplikacji i identyfikują podatności, które nie mogą być wykryte przez urządzenia działające w warstwie sieciowej lub transportowej. Zapobieganie eksfiltracji jest podobne do zapobiegania utracie danych lub wyciekowi danych i jest ściśle związane z rozwiązaniami międzydomenowymi oraz systemami nadzoru, które egzekwują wymagania dotyczące przepływu informacji.

Zabezpieczenia powiązane: AC-2, CA-8, SI-3.

(11) OCHRONA POŁĄCZEŃ BRZEGOWYCH | OGRANICZENIE PRZYCHODZĄCEGO RUCHU KOMUNIKACYJNEGO

Zezwolanie jedynie na kierowanie komunikacji przychodzącej z [***Realizacja: zdefiniowane przez organizację autoryzowane źródła***] **do** [***Realizacja: zdefiniowane przez organizację autoryzowane miejsca docelowe***]**.**

Omówienie: Ogólne techniki walidacji adresów źródłowych są stosowane w celu ograniczenia wykorzystywania nielegalnych i nieprzydzielonych adresów źródłowych, jak również adresów źródłowych, które powinny być wykorzystywane wyłącznie w ramach systemu. Ograniczenie ruchu połączeń przychodzących pozwala określić, że pary adresów źródłowych i docelowych reprezentują komunikację autoryzowaną lub dozwoloną. Ustalenia mogą być oparte na kilku czynnikach, w tym na obecności takich par adresów na listach autoryzowanych lub dozwolonych połączeń, braku takich par adresów na listach nieautoryzowanych lub niedozwolonych par, lub spełnieniu bardziej ogólnych zasad dotyczących autoryzowanych lub niedozwolonych par adresów źródłowych i docelowych. Silna autoryzacja adresów sieciowych nie jest możliwa bez użycia jawnych (*ang. explicit*) protokołów bezpieczeństwa, a tym samym adresy mogą

być często sfałszowane (*ang. spoofing*). Ponadto można stosować metody ograniczania ruchu przychodzącego oparte na tożsamości, w tym listy kontroli dostępu do routera i reguły zapory sieciowej.

Zabezpieczenia powiązane: AC-3.

(12) OCHRONA POŁĄCZEŃ BRZEGOWYCH | SYSTEM OCHRONY KOMPUTERA GŁÓWNEGO TYPU HOST

Wdrożenie [Realizacja: zdefiniowane przez organizację *mechanizmy ochrony połączeń brzegowych oparte na hostach*] w [Realizacja: *zdefiniowane przez organizację komponenty systemu*].

Omówienie: Mechanizmy ochrony połączeń brzegowych oparte na komputerze głównym typu host obejmują zapory sieciowe typu host. Do komponentów systemu, które wykorzystują mechanizmy ochrony połączeń brzegowych oparte na hostach, należą serwery, stacje robocze, notebooki i urządzenia mobilne.

Zabezpieczenia powiązane: Brak.

(13) OCHRONA POŁĄCZEŃ BRZEGOWYCH | IZOLACJA NARZĘDZI BEZPIECZEŃSTWA / MECHANIZMÓW / KOMPONENTÓW WSPARCIA

Odizolowanie [*Realizacja: zdefiniowane przez organizację narzędzia, mechanizmy i komponenty wspierające bezpieczeństwo informacji*] od innych wewnętrznych komponentów systemu poprzez wdrożenie fizycznie oddzielonych podsieci z zarządzanymi interfejsami do innych komponentów systemu.

Omówienie: Fizycznie odseparowane podsieci z zarządzanymi interfejsami są użyteczne w odizolowaniu systemów obronnych sieci komputerowych od krytycznych sieci przetwarzania operacyjnego, aby zapobiec odkrywaniu przez przeciwników technik analitycznych i kryminalistycznych stosowanych przez organizacje.

Zabezpieczenia powiązane: SC-2, SC-3.

(14) OCHRONA POŁĄCZEŃ BRZEGOWYCH | OCHRONA PRZED NIEAUTORYZOWANYMI POŁĄCZENIAMI FIZYCZNYMI

Ochrona przed nieautoryzowanymi połączeniami fizycznymi z [*Realizacja: zarządzane interfejsy zdefiniowane przez organizację*].

Omówienie: Systemy, które działają w różnych kategoriach bezpieczeństwa lub poziomach klasyfikacji, mogą podlegać wspólnym fizycznym i środowiskowym zabezpieczeniom, ponieważ systemy mogą korzystać ze wspólnej przestrzeni w ramach tych samych obiektów. W praktyce możliwe jest, że te oddzielne systemy mogą mieć wspólne pomieszczenia na sprzęt, szafy kablowe i tory dystrybucji kabli. Ochronę przed nieuprawnionymi połączeniami fizycznymi można osiągnąć poprzez zastosowanie dokładnie określonych i fizycznie oddzielonych korytek kablowych, stelaży połączeniowych i paneli krosowych dla każdej strony zarządzanych interfejsów wraz z fizycznymi kontrolami dostępu, które wymuszają ograniczony, autoryzowany dostęp do tych elementów.

Zabezpieczenia powiązane: PE-4, PE-19.

(15) OCHRONA POŁĄCZEŃ BRZEGOWYCH | SIECIOWY DOSTĘP UPRZYWILEJOWANY

Kierowanie wszystkich uprzywilejowanych połączeń sieciowych poprzez dedykowany, zarządzany interfejs w celu kontroli dostępu i audytu.

Omówienie: Uprzywilejowany dostęp zapewnia większą dostępność do funkcji systemu, w tym funkcji bezpieczeństwa. Adwersarze starają się uzyskać uprzywilejowany dostęp do systemów poprzez zdalny dostęp w celu wywołania niekorzystnych skutków dla organizacji, np. poprzez usunięcie informacji lub obniżenie krytycznych funkcji systemu. Ukierunkowane, sieciowe, uprzywilejowane żądania dostępu poprzez dedykowany, zarządzany interfejs dodatkowo ogranicza uprzywilejowany dostęp w celu zwiększenia kontroli dostępu i audytu.

Zabezpieczenia powiązane: AC-2, AC-3, AU-2, SI-4.

(16) OCHRONA POŁĄCZEŃ BRZEGOWYCH | ZAPOBIEGANIE WYKRYWANIU KOMPONENTÓW SYSTEMU

Zapobieganie wykryciu określonych komponentów systemu tworzących interfejs zarządzany.

Omówienie: Zapobieganie wykrywaniu komponentów systemu reprezentujących zarządzany interfejs pomaga chronić adresy sieciowe tych komponentów przed odkryciem za pomocą powszechnie stosowanych narzędzi i technik używanych do identyfikacji urządzeń w sieciach. Adresy sieciowe nie są dostępne do wykrycia i wymagają uzyskania wcześniejszej wiedzy w celu uzyskania dostępu. Zapobieganie wykryciu komponentów i urządzeń może być osiągnięte poprzez nie publikowanie adresów sieciowych, używanie translacji adresów sieciowych lub nie wprowadzanie adresów do systemów nazw domen. Inną techniką zapobiegania jest okresowa zmiana adresów sieciowych.

Zabezpieczenia powiązane: Brak.

(17) OCHRONA POŁĄCZEŃ BRZEGOWYCH | AUTOMATYCZNE EGZEKWOWANIE FORMATÓW PROTOKOŁU

Egzekwowanie przestrzegania formatów protokołów.

Omówienie: Komponenty systemu, które egzekwują formaty protokołów, obejmują firewalle z zaawansowaną inspekcją pakietów i bramy XML. Komponenty te weryfikują zgodność z formatami i specyfikacjami protokołów w warstwie aplikacji i identyfikują podatności, które nie mogą być wykryte przez urządzenia działające w warstwie sieciowej lub transportowej.

Zabezpieczenia powiązane: SC-4.

(18) OCHRONA POŁĄCZEŃ BRZEGOWYCH |BŁĄD BEZPIECZEŃSTWA

Zapobieganie wprowadzaniu systemów w stan niezabezpieczony w przypadku awarii urządzenia zabezpieczającego ochronę granicę systemu.

Omówienie: Bezpieczeństwo w przypadku awarii jest stanem osiąganym poprzez zastosowanie mechanizmów zapewniających, że w przypadku awarii operacyjnych urządzeń ochrony brzegowej opartych na zarządzanych interfejsach, systemy nie wchodzą w stany niezabezpieczone, w których zamierzone właściwości bezpieczeństwa nie są już zachowane. Zarządzane interfejsy obejmują routery, zapory sieciowe i bramy aplikacji, które znajdują się w chronionych podsieciach (powszechnie określanych jako strefy zdemilitaryzowane). Awarie urządzeń ochrony granic nie mogą prowadzić do przedostania się do nich informacji spoza urządzeń, ani powodować takiego przedostawania się, jak również nie mogą umożliwiać nieautoryzowanego uwolnienia informacji.

Zabezpieczenia powiązane: CP-2, CP-12, SC-24.

(19) OCHRONA POŁĄCZEŃ BRZEGOWYCH | BLOKOWANIE KOMUNIKACJI Z HOSTAMI SPOZA ORGANIZACJI

Blokowanie przychodzącego i wychodzącego ruchu telekomunikacyjnego pomiędzy [*Realizacja: klienci komunikacyjni zdefiniowani przez organizację*], którzy są niezależnie skonfigurowani przez użytkowników końcowych i zewnętrznych dostawców usług.

Omówienie: Klientami komunikacyjnymi konfigurowanymi niezależnie przez użytkowników końcowych i zewnętrznych dostawców usług są klienci komunikatorów internetowych oraz oprogramowanie i aplikacje do obsługi wideokonferencji. Blokowanie ruchu nie dotyczy klientów komunikacyjnych, którzy są skonfigurowani przez organizacje do wykonywania autoryzowanych funkcji.

Zabezpieczenia powiązane: Brak.

(20) OCHRONA POŁĄCZEŃ BRZEGOWYCH | DYNAMICZNA IZOLACJA I SEGREGACJA

Zapewnienie możliwości dynamicznego oddzielenia [*Realizacja: zdefiniowane przez organizację komponenty systemu*] od innych komponentów systemu.

Omówienie: Możliwość dynamicznego odizolowania niektórych wewnętrznych komponentów systemu jest przydatna, gdy konieczne jest wydzielenie lub oddzielenie komponentów systemu o wątpliwym pochodzeniu od komponentów, które są bardziej wiarygodne. Izolacja komponentów zmniejsza powierzchnię ataku systemów organizacyjnych. Izolacja wybranych komponentów systemu może również ograniczyć szkody spowodowane udanymi atakami, gdy takie ataki mają miejsce.

Zabezpieczenia powiązane: Brak.

(21) OCHRONA POŁĄCZEŃ BRZEGOWYCH | IZOLACJA KOMPONENTÓW SYSTEMU

Stosowanie mechanizmów ochrony granic w celu wyodrębnienia [*Realizacja: zdefiniowane przez organizację komponenty systemu*] wspierających [*Realizacja: zdefiniowane przez organizację misje i/lub funkcje biznesowe*].

Omówienie: Organizacje mogą izolować komponenty systemu, które wykonują różne zadania lub funkcje biznesowe. Taka izolacja ogranicza nieautoryzowany przepływ informacji pomiędzy komponentami systemu i daje możliwość zastosowania większego poziomu ochrony dla wybranych komponentów systemu. Izolacja komponentów systemu z mechanizmami ochrony brzegowej daje możliwość zwiększenia ochrony poszczególnych komponentów systemu i skuteczniejszej kontroli przepływu informacji pomiędzy tymi komponentami. Izolowanie elementów systemu zapewnia zwiększoną ochronę, która ogranicza potencjalne szkody wynikające z wrogich cyberataków i błędów. Stopień izolacji różni się w zależności od wybranych mechanizmów. Mechanizmy ochrony brzegowej obejmują routery, bramy i zapory sieciowe, które rozdzielają elementy systemu na fizycznie odrębne sieci lub podsieci; urządzenia międzydomenowe, które rozdzielają podsieci; techniki wirtualizacji; oraz szyfrowanie przepływów

informacji między komponentami systemu przy użyciu odrębnych kluczy szyfrujących.

Zabezpieczenia powiązane: CA-9.

(22) OCHRONA POŁĄCZEŃ BRZEGOWYCH | ODDZIELNE PODSIECI DO PODŁĄCZENIA DO RÓŻNYCH DOMEN BEZPIECZEŃSTWA

Wdrożenie oddzielnych adresów sieciowych w celu połączenia z systemami w różnych domenach bezpieczeństwa.

Omówienie: Dekompozycja systemów na podsieci pomaga zapewnić odpowiedni poziom ochrony połączeń sieciowych do różnych domen bezpieczeństwa, które zawierają informacje o różnych kategoriach bezpieczeństwa lub poziomach klasyfikacji.

Zabezpieczenia powiązane: Brak.

(23) OCHRONA POŁĄCZEŃ BRZEGOWYCH | WYŁĄCZENIE INFORMACJI ZWROTNEJ NADAWCY W PRZYPADKU AWARII PROTOKOŁU UWIERZYTELNIAJĄCEGO

Wyłączenie informacji zwrotnych do nadawców o niepowodzeniu weryfikacji formatu protokołu.

Omówienie: Wyłączenie informacji zwrotnej wysyłanej do nadawców w przypadku wystąpienia błędu w formacie walidacji protokołu uniemożliwia adwersarzom uzyskanie informacji, które byłyby niedostępne bez tego typu błędu.

Zabezpieczenia powiązane: Brak.

(24) OCHRONA POŁĄCZEŃ BRZEGOWYCH | DANE OSOBOWE

W przypadku systemów, które przetwarzają informacje umożliwiające identyfikację osób (dane osobowe), należy:

(a) Stosować następujące zasady przetwarzania: [*Realizacja: reguły przetwarzania danych osobowych zdefiniowane przez organizację*];

(b) Monitorować dozwolone procesy przetwarzania na zewnętrznych interfejsach systemu oraz na kluczowych wewnętrznych granicach systemu;

(c) Dokumentować każdy wyjątek dotyczący przetwarzania; oraz

(d) Dokonać przeglądu i usunąć wyjątki, które nie są już obsługiwane.

Omówienie: Zarządzanie przetwarzaniem danych osobowych jest ważnym aspektem ochrony prywatności obywateli. Stosowanie, monitorowanie i dokumentowanie wyjątków od zasad przetwarzania danych osobowych zapewnia, że dane osobowe są przetwarzane wyłącznie zgodnie z ustalonymi wymogami dotyczącymi prywatności.

Zabezpieczenia powiązane: PT-2, SI-15.

(25) OCHRONA POŁĄCZEŃ BRZEGOWYCH | BEZPIECZNE POŁĄCZENIA KRAJOWYCH SYSTEMÓW JAWNYCH

Zakazanie bezpośredniego podłączania [*Realizacja: zdefiniowany organizacyjnie krajowy system jawny*] do sieci zewnętrznej bez użycia [*Realizacja: zdefiniowane organizacyjnie urządzenia zabezpieczające granicę systemu*].

Omówienie: Bezpośrednie połączenie to dedykowane fizyczne lub wirtualne połączenie pomiędzy dwoma lub więcej systemami. Organizacje zazwyczaj nie mają pełnej kontroli nad zewnętrznymi sieciami, w tym nad Internetem. Urządzenia ochrony granic systemu (np. zapory ogniowe, bramy i routery) pośredniczą w komunikacji i przepływie informacji między krajowymi systemami jawnymi, a sieciami zewnętrznymi.

Zabezpieczenia powiązane: Brak.

(26) OCHRONA POŁĄCZEŃ BRZEGOWYCH | BEZPIECZNE POŁĄCZENIA KRAJOWYCH SYSTEMÓW NIEJAWNYCH

Zakazanie bezpośredniego podłączenia krajowego systemu niejawnego do sieci zewnętrznej bez użycia [***Realizacja: brzegowe urządzenie zabezpieczające zdefiniowane przez organizację***] [99].

Omówienie: Bezpośrednie połączenie to dedykowane fizyczne lub wirtualne połączenie pomiędzy dwoma lub więcej systemami. Organizacje zazwyczaj nie mają pełnej kontroli nad zewnętrznymi sieciami, w tym nad Internetem. Urządzenia ochrony granic systemu (np. zapory ogniowe, bramy i routery) pośredniczą w komunikacji i przepływie informacji między krajowymi systemami niejawnymi, a sieciami zewnętrznymi. Ponadto zatwierdzone brzegowe urządzenia zabezpieczające (zazwyczaj zarządzane systemy interfejsów lub międzydomenowe) zapewniają egzekwowanie przepływu informacji z systemów do sieci zewnętrznych.

Zgodnie obowiązującymi przepisami połączenie systemu niejawnego z siecią zewnętrzną odbywa się po spełnieniu wymogów określonych w przepisach wydanych na podstawie ustawy o ochronie informacji niejawnych.

Zabezpieczenia powiązane: Brak.

(27) OCHRONA POŁĄCZEŃ BRZEGOWYCH | BEZPIECZNE POŁĄCZENIA TRANSGRANICZNYCH SYSTEMÓW JAWNYCH

Zakazanie bezpośredniego podłączenia do sieci zewnętrznej [*Realizacja: zdefiniowany przez organizację jawny bezpieczny system transgraniczny*] bez użycia [*Realizacja: brzegowe urządzenie zabezpieczające zdefiniowane przez organizację*].

Omówienie: Bezpośrednie połączenie to dedykowane fizyczne lub wirtualne połączenie pomiędzy dwoma lub więcej systemami. Organizacje zazwyczaj nie mają pełnej kontroli nad zewnętrznymi sieciami, w tym nad Internetem.

[99] Realizowane zgodnie z przepisami ustawy o ochronie informacji niejawnych.

Urządzenia ochrony granic systemu (np. zapory ogniowe, bramy i routery) pośredniczą w komunikacji i przepływie informacji między krajowymi systemami jawnymi, a sieciami zewnętrznymi.

Zabezpieczenia powiązane: Brak.

(28) OCHRONA POŁĄCZEŃ BRZEGOWYCH | POŁĄCZENIA Z SIECIAMI PUBLICZNYMI

Zakazanie bezpośredniego podłączenia [***Realizacja: system zdefiniowany przez organizację***] **do sieci publicznej.**

Omówienie: Bezpośrednie połączenie to dedykowane fizyczne lub wirtualne połączenie pomiędzy dwoma lub więcej systemami. Sieć publiczna to sieć dostępna publicznie, w tym Internet i organizacyjne sieci ekstranet z dostępem publicznym.

Zabezpieczenia powiązane: Brak.

(29) OCHRONA POŁĄCZEŃ BRZEGOWYCH | SEPARACJA PODSIECI W CELU ODIZOLOWANIA FUNKCJI

Zaimplementowanie [*Wybór: fizyczne; logiczne*] oddzielenia podsieci w celu wyodrębnienia następujących krytycznych komponentów i funkcji systemu: [***Realizacja: zdefiniowane przez organizację krytyczne komponenty i funkcje systemu***]**.**

Omówienie: Oddzielenie krytycznych komponentów i funkcji systemu od innych, niekrytycznych komponentów i funkcji systemu poprzez oddzielne podsieci może być konieczne w celu zmniejszenia podatności na katastroficzne lub wyniszczające naruszenia lub kompromitacje, które prowadzą do awarii systemu. Na przykład, fizyczne oddzielenie funkcji sterowania i kontroli od funkcji rozrywkowych, poprzez oddzielne podsieci w komercyjnym obiekcie, zapewnia zwiększony poziom pewności co do wiarygodności krytycznych funkcji systemu.

Zabezpieczenia powiązane: Brak.

Referencje: [OMB A-130], [FIPS 199], [NIST SP 800-37], [NIST SP 800-41], [NIST SP 800-77], [NIST SP 800 189].

SC-8 POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI

Zabezpieczenie podstawowe: Ochrona [*Wybór (jeden lub więcej): poufność; integralność*] przekazywanych informacji.

Omówienie: Ochrona poufności i integralności przesyłanych informacji dotyczy sieci wewnętrznych i zewnętrznych, a także wszelkich komponeentów systemu, które mogą przesyłać informacje, w tym serwerów, notebooków, komputerów stacjonarnych, urządzeń przenośnych, drukarek, kopiarek, skanerów, faksów i urządzeń radiowych. Niezabezpieczone ścieżki komunikacyjne narażone są na możliwość przechwytywania i modyfikacji. Ochrona poufności i integralności informacji może być realizowana za pomocą środków fizycznych lub logicznych. Ochrona fizyczna może być osiągnięta poprzez zastosowanie chronionych systemów dystrybucyjnych. Chroniony system dystrybucyjny to przewodowy lub światłowodowy system telekomunikacyjny, w skład którego wchodzą terminale i odpowiednie elektromagnetyczne, akustyczne, elektryczne i fizyczne urządzenia zabezpieczające pozwalające na wykorzystanie go do niezaszyfrowanej transmisji informacji niejawnych. Ochrona logiczna może być osiągnięta poprzez zastosowanie technik szyfrowania.

Organizacje, które polegają na dostawcach komercyjnych, oferujących usługi przesyłowe jako masowe usługi towarowe, a nie jako usługi w pełni dedykowane, mogą mieć trudności z uzyskaniem niezbędnych poświadczeń dotyczących wdrożenia niezbędnych zabezpieczeń w zakresie poufności i integralności transmisji danych. W takich sytuacjach organizacje określają, jakie rodzaje usług w zakresie poufności lub integralności są dostępne w standardowych, komercyjnych pakietach usług telekomunikacyjnych. Jeżeli nie jest możliwe uzyskanie niezbędnych zabezpieczeń i zapewnień o skuteczności zabezpieczeń za pomocą odpowiednich kontraktowych środków transportowych, organizacje mogą wdrożyć odpowiednie zabezpieczenia wyrównawcze.

Zabezpieczenia powiązane: AC-17, AC-18, AU-10, IA-3, IA-8, IA-9, MA-4, PE-4, SA-4, SA-8, SC-7, SC-16, SC- 20, SC-23, SC-28.

Zabezpieczenia rozszerzone:

(1) POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI | OCHRONA KRYPTOGRAFICZNA

Zaimplementowanie mechanizmów kryptograficznych e celu [***Wybór (jeden lub więcej): zapobieganie nieautoryzowanemu ujawnieniu informacji; wykrywanie zmian w informacjach***] **podczas transmisji.**

Omówienie: Szyfrowanie chroni informacje przed nieautoryzowanym ujawnieniem i modyfikacją podczas transmisji. Mechanizmy kryptograficzne, które chronią poufność i integralność informacji podczas transmisji, obejmują protokoły TLS i IPSec. Mechanizmy kryptograficzne stosowane do ochrony integralności informacji obejmują kryptograficzne funkcje skrótów, które mają zastosowanie w podpisach cyfrowych, sumach zabezpieczeń i kodach uwierzytelniania wiadomości.

Zabezpieczenia powiązane: SC-12, SC-13.

(2) POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI | OBSŁUGA „PRZED" i „PO" TRANSMISJI

Zachowanie [***Wybór (jeden lub więcej): poufność; integralność***] **informacji podczas przygotowania do transmisji i podczas odbioru.**

Omówienie: Informacje mogą być nieumyślnie lub złośliwie ujawnione lub zmodyfikowane podczas przygotowywania do transmisji lub podczas odbioru, w tym podczas agregacji, w punktach przetwarzania protokołów oraz podczas pakowania i rozpakowywania. Takie nieautoryzowane ujawnienie lub modyfikacja naruszają poufność lub integralność informacji.

Zabezpieczenia powiązane: Brak.

(3) POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI | OCHRONA KRYPTOGRAFICZNA ZEWNĘTRZNYCH KOMUNIKATÓW

Zaimplementowanie mechanizmów kryptograficznych w celu ochrony zewnętrznych komunikatów, chyba że są one w inny sposób chronione przez [***Realizacja: zdefiniowane przez organizację alternatywne zabezpieczenia fizyczne***]**.**

Omówienie: Kryptograficzna ochrona wiadomości zewnętrznych dotyczy ochrony przed nieautoryzowanym ujawnieniem informacji. Elementy zewnętrzne wiadomości zawierają nagłówki wiadomości i informacje o routingu. Ochrona kryptograficzna zapobiega wykorzystywaniu zewnętrznych wiadomości i odnosi się do wewnętrznych i zewnętrznych sieci lub łączy, które mogą być widoczne dla osób nieupoważnionych. Nagłówki i informacje o routingu są czasami przesyłane w postaci jawnego tekstu (tj. niezaszyfrowane), ponieważ informacje te nie są identyfikowane przez organizacje jako mające znaczną wartość lub ponieważ szyfrowanie informacji może skutkować niższą wydajnością sieci lub wyższymi kosztami. Alternatywne zabezpieczenia fizyczne obejmują chronione systemy dystrybucji.

Zabezpieczenia powiązane: SC-12, SC-13.

(4) POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI | KOMUNIKACJA UKRYTA / LOSOWA

Zaimplementowanie mechanizmów kryptograficznych w celu maskowania lub nadania losowości schematom komunikacji, chyba że są one chronione przez [***Realizacja: zdefiniowane przez organizację alternatywne zabezpieczenia fizyczne***]**.**

Omówienie: Maskowanie lub randomizowanie (nadawanie losowości) wzorców komunikacji dotyczy ochrony przed nieautoryzowanym ujawnieniem informacji. Schematy komunikacji obejmują częstotliwość, okresy, przewidywalność i ilość. Zmiany w schematach komunikacji mogą ujawniać informacje o wartości wywiadowczej, szczególnie w połączeniu z innymi dostępnymi informacjami

związanymi z misją i funkcjami biznesowymi organizacji. Maskowanie lub randomizowanie komunikacji uniemożliwia pozyskiwanie informacji wywiadowczych w oparciu o wzorce komunikacji i dotyczy zarówno wewnętrznych, jak i zewnętrznych sieci lub łączy, które mogą być widoczne dla osób nieupoważnionych. Szyfrowanie łączy i przesyłanie ich w sposób ciągły, stały lub losowy uniemożliwia pozyskiwanie danych wywiadowczych na podstawie schematów komunikacyjnych systemu. Alternatywne środki zabezpieczeń fizycznych obejmują chronione systemy dystrybucji.

Zabezpieczenia powiązane: SC-12, SC-13.

(5) POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI | CHRONIONY SYSTEM DYSTRYBUCJI

Wdrożenie [*Realizacja: zdefiniowany przez organizację chroniony system dystrybucji*] w celu [*Wybór (jeden lub więcej): zapobieganie nieautoryzowanemu ujawnieniu informacji; wykrywanie zmian w informacji*] podczas transmisji.

Omówienie: Celem chronionego systemu dystrybucji jest powstrzymywanie, wykrywanie lub utrudnianie fizycznego dostępu do linii komunikacyjnych, którymi przesyłane są informacje dotyczące bezpieczeństwa narodowego.

Zabezpieczenia powiązane: Brak.

Referencje: [FIPS 140-3], [FIPS 197], [NIST SP 800-52], [NIST SP 800-77], [NIST SP 800-81-2], [NIST SP 800-113], [NIST SP 800-177], [IR 8023].

SC-9 POUFNOŚĆ TRANSMISJI

[Wycofane: Włączone do SC-8].

SC-10 ZAKOŃCZENIE POŁĄCZENIA SIECIOWEGO

Zabezpieczenie podstawowe: Zakończenie połączenia sieciowego związanego z sesją komunikacyjną na koniec sesji lub po [*Realizacja: określony przez organizację okres czasu*] braku aktywności.

Omówienie: Zakończenie połączenia sieciowego dotyczy sieci wewnętrznych i zewnętrznych. Zakończenie połączeń sieciowych związanych z określonymi sesjami komunikacyjnymi obejmuje odmowę przydzielenia adresu TCP/IP lub par portów na poziomie systemu operacyjnego oraz odmowę przydzielenia sieci na poziomie aplikacji, jeśli kilka sesji aplikacji korzysta z jednego połączenia sieciowego na poziomie systemu operacyjnego. Okresy nieaktywności mogą być ustalane przez organizacje i obejmują okresy według rodzaju dostępu do sieci lub dla określonych dostępów sieciowych.

Zabezpieczenia powiązane: AC-17, SC-23.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

SC-11 ZAUFANA ŚCIEŻKA KOMUNIKACYJNA

Zabezpieczenie podstawowe:

a. Ustanowienie [*Wybór: fizyczna; logiczna*] izolowanej zaufanej ścieżki komunikacyjnej do komunikacji między użytkownikiem, a zaufanymi komponentami systemu; oraz

b. Zezwolenie użytkownikom na odwoływanie się do zaufanej ścieżki komunikacyjnej do komunikacji między użytkownikiem, a następującymi funkcjami bezpieczeństwa systemu, w tym co najmniej uwierzytelnianie i ponowne uwierzytelnianie: [*Realizacja: funkcje bezpieczeństwa zdefiniowane przez organizację*].

Omówienie: Zaufane ścieżki to mechanizmy, za pomocą których użytkownicy mogą komunikować się (za pomocą urządzeń wejściowych, takich jak klawiatury) bezpośrednio z funkcjami bezpieczeństwa systemów z wymaganą pewnością do obsługi polityk bezpieczeństwa. Mechanizmy zaufanych ścieżek mogą być aktywowane tylko przez użytkowników lub funkcje bezpieczeństwa systemów organizacyjnych. Odpowiedzi użytkownika, które występują za pośrednictwem zaufanych ścieżek są chronione przed modyfikacją i ujawnieniem niezaufanym aplikacjom. Organizacje wykorzystują ścieżki zaufane do wiarygodnych, wysoce pewnych połączeń między funkcjami bezpieczeństwa systemów i użytkowników, w tym podczas logowania do systemu. Pierwotne implementacje ścieżek zaufanych wykorzystywały sygnał pozapasmowy do inicjowania ścieżki, taki jak użycie klucza <BREAK> nie transmitującego znaków, które mogą zostać sfałszowane. W późniejszych implementacjach używano kombinacji klawiszy, która nie może zostać przechwycona (np. klawisze <CTRL> + <ALT> + <DEL>). Takie kombinacje klawiszy są jednak specyficzne dla danej platformy i mogą nie zapewniać implementacji zaufanej ścieżki w każdym przypadku. Egzekwowanie zaufanych ścieżek komunikacyjnych jest zapewniane przez specyficzną implementację, która spełnia koncepcję monitora referencyjnego.

Zabezpieczenia powiązane: AC-16, AC-25, SC-12, SC-23.

Zabezpieczenia rozszerzone:

(1) ZAUFANA ŚCIEŻKA KOMUNIKACYJNA | NIEPODWAŻALNA ŚCIEŻKA KOMUNIKACYJNA

(a) Zapewnienie zaufanej ścieżki komunikacyjnej, która jest w sposób niepodważalny odróżnialna od innych ścieżek komunikacyjnych; oraz

(b) Inicjowanie zaufanej ścieżki komunikacyjnej do komunikacji pomiędzy systemem, a użytkownikiem z wykorzystaniem [***Realizacja: funkcje bezpieczeństwa zdefiniowane przez organizację***]**.**

Omówienie: Niepodważalna ścieżka komunikacji pozwala systemowi na zainicjowanie ścieżki zaufanej, co wymaga, aby użytkownik mógł jednoznacznie rozpoznać źródło komunikacji jako zaufany element systemu. Na przykład, zaufana ścieżka może pojawić się w obszarze wyświetlacza, do którego inne aplikacje nie mają dostępu lub opierać się na obecności identyfikatora, którego nie można sfałszować.

Zabezpieczenia powiązane: Brak.

Referencje: [OMB A-130].

SC-12 GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI

Zabezpieczenie podstawowe: Wprowadzanie i zarządzanie kluczami kryptograficznymi w przypadku stosowania kryptografii w systemie zgodnie z poniższymi wymaganiami dotyczącymi zarządzania kluczami: [*Realizacja: określone przez organizację wymagania dotyczące generowania, dystrybucji, przechowywania, dostępu i niszczenia kluczy*].

Omówienie: Zarządzanie i gener owaniekluczy kryptograficznych może być realizowane z wykorzystaniem procedur ręcznych lub mechanizmów automatycznych z towarzyszącymi procedurami ręcznymi. Organizacje definiują wymagania dotyczące zarządzania kluczami zgodnie z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, politykami, standardami i wytycznymi oraz określają odpowiednie opcje, parametry i poziomy. Organizacje zarządzają zaufanymi magazynami w celu zapewnienia, że tylko zatwierdzone kotwice zaufania są częścią takich magazynów zaufania. Obejmuje to certyfikaty o dostępności zewnętrznej w stosunku do systemów organizacyjnych oraz certyfikaty związane z wewnętrznymi operacjami systemów. Publikacje [NIST CMVP] i [NIST CAVP] dostarczają dodatkowych informacji na temat uwierzytelnionych modułów kryptograficznych i algorytmów, które mogą być wykorzystywane w zarządzaniu i generowaniu kluczy kryptograficznych.

Zabezpieczenia powiązane: AC-17, AU-9, AU-10, CM-3, IA-3, IA-7, SA-4, SA-8, SA-9, SC-8, SC-11, SC-12, SC- 13, SC-17, SC-20, SC-37, SC-40, SI-3, SI-7.

Zabezpieczenia rozszerzone:

(1) GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | DOSTĘPNOŚĆ

Utrzymanie dostępności informacji w przypadku utraty kluczy kryptograficznych przez użytkowników.

Omówienie: Deponowanie kluczy szyfrujących jest powszechną praktyką zapewniającą dostępność w przypadku utraty klucza. Zapomniana fraza hasła jest przykładem utraty klucza kryptograficznego.

Zabezpieczenia powiązane: Brak.

(2) GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | KLUCZE SYMETRYCZNE

Generowanie, kontrolowanie i dystrybucja symetrycznych kluczy kryptograficznych przy użyciu technologii i procesów zarządzania kluczami [*Wybór: zatwierdzone przez organizacje; zatwierdzone przez krajową władzę bezpieczeństwa*].

Omówienie: Publikacje [NIST SP 800-56A], [NIST SP 800-56B] i [NIST SP 800-56C] zawierają wytyczne dotyczące systemów ustanawiania kluczy kryptograficznych i metod ich uzyskiwania. Zalecenia [NIST SP 800-57-1], [NIST SP 800-57-2] i [NIST SP 800-57-3] zawierają wytyczne dotyczące zarządzania kluczami kryptograficznymi.

Zabezpieczenia powiązane: Brak.

(3) GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | KLUCZE ASYMETRYCZNE

Generowanie, kontrolowanie i dystrybucja asymetrycznych kluczy kryptograficznych za pomocą funkcji [*Wybór*]*: technologia i procesy zarządzania kluczami zatwierdzone przez rolę w organizacji; zatwierdzone certyfikaty infrastruktury klucza publicznego klasy 3 lub wstępnie przygotowany materiał klucza; zatwierdzone certyfikaty infrastruktury klucza publicznego klasy 3 lub*

***klasy 4[100]; oraz sprzętowe tokeny zabezpieczające, które chronią klucz prywatny użytkownika*].**

Omówienie: Publikacje [NIST SP 800-56A], [NIST SP 800-56B] i [NIST SP 800-56C] zawierają wytyczne dotyczące systemów ustanawiania kluczy kryptograficznych i metod ich uzyskiwania. Zalecenia [NIST SP 800-57-1], [NIST SP 800-57-2] i [NIST SP 800-57-3] zawierają wytyczne dotyczące zarządzania kluczami kryptograficznymi.

Zabezpieczenia powiązane: Brak.

(4) GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO

[Wycofane: Włączone do SC-12(3)].

(5) GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO / TOKENY SPRZĘTOWE

[Wycofane: Włączone do SC-12(3)].

(6) GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | FIZYCZNE ZABEZPIECZENIE KLUCZY KRYPTOGRAFICZNYCH

Zapewnianie fizycznego zabezpieczenia kluczy kryptograficznych, jeżeli składowane informacje są szyfrowane przez zewnętrznych dostawców usług.

Omówienie: W przypadku organizacji, które korzystają z usług zewnętrznych dostawców (np. dostawców usług w chmurze lub dostawców centrów danych), fizyczna zabezpieczenie kluczy kryptograficznych daje dodatkową pewność, że

[100] Klasa 1 dla osób fizycznych, przeznaczona do wiadomości e-mail.
Klasa 2 dla organizacji, dla których wymagany jest dowód tożsamości.
Klasa 3 do podpisywania serwerów i oprogramowania, dla których przeprowadzana jest niezależna weryfikacja i kontrola tożsamości i uprawnień przez urząd certyfikacji.
Klasa 4 do transakcji biznesowych online między firmami.
Klasa 5 dla organizacji prywatnych lub bezpieczeństwa narodowego.

informacje przechowywane przez takich zewnętrznych dostawców nie są przedmiotem nieautoryzowanego ujawnienia lub modyfikacji.

Zabezpieczenia powiązane: Brak.

Referencje: [FIPS 140-3], [NIST SP 800-56A], [NIST SP 800-56B], [NIST SP 800-56C], [NIST SP 800-57-1], [NIST SP 800-57-2], [NIST SP 800-57-3], [NIST SP 800-63-3], [IR 7956], [IR 7966].

SC-13 OCHRONA KRYPTOGRAFICZNA

Zabezpieczenie podstawowe:

a. Ustalanie [*Realizacja: zdefiniowane przez organizację zastosowania kryptograficzne*]; oraz

b. Zaimplementowanie następujących rodzajów kryptografii wymaganych dla każdego określonego zastosowania kryptograficznego: [*Realizacja: zdefiniowane przez organizację rodzaje kryptografii dla każdego określonego zastosowania kryptograficznego*].

Omówienie: Kryptografia może być stosowana w celu wspierania różnych rozwiązań w zakresie bezpieczeństwa, w tym ochrony informacji niejawnych i nadzorowanych informacji jawnych, dostarczania i wdrażania podpisów cyfrowych oraz egzekwowania rozdziału informacji w przypadku, gdy upoważnione osoby posiadają niezbędne poświadczenia bezpieczeństwa, ale nie posiadają niezbędnych formalnych zatwierdzeń dostępu. Kryptografia może być również wykorzystywana do wspomagania generowania liczb losowych i haszy. Powszechnie stosowane standardy kryptograficzne obejmują kryptografię zatwierdzoną przez stosowny organ. Na przykład organizacje, które muszą chronić informacje niejawne, mogą określić zastosowanie kryptografii zatwierdzonej przez krajową władzę bezpieczeństwa. Organizacje, które muszą dostarczać i wdrożać podpisy cyfrowe, mogą określić wykorzystanie kryptografii zatwierdzonej przez stosowną władzę. Kryptografia jest wdrażana zgodnie z obowiązującymi przepisami prawa, rozporządzeniami wykonawczymi, dyrektywami, regulacjami, zasadami, standardami i wytycznymi.

Zabezpieczenia powiązane: AC-2, AC-3, AC-7, AC-17, AC-18, AC-19, AU-9, AU-10, CM-11, CP-9, IA-3, IA-5, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SA-8, SA-9, SC-8, SC-12, SC-20, SC-23, SC-28, SC-40, SI-3, SI- 7.

Zabezpieczenia rozszerzone: Brak.

(1) OCHRONA KRYPTOGRAFICZNA | KRYPTOGRAFIA KOMERCYJNA

[Wycofane: Włączone do SC-13].

(2) OCHRONA KRYPTOGRAFICZNA | KRYPTOGRAFIA ZATWIERDZONA PRZEZ KRAJOWĄ WŁADZĘ BEZPIECZEŃSTWA

[Wycofane: Włączone do SC-13].

(3) OCHRONA KRYPTOGRAFICZNA | OSOBY BEZ FORMALNYCH ZATWIERDZEŃ DOSTĘPU

[Wycofane: Włączone do SC-13].

(4) OCHRONA KRYPTOGRAFICZNA | PODPISY CYFROWE

[Wycofane: Włączone do SC-13].

Referencje: [FIPS 140-3].

SC-14 OCHRONA DOSTĘPU PUBLICZNEGO

[Wycofane: Włączone do AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7 i SI-10].

SC-15 WSPÓŁPRACUJĄCE URZĄDZENIA I APLIKACJE

Zabezpieczenie podstawowe:

a. Zakazanie zdalnej aktywacji urządzeń i aplikacji do pracy zespołowej z następującymi wyjątkami: [*Realizacja: wyjątki zdefiniowane przez organizację, gdzie zdalna aktywacja jest dozwolona*]; oraz

b. Zapewnienie użytkownikom fizycznie pracującym na urządzeniach jednoznacznej informacji o sposobie korzystania z nich.

Omówienie: Współpracujące urządzenia i aplikacje przetwarzające dane obejmują zdalne urządzenia i aplikacje do spotkań, tablice sieciowe, kamery i mikrofony.

W przypadku ich aktywowania do użytkowników kierowane są jednoznaczne sygnały informujące o sposobie korzystania z nich.

Zabezpieczenia powiązane: AC-21, SC-42.

Zabezpieczenia rozszerzone:

(1) WSPÓŁPRACUJĄCE URZĄDZENIA I APLIKACJE | ODŁĄCZENIE FIZYCZNE LUB LOGICZNE

Zapewnienie [***Wybór (jeden lub więcej): fizyczne; logiczne***] **rozłączenie współpracujących urządzeń przetwarzających w sposób ułatwiający obsługę.**

Omówienie: Nieodłączenie się od współpracujących urządzeń przetwarzających może w następstwie spowodować kompromitację informacji organizacyjnych. Zapewnienie prostych metod odłączania się od takich urządzeń po zakończeniu sesji gwarantuje, że uczestnicy wykonają czynność odłączenia się bez konieczności przechodzenia przez skomplikowane i żmudne procedury. Odłączanie od współpracujących urządzeń przetwarzających może odbywać się w sposób ręczny lub automatyczny.

Zabezpieczenia powiązane: Brak.

(2) WSPÓŁPRACUJĄCE URZĄDZENIA I APLIKACJE | BLOKOWANIE RUCHU WEJŚCIOWEGO / WYJŚCIOWEGO

[Wycofane: Włączone do SC-7].

(3) WSPÓŁPRACUJĄCE URZĄDZENIA I APLIKACJE | DEZAKTYWACJA / USUWANIE W CHRONIONYCH OBSZARACH PRACY

Wyłączanie lub usuwanie współpracujących urządzeń i aplikacji z [*Realizacja: systemy lub komponenty systemowe zdefiniowane przez organizację*] w [*Realizacja: chronione obszary pracy zdefiniowane przez organizację*].

Omówienie: Niewyłączenie lub nieusunięcie współpracujących urządzeń i aplikacji z systemów lub komponentów systemu może prowadzić do utraty informacji, w tym podsłuchu rozmów. Przykładem bezpiecznego obszaru pracy jest zamknięty obszar używany do przetwarzania nadzorowanych/niejawnych informacji (*ang. Sensitive Compartmented Information Facility - SCIF*).

Zabezpieczenia powiązane: Brak.

(4) WSPÓŁPRACUJĄCE URZĄDZENIA I APLIKACJE | WYRAŹNIE WYKAZANIE AKTUALNYCH UŻYTKOWNIKÓW

Jednoznaczne wskazanie aktualnych uczestników [***Realizacja: zdefiniowane przez organizację spotkania online i telekonferencje***]**.**

Omówienie: Wyraźne wskazanie obecnych uczestników uniemożliwia osobom nieupoważnionym udział we wspólnych sesjach bez wyraźnej wiedzy innych uczestników.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

SC-16 TRANSMISJA ATRYBUTÓW BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Zabezpieczenie podstawowe: Powiązanie [*Realizacja: atrybuty bezpieczeństwa i ochrony prywatności zdefiniowane przez organizację*] z informacjami wymienianymi pomiędzy systemami i pomiędzy komponentami systemu.

Omówienie: Atrybuty bezpieczeństwa i ochrony prywatności mogą być w sposób wyraźny lub domniemany powiązane z informacjami zawartymi w systemach organizacyjnych lub komponentach systemu. Atrybuty są abstrakcjami, które reprezentują podstawowe właściwości lub cechy danego podmiotu w odniesieniu do ochrony informacji lub zarządzania informacjami umożliwiającymi identyfikację osób. Atrybuty są zazwyczaj związane z wewnętrznymi strukturami danych, w tym zapisami, buforami i plikami w systemie. Atrybuty bezpieczeństwa i ochrony prywatności są wykorzystywane do wdrażania zasady kontroli dostępu i kontroli przepływu informacji; odzwierciedlają specjalne instrukcje dotyczące rozpowszechniania, zarządzania lub dystrybucji, w tym dozwolone wykorzystanie informacji umożliwiających identyfikację osób; lub wspierają inne aspekty polityki bezpieczeństwa i ochrony prywatności informacji. Atrybuty ochrony prywatności mogą być wykorzystywane niezależnie lub w połączeniu z atrybutami bezpieczeństwa.

Zabezpieczenia powiązane: AC-3, AC-4, AC-16.

Zabezpieczenia rozszerzone:

(1) TRANSMISJA ATRYBUTÓW BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | WERYFIKACJA INTEGRALNOŚCI

Weryfikowanie integralności przesyłanych atrybutów bezpieczeństwa i ochrony prywatności.

Omówienie: Częścią weryfikacji integralności przesyłanych informacji jest upewnienie się, że atrybuty bezpieczeństwa i ochrony prywatności, które są związane z takimi informacjami, nie zostały zmienione w sposób nieupoważniony.

Nieautoryzowane modyfikacje atrybutów bezpieczeństwa i ochrony prywatności mogą spowodować utratę integralności przesyłanych informacji.

Zabezpieczenia powiązane: AU-10, SC-8.

(2) TRANSMISJA ATRYBUTÓW BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | MECHANIZMY ANTYSPOOFINGOWE

Wdrożenie mechanizmów antyspoofingowych w celu uniemożliwienia przeciwnikom sfałszowania atrybutów bezpieczeństwa wskazujących na pomyślne zastosowanie procesu bezpieczeństwa..

Omówienie: Niektóre wektory ataków wykorzystują zmianę atrybutów bezpieczeństwa systemu informatycznego w celu celowego i złośliwego wprowadzenia niewystarczającego poziomu bezpieczeństwa w systemie. Zmiana atrybutów prowadzi organizacje do przekonania, że została wdrożona i funkcjonuje znacznie większa liczba funkcji bezpieczeństwa niż w rzeczywistości.

Zabezpieczenia powiązane: SI-3, SI-4, SI-7.

(3) TRANSMISJA ATRYBUTÓW BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | POWIĄZANIE KRYPTOGRAFICZNE

Wdrożenie [***Realizacja: mechanizmy lub techniki zdefiniowane przez organizację***] ***w*** **celu powiązania atrybutów bezpieczeństwa i ochrony prywatności z przesyłanymi informacjami.**

Omówienie: Mechanizmy i techniki kryptograficzne mogą zapewnić silny atrybut bezpieczeństwa i ochrony prywatności wiążący się z przesyłanymi informacjami, co pomoże zapewnić ich integralność.

Zabezpieczenia powiązane: AC-16, SC-12, SC-13.

Referencje: [OMB A-130].

SC-17 CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO

Zabezpieczenie podstawowe:

a. Wydawanie certyfikatów klucza publicznego w ramach [*Realizacja: polityka certyfikacji określona przez organizację*] lub uzyskiwanie certyfikatów klucza publicznego od zatwierdzonego dostawcy usług; oraz

b. Uwzględnianie tylko zatwierdzonych kotwic zaufania do zaufanych sklepów lub magazynów certyfikatów zarządzanych przez organizację.

Omówienie: Certyfikaty infrastruktury klucza publicznego to certyfikaty z widocznością zewnętrzną w stosunku do systemów organizacyjnych oraz certyfikaty związane z wewnętrznymi operacjami systemów, np. specyficznymi dla aplikacji usługami czasowymi. W systemach kryptograficznych o strukturze hierarchicznej kotwica zaufania jest miarodajnym źródłem (np. organem wydającym certyfikaty), dla którego zakłada się zaufanie, a nie je uzyskuje. Przykładem kotwicy zaufania jest certyfikat główny dla systemu infrastruktury klucza publicznego (*ang. Public key infrastructure – PKI*). Podmiot świadczący usługi zaufania lub przechowujący certyfikaty prowadzi listę zaufanych certyfikatów głównych.

Zabezpieczenia powiązane: AU-10, IA-5, SC-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [NIST SP 800-32], [NIST SP 800-57-1], [NIST SP 800-57-2], [NIST SP 800-57-3], [NIST SP 800-63-3].

SC-18 KOD MOBILNY

Zabezpieczenie podstawowe:

a. Określanie akceptowalnych i nieakceptowalnych kodów mobilnych i technologii kodów mobilnych; oraz

b. Autoryzowanie, monitorowanie i zabezpieczanie wykorzystania kodu mobilnego w systemie.

Omówienie: Kod mobilny zawiera dowolny program, aplikację lub treść, która może być przesyłana przez sieć (np. wbudowana w email, dokument lub stronę internetową) i wykonywana na zdalnym systemie. Decyzje dotyczące korzystania z kodu mobilnego w ramach systemów organizacyjnych opierają się na możliwości spowodowania przez kod uszkodzenia systemów w przypadku jego złośliwego użycia. Technologie kodu mobilnego obejmują aplety Java, JavaScript, HTML5, WebGL i VBScript. Ograniczenia w użytkowaniu i wytyczne wdrożeniowe dotyczą zarówno wyboru i wykorzystania kodu mobilnego zainstalowanego na serwerach, jak i kodu mobilnego pobranego i wykonywanego na poszczególnych stacjach roboczych i urządzeniach, w tym na notebookach i smartfonach. Polityka i procedury dotyczące kodu mobilnego odnoszą się do konkretnych działań podejmowanych w celu zapobiegania tworzeniu, pozyskiwaniu i wprowadzaniu niedopuszczalnego kodu mobilnego do systemów organizacyjnych, w tym wymagających podpisywania cyfrowego kodu mobilnego przez zaufane źródło.

Zabezpieczenia powiązane: AU-2, AU-12, CM-2, CM-6, SI-3.

Zabezpieczenia rozszerzone:

(1) KOD MOBILNY | IDENTYFIKACJA NIEDOPUSZCZALNEGO KODU / PODEJMOWANIE DZIAŁAŃ NAPRAWCZYCH

Identyfikowanie [*Realizacja: zdefiniowany przez organizację niedopuszczalny kod mobilny*] i podjęcie [*Realizacja: zdefiniowane przez organizację działania naprawcze*].

Omówienie: Działania naprawcze w przypadku wykrycia niedopuszczalnego kodu komórkowego obejmują blokowanie, kwarantannę lub ostrzeganie administratorów. Blokowanie obejmuje zapobieganie przesyłaniu plików edytorów tekstu z wbudowanymi makrami, jeżeli takie makra zostaną uznane za niedopuszczalny kod mobilny.

Zabezpieczenia powiązane: Brak.

(2) KOD MOBILNY | NABYCIE / OPRACOWYWANIE / UŻYTKOWANIE

Sprawdzanie, czy nabywany, opracowywany i wykorzystywany kod mobilny, który ma zostać wdrożony w systemie, spełnia [***Realizacja: wymagania dotyczące kodu mobilnego zdefiniowane przez organizację***]**.**

Omówienie: Brak.

Zabezpieczenia powiązane: Brak.

(3) KOD MOBILNY | ZAPOBIEGANIE POBIERANIU I WYKONYWANIU

Zapobieganie pobieraniu i wykonywaniu [***Realizacja: zdefiniowany przez organizację niedopuszczalny kod mobilny***]**.**

Omówienie: Brak.

Zabezpieczenia powiązane: Brak.

(4) KOD MOBILNY | ZAPOBIEGANIE AUTOMATYCZNEMU WYKONANIU

Zapobieganie automatycznemu wykonywaniu kodu mobilnego w [***Realizacja: aplikacje zdefiniowane przez organizację***] **i egzekwowanie** [***Realizacja: działania zdefiniowane przez organizację***] **przed wykonaniem kodu.**

Omówienie: Działania wymuszone przed wykonaniem kodu mobilnego obejmują wyświetlanie użytkownikom monitów przed otwarciem załączników e-mail lub kliknięciem linków internetowych. Zapobieganie automatycznemu wykonaniu kodu mobilnego obejmuje wyłączenie funkcji automatycznego wykonywania operacji na komponentach systemu, które wykorzystują przenośne urządzenia

pamięci masowej, takie jak dyski kompaktowe, uniwersalne dyski cyfrowe i uniwersalne urządzenia magistrali szeregowej.

Zabezpieczenia powiązane: Brak.

(5) KOD MOBILNY | POZWALANIE NA WYKONANIE TYLKO W OGRANICZONYCH ŚRODOWISKACH

Zezwalanie na wykonywanie dozwolonego kodu mobilnego tylko w ograniczonych środowiskach maszyn wirtualnych.

Omówienie: Zezwolenie na wykonywanie kodu mobilnego tylko w zamkniętych środowiskach maszyn wirtualnych pomaga zapobiec wprowadzeniu złośliwego kodu do innych systemów i komponentów systemu.

Zabezpieczenia powiązane: SC-44, SI-7.

Referencje: [NIST SP 800-28].

SC-19 PROTOKÓŁ TRANSMISJI PAKIETOWEJ (VoIP)

[Wycofano: Specyficzne dla danej technologii; adresowane jak każda inna technologia lub protokół].

SC-20 BEZPIECZEŃSTWO NAZW DOMEN / ADRESÓW IP (AUTENTYCZNOŚĆ POCHODZENIA)

Zabezpieczenie podstawowe:

a. Dostarczanie dodatkowych artefaktów uwierzytelniania pochodzenia danych i weryfikacji integralności wraz z autorytatywnymi danymi dotyczącymi rozpoznawania nazwy, które system zwraca w odpowiedzi na zewnętrzne zapytania dotyczące rozpoznawnia nazwy/adresu; oraz

b. Zapewnienie środków do wskazywania statusu bezpieczeństwa stref podrzędnych i (jeśli ta podrzędna strefa zapewnia obsługę środków bezpiecze ństwa) w celu umożliwienia weryfikacji łańcucha zaufania między domenami nadrzędnymi i podrzędnymi, w przypadku gdy działają one w ramach rozproszonej, hierarchicznej przestrzeni nazw.

Omówienie: Dostarczanie informacji o autorytatywnym źródle umożliwia klientom zewnętrznym, w tym zdalnym użytkownikom Internetu, uzyskanie uwierzytelnienia pochodzenia i zapewnienia weryfikacji integralności nazwy hosta/usługi w odniesieniu do informacji umożliwiających rozpoznawanie adresów sieciowych uzyskanych za pośrednictwem usługi. Systemy, które zapewniają usługi rozpoznawania nazw i adresów, obejmują serwery systemu nazw domen (DNS). Dodatkowe artefakty obejmują podpisy cyfrowe i klucze kryptograficzne DNS Security Extensions (DNSSEC) rozszerzające system DNS w celu zwiększenie jego bezpieczeństwa. Dane autorytatywne obejmują rekordy zasobów DNS. Środki do wskazywania stanu bezpieczeństwa stref podrzędnych obejmują wykorzystanie zapisów zasobów podpisujących przekazania w DNS. Systemy, które wykorzystują technologie inne niż DNS do mapowania między nazwami hostów i usług, a adresami sieciowymi, dostarczają innych środków zapewniających autentyczność i integralność danych odpowiedzi.

Zabezpieczenia powiązane: AU-10, SC-8, SC-12, SC-13, SC-21, SC-22.

Zabezpieczenia rozszerzone:

(1) BEZPIECZEŃSTWO NAZW DOMEN / ADRESÓW IP (AUTENTYCZNOŚĆ POCHODZENIA)| STREFA PODRZĘDNA (PODPRZESTRZEŃ)

[Wycofane: Włączone do SC-20].

(2) BEZPIECZEŃSTWO NAZW DOMEN / ADRESÓW IP (AUTENTYCZNOŚĆ POCHODZENIA) | INTEGRALNOŚĆ DANYCH

Dostarczanie artefaktów dotyczących pochodzenia danych i ochrony integralności wewnętrznych zapytań dotyczących rozpoznawania nazwy/adresu.

Omówienie: Brak.

Zabezpieczenia powiązane: Brak.

Referencje: [FIPS 140-3], [FIPS 186-4], [SP 800-81-2].

SC-21 BEZPIECZEŃSTWO NAZW DOMEN / USŁUGA USTALANIA ADRESU IP

Zabezpieczenie podstawowe: Żądanie i przeprowadzanie weryfikacji autentyczności pochodzenia danych i integralności danych na podstawie odpowiedzi dotyczących rozpoznawalności nazwy/adresu, które system otrzymuje z wiarygodnych źródeł.

Omówienie: Każdy klient usług rozpoznawania nazw albo wykonuje tę walidację samodzielnie, albo posiada uwierzytelnione kanały do zaufanych dostawców walidacji. Systemy, które dostarczają usługi rozpoznawania nazw i adresów lokalnych klientów zawierają rekurencyjnie rozwiązujące lub buforujące serwery systemu nazw domen (DNS). Klienckie systemy rozpoznawania nazw DNS albo wykonują walidację podpisów DNSSEC, albo korzystają z uwierzytelnionych kanałów do rekurencyjnych programów rozpoznawania, które wykonują taką walidację. Systemy, które wykorzystują technologie inne niż DNS do mapowania między nazwami hostów i usług, a adresami sieciowymi, zapewniają inne środki umożliwiające klientom weryfikację autentyczności i integralności danych zwrotnych.

Zabezpieczenia powiązane: SC-20, SC-22.

Zabezpieczenia rozszerzone: Brak.

1) BEZPIECZEŃSTWO NAZW DOMEN / USŁUGA USTALANIA ADRESU IP /ADRESÓW (REKURENCYJNA LUB BUFOROWA) | INTEGRALNOŚĆ

[Wycofane: Włączone do SC-21].

Referencje: [NIST SP 800-81-2].

SC-22 ARCHITEKTURA NAZW DOMEN / ADRESÓW IP / ZAMAWIANIE USŁUGI DNS

Zabezpieczenie podstawowe: Zapewnienie, że systemy, które wspólnie świadczą usługi rozwiązywania problemów dotyczących rozpoznawania nazw/adresów organizacji, są odporne na błędy i wdrażają wewnętrzny i zewnętrzny rozdział ról.

Omówienie: Systemy świadczące usługi rozpoznawania nazw i adresów obejmują serwery systemu nazw domenowych (DNS). Aby wyeliminować pojedyncze punkty awarii w systemach i zwiększyć redundancję, organizacje wykorzystują co najmniej dwa autorytatywne serwery systemu nazw domenowych - jeden skonfigurowany jako serwer główny i drugi jako serwer dodatkowy. Dodatkowo, organizacje zazwyczaj wdrażają serwery w dwóch geograficznie oddzielonych podsieciach (tj. nie znajdujących się w tym samym obiekcie fizycznym). W przypadku separacji ról, serwery DNS z rolami wewnętrznymi przetwarzają tylko żądania rozpoznawania nazw i adresów z wewnątrz organizacji (tj. od klientów wewnętrznych). Serwery DNS z rolami zewnętrznymi przetwarzają tylko żądania rozpoznawania nazw i adresów od klientów zewnętrznych w stosunku do organizacji (tj. w sieciach zewnętrznych, w tym w Internecie). Organizacje określają kto może mieć dostęp do autorytatywnych serwerów DNS w określonych rolach (np. według zakresów adresów i przejrzystych list).

Zabezpieczenia powiązane: SC-2, SC-20, SC-21, SC-24.

Zabezpieczenia rozszerzone: Brak.

Referencje: [NIST SP 800-81-2].

SC-23 AUTENTYCZNOŚĆ SESJI

Zabezpieczenie podstawowe: Zapewnienie autentyczność sesji komunikacyjnych.

Omówienie: Zapewnienie autentyczności sesji odnosi się do ochrony komunikacji na poziomie sesji, a nie na poziomie pakietów. Taka ochrona stanowi podstawę zaufania po obu stronach sesji komunikacyjnych do aktualnej tożsamości innych stron oraz do ważności przekazywanych informacji. Ochrona autentyczności obejmuje ochronę przed atakami typu "man-in-the-middle", przejęciem sesji oraz wprowadzaniem fałszywych informacji do sesji.

Zabezpieczenia powiązane: AU-10, SC-8, SC-10, SC-11.

Zabezpieczenia rozszerzone:

(1) AUTENTYCZNOŚĆ SESJI | UNIEWAŻNIENIE IDENTYFIKATORÓW SESJI PO WYLOGOWANIU

Unieważnienie identyfikatorów sesji po wylogowaniu się użytkownika lub innym zakończeniu sesji.

Omówienie: Unieważnienie identyfikatorów sesji po wylogowaniu ogranicza zdolność przeciwników do przechwytywania i dalszego wykorzystywania poprzednio obowiązujących identyfikatorów sesji.

Zabezpieczenia powiązane: Brak.

(2) AUTENTYCZNOŚĆ SESJI | WYLOGOWANIE INICJOWANE PRZEZ UŻYTKOWNIKA / WYŚWIETLANIE WIADOMOŚCI

[Wycofane: Włączone do AC-12(1)].

(3) AUTENTYCZNOŚĆ SESJI | UNIKATOWE IDENTYFIKATORY SESJI GENEROWANE PRZEZ SYSTEM

Generowanie unikatowych identyfikator sesji dla każdej sesji z [*Realizacja: zdefiniowane przez organizację wymagania dotyczące losowości*]

i rozpoznawanie tylko tych identyfikatorów sesji, które są generowane przez system.

Omówienie: Generowanie unikalnych identyfikatorów sesji ogranicza możliwość ponownego wykorzystania przez przeciwników wcześniej obowiązujących identyfikatorów sesji. Wykorzystanie koncepcji losowości w generowaniu unikalnych identyfikatorów sesji chroni przed atakami typu "brute-force" zmierzającymi do określenia przyszłych identyfikatorów sesji.

Zabezpieczenia powiązane: AC-10, SC-12, SC-13.

(4) AUTENTYCZNOŚĆ SESJI | LOSOWE UNIKALNE IDENTYFIKATORY SESJI

[Wycofane: Włączone do SC-23(3)].

(5) AUTENTYCZNOŚĆ SESJI | AUTORYZOWANE URZĘDY CERTYFIKACYJNE

Zezwolenie na korzystanie jedynie z [***Realizacja: organy certyfikacyjne określone przez organizację***] **do weryfikacji ustanowienia chronionych sesji.**

Omówienie: Poleganie na organach wydających certyfikaty w celu ustanowienia bezpiecznych sesji obejmuje stosowanie certyfikatów bezpieczeństwa warstw transportowych (*ang. Transport Layer Security - TLS*). Certyfikaty te, po weryfikacji przez odpowiednie organy certyfikacyjne, ułatwiają zestawianie chronionych sesji pomiędzy klientami internetowymi, a serwerami internetowymi.

Zabezpieczenia powiązane: SC-12, SC-13.

Referencje: [NIST SP 800-52], [NIST SP 800-77], [NIST SP 800-95], [NIST SP 800-113].

SC-24 PRZEJŚCIE DO OKREŚLONEGO STANU SYSTEMU PO BŁĘDZIE

Zabezpieczenie podstawowe: Przejście do stanu bezpiecznego (po błędzie) [*Realizacja: znany stan zdefiniowany przez organizację*] w odniesieniu do [*Realizacja: typy błędów zdefiniowane przez organizację*] zachowując [*Realizacja: informacje o stanie systemu zdefiniowane przez organizację*] w przypadku niepowodzenia.

Omówienie: Przejście do stanu bezpiecznego (po błędzie) odnosi się do kwestii bezpieczeństwa wynikających z misji i potrzeb biznesowych organizacji. Zapobiega utracie poufności, integralności lub dostępności informacji w przypadku awarii systemów organizacyjnych lub komponentów systemu. Pomaga zapobiegać awariom systemów, które mogą spowodować obrażenia u osób lub zniszczenie mienia. Zachowanie informacji o stanie systemu ułatwia jego ponowne uruchomienie i powrót do trybu operacyjnego przy mniejszym zakłóceniu misji i procesów biznesowych.

Zabezpieczenia powiązane: CP-2, CP-4, CP-10, CP-12, SA-8, SC-7, SC-22, SI-13.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

SC-25 THIN NODES / TERMINALOWE STACJE ROBOCZE

Zabezpieczenie podstawowe: Stosowanie [*Realizacja: zdefiniowane przez organizację komponenty systemu*] *o* zminimalizowanej funkcjonalności i pojemności.

Omówienie: Wdrożenie komponentów systemu o minimalnej funkcjonalności zmniejsza potrzebę zabezpieczenia każdego punktu końcowego i może zmniejszyć narażenie informacji, systemów i usług na ataki. Ograniczona lub minimalna funkcjonalność obejmuje terminale bezdyskowe i technologie „cienkich klientów" (*ang. thin nodes*).

Zabezpieczenia powiązane: SC-30, SC-44.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

SC-26 WABIKI

Zabezpieczenie podstawowe: Włączenie do systemów organizacyjnych komponentów zaprojektowanych specjalnie jako cel złośliwych ataków, służących do wykrywania, odpierania i analizowania takich ataków.

Omówienie: Wabiki, tj. „honeypot", „honeynet" lub sieci oszukańcze (*ang. deception nets*) są tworzone w celu przyciągnięcia przeciwników i odwrócenia ataków od systemów operacyjnych, które wspierają misję organizacyjną i funkcje biznesowe. Użycie wabików wymaga zastosowania pewnych wspierających środków izolacyjnych, aby upewnić się, że każdy odbity złośliwy kod nie zainfekuje systemów organizacyjnych. W zależności od konkretnego zastosowania wabika, przed wdrożeniem może być konieczna konsultacja z odpowiednim organem zajmującym się cyberbezpieczeństwem.

Zabezpieczenia powiązane: RA-5, SC-7, SC-30, SC-35, SC-44, SI-3, SI-4.

Zabezpieczenia rozszerzone: Brak.

(1) WABIKI | WYKRYWANIE KODU ZŁOŚLIWEGO

[Wycofane: Włączone do SC-35].

Referencje: Brak.

SC-27 WIELOPLATFORMOWOŚĆ APLIKACJI

Zabezpieczenie podstawowe: Włączenie do systemów organizacyjnych następujących aplikacji niezależnych od platformy: [*Realizacja: zdefiniowane przez organizację aplikacje niezależne od platformy*].

Omówienie: Platformy są kombinacją sprzętu, firmware'u i komponentów oprogramowania używanych do wykonywania aplikacji. Platformy obejmują systemy operacyjne, podstawowe architektury komputerowe lub oba te elementy. Aplikacje niezależne od platformy to aplikacje, które mogą być uruchamiane na wielu platformach. Tego typu aplikacje wspierają możliwość przenoszenia i odtwarzania na różnych platformach. Przenośność aplikacji i zdolność do odtworzenia na różnych platformach zwiększa dostępność funkcji istotnych dla misji organizacji w sytuacjach, gdy atakowane są systemy ze specyficznymi systemami operacyjnymi.

Zabezpieczenia powiązane: SC-29.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

SC-28 OCHRONA DANYCH W SKŁADOWANIU / KOPIE KONFIGURACJI SYSTEMU

Zabezpieczenie podstawowe: Chronienie [*Wybór (jeden lub więcej): poufność; integralność*] następujących informacji w stanie spoczynku (w składowaniu): [*Realizacja: informacje określone przez organizację w stanie spoczynku (w składowaniu)*].

Omówienie: Informacje w stanie spoczynku to informacje zlokalizowane na komponentach systemu, które nie są przetwarzane, ani przesyłane. Do takich komponentów należą wewnętrzne lub zewnętrzne dyski twarde, sieciowe urządzenia magazynujące lub bazy danych. Ochrona informacji w stanie spoczynku nie koncentruje się jednak na rodzaju urządzenia pamięci masowej lub częstotliwości korzystania z tego urządzenia, ale na samym stanie informacji. Informacje w stanie spoczynku uwzględniają poufność oraz integralność informacji i są związane z informacjami o użytkownikach oraz informacjami systemowymi. Informacje związane z systemem, które wymagają ochrony, obejmują konfiguracje lub zestawy reguł dla zapór ogniowych, systemów wykrywania i zapobiegania włamaniom, routerów filtrujących oraz informacje uwierzytelniające. Organizacje mogą stosować różne mechanizmy w celu osiągnięcia ochrony poufności i integralności, w tym wykorzystanie mechanizmów kryptograficznych i skanowanie udostępnianych plików. Ochrona integralności może być osiągnięta na przykład poprzez wdrożenie technologii przechowywania danych "zapisz raz - czytaj wiele razy" (ang. write-once-read-many - WORM). W przypadku braku możliwości zapewnienia odpowiedniej ochrony informacji w stanie spoczynku, organizacje mogą stosować inne środki bezpieczeństwa, w tym częste skanowanie w celu identyfikacji złośliwego kodu w stanie spoczynku oraz bezpieczne przechowywanie w trybie offline zamiast przechowywania w trybie online.

Zabezpieczenia powiązane: AC-3, AC-4, AC-6, AC-19, CA-7, CM-3, CM-5, CM-6, CP-9, MP-4, MP-5, PE-3, SC- 8, SC-12, SC-13, SC-34, SI-3, SI-7, SI-16.

Zabezpieczenia rozszerzone:

(1) OCHRONA DANYCH W SKŁADOWANIU / KOPIE KONFIGURACJI SYSTEMU | OCHRONA KRYPTOGRAFICZNA

Wdrożenie mechanizmów kryptograficznych zapobiegających nieautoryzowanemu ujawnieniu i modyfikacji następujących informacji w spoczynku na [***Realizacja: zdefiniowanych przez organizację składników systemu lub nośników***]***:*** [***Realizacja: informacja zdefiniowana przez organizację***]***:*** [***Realizacja: informacja zdefiniowana przez organizację***]**.**

Omówienie: Wybór mechanizmów kryptograficznych opiera się na potrzebie ochrony poufności i integralności informacji organizacyjnych. Siła mechanizmu jest współmierna do kategorii bezpieczeństwa lub klasyfikacji informacji. Organizacje mają możliwość elastycznego szyfrowania informacji na komponentach systemu lub nośnikach lub szyfrowania struktur danych, w tym plików, zapisów lub pól.

Zabezpieczenia powiązane: AC-19, SC-12, SC-13.

(2) OCHRONA DANYCH W SKŁADOWANIU / KOPIE KONFIGURACJI SYSTEMU | PRZECHOWYWANIE W TRYBIE OFF-LINE

Usuwanie z pamięci online i przechowywanie w bezpiecznym miejscu trybie w offline poniższych informacji : [Realizacja: ***informacje określone przez organizację*****].**

Omówienie: Usuwanie informacji organizacyjnych z pamięci online do pamięci offline eliminuje możliwość uzyskania nieupoważnionego dostępu do informacji za pośrednictwem sieci. Dlatego też organizacje mogą zdecydować się na przeniesienie informacji do pamięci w trybie offline zamiast chronić takie informacje w pamięci w trybie online.

Zabezpieczenia powiązane: Brak.

(3) OCHRONA DANYCH W SKŁADOWANIU / KOPIE KONFIGURACJI SYSTEMU | KLUCZE KRYPTOGRAFICZNE

Udostępnianie chronionej pamięci do przechowywania kluczy kryptograficznych [***Wybór:*** [***Realizacja: zabezpieczenia zdefiniowane przez organizację***]***; chroniony sprzętowo magazyn kluczy kryptograficznych***]**.**

Omówienie: Standard układu scalonego TPM (Trusted Platform Module) jest przykładem sprzętowo zabezpieczonego magazynu danych, który może być wykorzystywany do ochrony kluczy kryptograficznych.

Zabezpieczenia powiązane: SC-12, SC-13.

Referencje: [OMB A-130], [NIST SP 800-56A], [NIST SP 800-56B], [NIST SP 800-56C], [NIST SP 800-57-1], [NIST SP 800-57- 2], [NIST SP 800-57-3], [NIST SP 800-111], [NIST SP 800-124].

SC-29 HETEROGENICZNOŚĆ SYSTEMU

Zabezpieczenie podstawowe: Zastosowanie zróżnicowanego zestawu technologii informatycznych do wdrażania następujących komponentów systemu: [*Realizacja: zdefiniowane przez organizację komponenty systemu*].

Omówienie: Zwiększenie różnorodności technologii informatycznych w systemach organizacyjnych zmniejsza wpływ potencjalnych przypadków niewłaściwego wykorzystania lub kompromitowania określonych technologii. Taka różnorodność chroni przed powszechnymi awariami, w tym awariami spowodowanymi atakami w łańcuchu dostaw. Różnorodność technologii informatycznych zmniejsza również prawdopodobieństwo, że środki użyte przez przeciwników do skompromitowania jednego komponentu systemu będą skuteczne wobec innych komponentów systemu, co jeszcze bardziej zwiększa współczynnik nakładu pracy przeciwnika w celu pomyślnego przeprowadzenia zaplanowanych ataków. Wzrost różnorodności może zwiększyć złożoność i koszty ogólne zarządzania, co ostatecznie może prowadzić do błędów i nieuprawnionych konfiguracji.

Zabezpieczenia powiązane: AU-9, PL-8, SC-27, SC-30, SR-3.

Zabezpieczenia rozszerzone:

(1) HETEROGENICZNOŚĆ | TECHNIK WIRTUALIZACJI

Zastosowanie technik wirtualizacji w celu wsparcia wdrażania różnych systemów operacyjnych i aplikacji, które są zmieniane z częstotliwością [***Realizacja: częstotliwość zdefiniowana przez organizację***]**.**

Omówienie: Częste zmiany w systemach operacyjnych i aplikacjach mogą stanowić istotne wyzwanie w zarządzaniu konfiguracją, jednak zmiany te mogą skutkować zwiększonym współczynnikiem nakładu pracy przeciwników w celu przeprowadzenia udanych ataków. Zmiana wirtualnych systemów operacyjnych lub aplikacji, w przeciwieństwie do zmiany rzeczywistych systemów operacyjnych lub aplikacji, zapewnia wirtualne zmiany, które utrudniają powodzenie ataku przy

jednoczesnym zmniejszeniu wysiłków związanych z zarządzaniem konfiguracją. Techniki wirtualizacji mogą pomóc w izolowaniu niezaufanego oprogramowania lub oprogramowania o wątpliwym pochodzeniu w ograniczonych środowiskach wykonawczych.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

SC-30 MASKOWANIE I DEZINFORMACJA

Zabezpieczenie podstawowe: Stosowanie następujących technik maskowania i dezinformacji [*Realizacja: systemy określone przez organizację*] w [*Realizacja: okresy czasu określone przez organizację*] *w* celu dezorientowania i wprowadzania w błąd przeciwników: [*Realizacja: zdefiniowane przez organizację techniki maskowania i dezinformacji*].

Omówienie: Techniki maskowania i dezinformacji mogą znacząco zmniejszyć możliwości przeciwników w zakresie ukierunkowania (tj. możliwości i dostępnej powierzchni ataku) w celu inicjowania i przeprowadzania ataków. Na przykład, techniki wirtualizacji zapewniają organizacjom możliwość ukrycia systemów, potencjalnie zmniejszając prawdopodobieństwo udanych ataków bez ponoszenia kosztów posiadania wielu platform. Zwiększone wykorzystanie technik i metod maskowania i dezinformacji - w tym losowości, nieprzewidywalności i wirtualizacji - może w wystarczającym stopniu zdezorientować i wprowadzić w błąd przeciwników, a następnie zwiększyć ryzyko wykrycia i/lub ujawnienia nielegalnych działań. Techniki maskowania i dezinformacji mogą zapewnić dodatkowy czas na wykonywanie podstawowych funkcji misji i działalności. Wdrożenie technik maskowania i dezinformacji może zwiększyć złożoność systemu i koszty ogólne zarządzania nim.

Zabezpieczenia powiązane: AC-6, SC-25, SC-26, SC-29, SC-44, SI-14.

Zabezpieczenia rozszerzone:

(1) MASKOWANIE I DEZINFORMACJA | TECHNIKI WIRTUALIZACJI

[Wycofane: Włączone do SC-29(1)].

(2) MASKOWANIE I DEZINFORMACJA | LOSOWOŚĆ

Wykorzystywanie [***Realizacja: zdefiniowane przez organizację losowe techniki wprowadzające w błąd***] ***w*** **celu wprowadzenia losowości w operacjach i zasobach organizacyjnych.**

Omówienie: Losowość wprowadza zwiększony poziom niepewności dla przeciwników w odniesieniu do działań, które organizacje podejmują w celu obrony swoich systemów przed atakami. Takie działania mogą utrudnić zdolność przeciwników do właściwego namierzania zasobów informacyjnych organizacji, które wspierają krytyczne misje lub funkcje biznesowe. Niepewność może również spowodować, że przeciwnicy będą się wahać przed rozpoczęciem lub kontynuowaniem ataków. Techniki odwracania uwagi, które wykorzystują losowość, obejmują wykonywanie pewnych rutynowych czynności o różnych porach dnia, stosowanie różnych technologii informatycznych, korzystanie z różnych dostawców oraz rotację ról i obowiązków personelu organizacyjnego.

Zabezpieczenia powiązane: Brak.

(3) MASKOWANIE I DEZINFORMACJA | ZMIANA LOKALIZACJI PRZETWARZANIA / PRZECHOWYWANIA

Zmiana lokalizacji [***Realizacja: zdefiniowane przez organizację przetwarzanie i/lub przechowywanie***] **z częstotliwością** [***Wybór:*** [***Realizacja: częstotliwość zdefiniowana przez organizację; w przypadkowych odstępach czasu***]]]**.**

Omówienie: Przeciwnicy atakują krytyczne funkcje misji i biznesu oraz systemy, które wspierają te funkcje, starając się jednocześnie zminimalizować ujawnienie swojego istnienia i umiejętności. Statyczna, jednorodna i deterministyczna natura systemów organizacyjnych, które są celem ataków, sprawia, że są one bardziej podatne na ataki przy mniejszych kosztach i wysiłkach podejmowanych przez przeciwnika, które mogą zakończyć się sukcesem. Zmiana lokalizacji przetwarzania i przechowywania danych, określana również jako obrona wykorzystująca metodę ruchomego/zmiennego celu (ang. moving target defense - MTD), jest odpowiedzią na zaawansowane trwałe zagrożenie, wykorzystującą techniki takie jak wirtualizacja, przetwarzanie rozproszone i replikacja. Umożliwia to organizacjom zmianę lokalizacji komponentów systemu (tj. przetwarzania, przechowywania), które wspierają krytyczne funkcje misji i biznesu. Zmiana

lokalizacji działań związanych z przetwarzaniem i/lub miejsc składowania wprowadza pewien stopień niepewności do ukierunkowanych działań przeciwników. Niepewność celu zwiększa czynnik pracy przeciwników i sprawia, że kompromitacja lub naruszenie systemów organizacyjnych jest trudniejsze i bardziej czasochłonne. Zwiększa to również prawdopodobieństwo, że przeciwnicy mogą nieumyślnie ujawnić pewne aspekty swojej wiedzy technicznej podczas próby zlokalizowania krytycznych zasobów organizacyjnych.

Zabezpieczenia powiązane: Brak.

(4) MASKOWANIE I DEZINFORMACJA | INFORMACJE DEZINFORMUJĄCE

Stosowanie realistycznych, lecz wprowadzających w błąd informacji o statusie lub stanie bezpieczeństwa w [***Realizacja: komponenty systemu zdefiniowane przez organizację***]**.**

Omówienie: Stosowanie informacji wprowadzających w błąd ma na celu dezorientację potencjalnych przeciwników co do charakteru i zakresu zabezpieczeń stosowanych przez organizacje. Adwersarze mogą zatem stosować niewłaściwe i nieskuteczne techniki ataku. Jedną z technik wprowadzania w błąd adwersarzy jest umieszczanie przez organizacje wprowadzających w błąd informacji dotyczących poszczególnych środków bezpieczeństwa stosowanych w zewnętrznych systemach, o których wiadomo, że są celem ataków. Inną techniką jest stosowanie sieci wprowadzających w błąd, które naśladują rzeczywiste aspekty systemów organizacyjnych, ale wykorzystują na przykład przestarzałe konfiguracje oprogramowania.

Zabezpieczenia powiązane: Brak.

(5) MASKOWANIE I DEZINFORMACJA | UKRYWANIE KOMPONENTÓW SYSTEMU

Stosowanie następujących technik ukrywania i maskowania [***Realizacja: komponenty systemu zdefiniowane przez organizację***]***:*** [***Realizacja: techniki zdefiniowane przez organizację***]**.**

Omówienie: Ukrywając, kamuflując lub ukrywając krytyczne komponenty systemu, organizacje mogą być w stanie zmniejszyć prawdopodobieństwo, że przeciwnicy namierzą i skutecznie skompromitują te zasoby. Potencjalne sposoby ukrywania, maskowania lub zakamuflowania komponentów systemu obejmują konfigurację routerów lub wykorzystanie technik szyfrowania lub wirtualizacji.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

SC-31 ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI

Zabezpieczenie podstawowe:

a. Przeprowadzanie analizy ukrytych kanałów w celu zidentyfikowania tych aspektów komunikacji w systemie, które są potencjalnymi trasami ukrytych kanałów [*Wybór (jeden lub więcej): przechowywanie; synchronizacja*]; oraz

b. Szacowanie maksymalnej przepustowości kanałów ukrytych.

Omówienie: Deweloperzy mają największe możliwości identyfikacji potencjalnych obszarów w systemach, które mogą prowadzić do powstawania ukrytych kanałów. Analiza ukrytych kanałów jest istotnym działaniem, szczególnie gdy istnieje możliwość nieautoryzowanego przepływu informacji pomiędzy domenami bezpieczeństwa, np. w przypadku systemów zawierających informacje nadzorowane pod kątem bezpieczeństwa transferu i posiadających połączenia z sieciami zewnętrznymi (tj. sieciami, które nie są kontrolowane przez organizacje). Analiza ukrytych kanałów jest również przydatna w przypadku wielopoziomowych systemów bezpieczeństwa, systemów o zróżnicowanych poziomach zabezpieczeń oraz systemów międzydomenowych.

Zabezpieczenia powiązane: AC-3, AC-4, SA-8, SI-11.

Zabezpieczenia rozszerzone:

(1) ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI | TESTOWANIE KANAŁÓW UKRYTYCH POD KĄTEM MOŻLIWOŚCI ICH WYKORZYSTANIA

Testowanie podzbioru zidentyfikowanych ukrytych kanałów możliwych do prowadzenia wyzyskiwania.

Omówienie: Brak.

Zabezpieczenia powiązane: Brak.

(2) ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI | MAKSYMALNA PRZEPUSTOWOŚĆ ŁĄCZA

Zmniejszenie maksymalnej szerokości pasma zidentyfikowanych ukrytych kanałów [***Wybór (jeden lub więcej): przechowywanie; synchronizacja***] **do** [***Realizacja: wartości przepustowości zdefiniowana przez organizację***]**.**

Omówienie: Całkowite wyeliminowanie ukrytych kanałów, zwłaszcza ukrytych kanałów synchronizacyjnych, nie jest zazwyczaj możliwe bez znaczącego wpływu na wydajność.

Zabezpieczenia powiązane: Brak.

(3) ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI | POMIAR PRZEPUSTOWOŚCI W ŚRODOWISKU OPERACYJNYM

Mierzenie przepustowości pasma [***Realizacja: zdefiniowany przez organizację podzbiór zidentyfikowanych ukrytych kanałów***] **w środowisku operacyjnym systemu.**

Omówienie: Pomiar przepustowości kanału ukrytego w określonych środowiskach operacyjnych pomaga organizacjom określić, ile informacji może zostać ukrytych, zanim taki wyciek negatywnie wpłynie na misję lub funkcje biznesowe. Szerokość pasma kanału ukrytego może być znacząco różna w przypadku pomiaru w ustawieniach niezależnych od konkretnych środowisk pracy, w tym laboratoriów lub środowisk rozwoju systemów.

Zabezpieczenia powiązane: Brak.

Referencje: Brak.

SC-32 DZIELENIE SYSTEMU NA PARTYCJE

Zabezpieczenie podstawowe: Podział systemu na [*Realizacja: zdefiniowane przez organizację komponenty systemu*] rezydujące w oddzielnych [*Wybór: fizyczne; logiczne*] domenach lub środowiskach opartych na [*Realizacja: zdefiniowane przez organizację okoliczności fizycznego lub logicznego rozdzielenia składników*].

Omówienie: Podział na systemy jest częścią strategii ochrony obronnej. Organizacje określają stopień fizycznej separacji elementów systemu. Opcje fizycznej separacji obejmują fizycznie odrębne komponenty w oddzielnych stojakach w tym samym pomieszczeniu, krytyczne komponenty w oddzielnych pomieszczeniach oraz geograficzną separację krytycznych komponentów. Kategoryzacja bezpieczeństwa może pomóc w wyborze składników do partycjonowania domeny. Zarządzane interfejsy ograniczają lub zabraniają dostępu do sieci i przepływu informacji pomiędzy partycjonowanymi komponentami systemu.

Zabezpieczenia powiązane: AC-4, AC-6, SA-8, SC-2, SC-3, SC-7, SC-36.

Zabezpieczenia rozszerzone:

(1) DZIELENIE SYSTEMU NA PARTYCJE | FIZYCZNIE WYDZIELONE DOMENY DLA FUNKCJI UPRZYWILEJOWANYCH

Dzielenie uprzywilejowanych funkcji na odrębne fizyczne domeny.

Omówienie: Uprzywilejowane funkcje, które działają w pojedynczej domenie fizycznej, mogą stanowić pojedynczy punkt awarii, jeśli domena ta zostanie naruszona lub nastąpi odmowa świadczenia usług.

Zabezpieczenia powiązane: Brak.

Referencje: [FIPS 199], [IR 8179].

SC-33 INTEGRALNOŚĆ TRANSMISJI

[Wycofane: Włączone do SC-8].

SC-34 NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE

Zabezpieczenie podstawowe: Załadowanie i wykonanie w [*Realizacja: zdefiniowane przez organizację komponenty systemu*]:

a. Środowiska pracy z nośników wymuszonych sprzętowo tylko do odczytu; oraz

b. Następujących aplikacji z nośników wymuszonych sprzętowo tylko do odczytu: [*Realizacja: aplikacje zdefiniowane przez organizację*].

Omówienie: Środowisko operacyjne systemu zawiera kod, który hostuje aplikacje, w tym systemy operacyjne, systemy wykonawcze lub monitory maszyn wirtualnych (*tzw. hipernadzorcy, ang. hipervisor*). Może ono również zawierać wybrane aplikacje, które są uruchamiane bezpośrednio na platformach sprzętowych. Wymuszone sprzętowo nośniki tylko do odczytu obejmują napędy dyskowe CD-R (*ang. Compact Disc-Recordable*) i DVD-R (*ang. Digital Versatile Disc-Recordable*), a także jednorazową, programowalną pamięć tylko do odczytu. Użycie pamięci niemodyfikowalnej zapewnia integralność oprogramowania od momentu utworzenia obrazu tylko do odczytu. Wykorzystanie reprogramowalnej pamięci tylko do odczytu może być zaakceptowane jako nośnik tylko do odczytu pod warunkiem, że integralność może być odpowiednio chroniona od punktu początkowego zapisu do wprowadzenia pamięci do systemu oraz, że istnieją niezawodne zabezpieczenia sprzętowe przed przeprogramowaniem pamięci, gdy jest ona zainstalowana w systemach organizacyjnych.

Zabezpieczenia powiązane: AC-3, SI-7, SI-14.

Zabezpieczenia rozszerzone:

(1) NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE | NIEZAPISYWALNE PAMIĘCI

Wykorzystywanie [*Realizacja: komponenty systemu zdefiniowane przez organizację*] z niezapisywalnymi pamięciami, których zawartość pozostaje niezmienna po ponownym uruchomieniu komponentu lub włączeniu / wyłączeniu zasilania.

Omówienie: Wyłączenie możliwości zapisu eliminuje możliwość wprowadzenia złośliwego kodu za pośrednictwem trwałego, zapisywalnego nośnika danych w wyznaczonych komponentach systemu. Ograniczenie to ma zastosowanie do pamięci stałej i wymiennej, przy czym w przypadku pamieci wymiennej jest ono uwzględniane bezpośrednio w pamięci lub w postaci specjalnych ograniczeń nakładanych za pośrednictwem zabezpieczeń dostępu do urządzeń przenośnych.

Zabezpieczenia powiązane: AC-19, MP-7.

(2) NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE | OCHRONA INTEGRALNOŚCI / NOŚNIKI TYLKO DO ODCZYTU

Ochrona integralność informacji przechowywanej na nośniku tylko do odczytu i zabezpieczanie nośnika po zapisaniu takich informacji na nośniku.

Omówienie: Mechanizmy zabezpieczeniowe uniemożliwiają podmianę nośników w systemach lub przeprogramowanie programowalnych nośników tylko do odczytu przed ich zainstalowaniem w systemach. Zabezpieczenia integralności obejmują połączenie zapobiegania, wykrywania i reagowania.

Zabezpieczenia powiązane: CM-3, CM-5, CM-9, MP-2, MP-4, MP-5, SC-28, SI-3.

(3) NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE | OCHRONA SPRZĘTOWA

[Wycofane: Przeniesione do: SC-51].

SC-35 ZEWNĘTRZNA IDENTYFIKACJA ZŁOŚLIWEGO KODU

Zabezpieczenie podstawowe: Włączanie komponentów systemu, które proaktywnie starają się zidentyfikować złośliwy kod sieciowy lub złośliwe strony internetowe.

Omówienie: Zewnętrzna identyfikacja złośliwego kodu różni się od wabików opisanych w zabezpieczeniu SC-26 tym, że komponenty te aktywnie przeszukują sieci, w tym Internet, w poszukiwaniu złośliwego kodu zawartego na zewnętrznych stronach internetowych. Podobnie jak wabiki, wykorzystanie technik zewnętrznej identyfikacji złośliwego kodu wymaga pewnych pomocniczych środków izolacyjnych w celu zapewnienia, że jakikolwiek złośliwy kod wykryty podczas przeszukiwania i następnie wykonany, nie zainfekuje systemów organizacyjnych. Wirtualizacja jest powszechną techniką służącą do osiągnięcia takiej izolacji.

Zabezpieczenia powiązane: SC-7, SC-26, SC-44, SI-3, SI-4.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

SC-36 PRZETWARZANIE I PRZECHOWYWANIE ROZPROSZONE

Zabezpieczenie podstawowe: Rozlokowanie następujących komponentów przetwarzania i przechowywania danych w przestrzeni [*Wybór: lokalizacje fizyczne; domeny logiczne*]: [*Realizacja: zdefiniowane przez organizację komponenty przetwarzania i przechowywania danych*].

Omówienie: Rozmieszczenie przetwarzania i przechowywania danych w wielu lokalizacjach fizycznych lub domenach logicznych zapewnia organizacjom pewien stopień redundancji lub nakładania się. Nadmiarowość i nakładanie się zwiększają współczynnik pracy przeciwników w celu negatywnego oddziaływania na operacje organizacyjne, aktywa i osoby. Zastosowanie rozproszonego przetwarzania i przechowywania nie zakłada jednej głównej lokalizacji przetwarzania lub przechowywania. Dlatego też pozwala na równoległe przetwarzanie i przechowywanie danych.

Zabezpieczenia powiązane: CP-6, CP-7, PL-8, SC-32.

Zabezpieczenia rozszerzone:

(1) PRZETWARZANIE I PRZECHOWYWANIE ROZPROSZONE | TECHNIKI PRZEGLĄDANIA CYKLICZNEGO

(a) Stosowanie technik cyklicznego przeglądania w celu zidentyfikowania potencjalnych usterek, błędów lub naruszeń w następujących komponentach przetwarzania i przechowywania: [***Realizacja: zdefiniowane przez organizację rozproszone komponenty przetwarzania i przechowywania***]**; oraz**

(b) W odpowiedzi na zidentyfikowane usterki, błędy lub naruszenia podejmowanie następujących działań: [Realizacja: *działania zdefiniowane przez organizację*].

Omówienie: Rozproszone przetwarzanie i/lub przechowywanie może być stosowane w celu ograniczenia możliwości naruszenia przez przeciwników

poufności, integralności lub dostępności informacji i systemów organizacyjnych. Jednakże, dystrybucja komponentów przetwarzających i przechowujących nie zapobiega narażaniu na kompromitację jednego lub więcej komponentów przez przeciwników. Przetwarzanie rozproszone porównuje wyniki przetwarzania i/lub zawartość zasobów magazynowych z rozproszonych komponentów, a następnie dokonuje oceny wyników. Przetwarzanie rozproszone identyfikuje potencjalne wady, zagrożenia lub błędy w rozproszonych komponentach przetwarzania i przechowywania danych.

Zabezpieczenia powiązane: SI-4.

(2) PRZETWARZANIE I PRZECHOWYWANIE ROZPROSZONE | SYNCHRONIZACJA

Zsynchronizowanie następujących zdublowanych systemów lub komponentów systemowych: [*Realizacja: zdefiniowane przez organizację zdublowane systemy lub komponenty systemowe*].

Omówienie: Zabezpieczenia SC-36 i CP-9(6) nakładają wymóg powielania systemów lub komponentów systemowych w lokalizacjach rozproszonych. Synchronizacja zdublowanych i nadmiarowych usług i danych pomaga zapewnić, że informacje zawarte w rozproszonych lokalizacjach mogą być wykorzystane w misji lub funkcjach biznesowych organizacji, w zależności od potrzeb.

Zabezpieczenia powiązane: CP-9.

Referencje: [NIST SP 800-160-2].

SC-37 KANAŁY POZAPASMOWE

Zabezpieczenie podstawowe: Stosowanie następujących kanałów pozapasmowych [*Realizacja: zdefiniowane przez organizację kanały pozapasmowe*] do fizycznej dostawy lub elektronicznej transmisji [*Realizacja: określone przez organizację informacje, komponenty systemu lub urządzenia*] do [*Realizacja: określone przez organizację osoby lub systemy*].

Omówienie: Kanały pozapasmowe obejmują lokalne (złącza RS, USB, itp.), pozasieciowe dostępy do systemów; ścieżki sieciowe fizycznie oddzielone od ścieżek sieciowych wykorzystywanych do ruchu operacyjnego; lub ścieżki nieelektroniczne, takie jak serwisy pocztowe. Wykorzystanie kanałów pozapasmowych jest odróżniane od użycia kanałów wewnątrzpasmowych, które przenoszą rutynowy ruch operacyjny. Kanały pozapasmowe nie są narażone na takie same zagrożenia jak kanały wewnątrzpasmowe. W związku z tym, naruszenia poufności, integralności lub dostępności kanałów wewnątrzpasmowych nie będą miały negatywnego wpływu na kanały pozapasmowe. Organizacje mogą wykorzystywać kanały pozapasmowe do dostarczania lub przesyłania materiałów organizacyjnych, w tym identyfikatorów i danych uwierzytelniających, informacji o zarządzaniu kluczami kryptograficznymi, kopii zapasowych systemów i danych, zmian w zarządzaniu konfiguracją sprzętu, oprogramowania układowego lub aplikacji, aktualizacji zabezpieczeń, informacji o konserwacji oraz aktualizacji ochrony przed złośliwym kodem.

Zabezpieczenia powiązane: AC-2, CM-3, CM-5, CM-7, IA-2, IA-4 , MA-4, SC-12, SI-3, SI-4, SI-7.

Zabezpieczenia rozszerzone:

(1) KANAŁY POZAPASMOWE | GWARANTOWANA DOSTAWA / TRANSMISJA

Stosowanie [***Realizacja: środki bezpieczeństwa określone przez organizację***] ***w* celu zapewnienia, że tylko** [***Realizacja: osoby lub systemy określone przez organizację***] **otrzymują następujące informacje, komponenty systemu lub**

urządzenia: [***Realizacja: informacje, komponenty systemu lub urządzenia określone przez organizację***]**.**

Omówienie: Techniki stosowane przez organizacje w celu zapewnienia, że tylko wyznaczone systemy lub osoby otrzymują określone informacje, komponenty systemu lub urządzenia, obejmują wysyłanie elementów uwierzytelniających za pośrednictwem zatwierdzonej organizacji świadczącej usługi pocztowe (kurierskie), wymagając od odbiorców okazania dokumentu tożsamości ze zdjęciem, jako warunku odbioru przesyłki.

Zabezpieczenia powiązane: Brak.

Referencje: [NIST SP 800-57-1], [NIST SP 800-57-2], [NIST SP 800-57-3].

SC-38 BEZPIECZEŃSTWO OPERACJI

Zabezpieczenie podstawowe: Stosowanie następujących środków bezpieczeństwa operacyjnego w celu ochrony kluczowych informacji organizacyjnych w całym cyklu życia systemu: [*Realizacja: środki bezpieczeństwa operacji zdefiniowane przez organizację*].

Omówienie: Bezpieczeństwo operacyjne (*ang. Operations security - OPSEC*) jest usystematyzowanym procesem, dzięki któremu potencjalni przeciwnicy mogą być pozbawieni informacji dotyczących zdolności i zamiarów organizacji. Osiągane jest to poprzez identyfikację, kontrolę i ochronę informacji jawnych, które w sposób szczególny odnoszą się do planowania i wykonywania wrażliwych działań organizacyjnych. Proces OPSEC obejmuje pięć etapów: identyfikację informacji krytycznych, analizę zagrożeń, analizę podatności, ocenę ryzyka oraz zastosowanie odpowiednich środków zaradczych. Środki bezpieczeństwa OPSEC są stosowane w systemach organizacyjnych i środowiskach, w których te systemy funkcjonują. Zabezpieczenia OPSEC chronią poufność informacji, w tym ograniczają dzielenie się informacjami z dostawcami, potencjalnymi dostawcami oraz innymi pozaorganizacyjnymi podmiotami i osobami. Informacje krytyczne dla misji organizacji i jej funkcji biznesowych obejmują dane identyfikacyjne użytkowników, wykorzystanie elementów, dostawców, procesy łańcucha dostaw, wymagania funkcjonalne, wymagania bezpieczeństwa, specyfikacje projektowe systemu, protokoły testowania i oceny oraz szczegóły wdrożenia środków bezpieczeństwa.

Zabezpieczenia powiązane: CA-2, CA-7, PL-1, PM-9, PM-12, RA-2, RA-3, RA-5, SC-7, SR-3, SR-7.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

SC-39 IZOLACJA PROCESÓW

Zabezpieczenie podstawowe: Utrzymywanie osobnej domeny wykonawczej dla każdego systemowego procesu wykonawczego.

Omówienie: Systemy mogą utrzymywać osobne domeny wykonawcze dla każdego procesu wykonawczego poprzez przypisanie każdemu procesowi osobnej przestrzeni adresowej. Każdy proces systemowy posiada odrębną przestrzeń adresową, dzięki czemu komunikacja pomiędzy procesami odbywa się w sposób kontrolowany przez funkcje bezpieczeństwa, a jeden proces nie może modyfikować kodu wykonawczego innego procesu. Zachowanie oddzielnych domen procesów wykonawczych może być osiągnięte na przykład przez zaimplementowanie oddzielnych przestrzeni adresowych. Technologie separacji procesów, w tym sandboxing (piaskownica) lub wirtualizacja, logiczne oddzielenie aplikacji i oprogramowania układowego od innego oprogramowania, firmware'u i danych. Izolacja procesów pomaga ograniczyć dostęp potencjalnie niezaufanego oprogramowania do innych zasobów systemowych. Możliwość utrzymania oddzielnych domen wykonawczych jest dostępna w komercyjnych systemach operacyjnych, które wykorzystują technologie wieloprocesorowe.

Zabezpieczenia powiązane: AC-3, AC-4, AC-6, AC-25, SA-8, SC-2, SC-3, SI-16.

Zabezpieczenia rozszerzone:

(1) IZOLACJA PROCESÓW | SEPARACJA SPRZĘTOWA

Wdrożenie mechanizmów separacji sprzętowej w celu ułatwienia izolacji procesów.

Omówienie: Sprzętowa separacja procesów systemowych jest generalnie mniej podatna na naruszenia niż separacja programowa, co daje większą pewność, że separacja będzie egzekwowana. Sprzętowe mechanizmy separacji obejmują sprzętowe zarządzanie pamięcią.

Zabezpieczenia powiązane: Brak.

(2) IZOLACJA PROCESÓW | ODDZIELNA DOMENA WYKONAWCZA DLA KAŻDEGO WĄTKU

Zachowanie oddzielnej domeny wykonawczej dla każdego wątku w [***Realizacja: zdefiniowane przez organizację przetwarzanie wielowątkowe***]**.**

Omówienie: Brak.

Zabezpieczenia powiązane: Brak.

Referencje: [NIST SP 800-160-1].

SC-40 OCHRONA ŁĄCZA BEZPRZEWODOWEGO

Zabezpieczenie podstawowe: Zabezpieczanie zewnętrznych i wewnętrznych [*Realizacja: zdefiniowane przez organizację łącza bezprzewodowe*] przed następującymi rodzajami ataków na parametry sygnału: [*Realizacja: zdefiniowane przez organizację rodzaje ataków na parametry sygnału lub odwołania do źródeł takich ataków*].

Omówienie: Ochrona połączeń bezprzewodowych dotyczy wewnętrznych i zewnętrznych połączeń bezprzewodowych, które mogą być widoczne dla osób nie będących autoryzowanymi użytkownikami systemu. Adwersarze mogą wykorzystywać parametry sygnału łączy bezprzewodowych, jeśli takie łącza nie są odpowiednio chronione. Istnieje wiele sposobów na wykorzystanie parametrów sygnału łączy bezprzewodowych w celu zdobycia informacji, odmowy świadczenia usług lub podszywania się pod użytkowników systemu. Ochrona łączy bezprzewodowych zmniejsza wpływ ataków, które są unikalne dla systemów bezprzewodowych. Jeżeli organizacje polegają na komercyjnych dostawcach usług transmisyjnych traktując je jako towary, a nie jako usługi w pełni dedykowane, wdrożenie ochrony łączy bezprzewodowych w stopniu niezbędnym do spełnienia organizacyjnych wymagań bezpieczeństwa może okazać się niemożliwe.

Zabezpieczenia powiązane: AC-18, SC-5.

Zabezpieczenia rozszerzone:

(1) OCHRONA ŁĄCZA BEZPRZEWODOWEGO | INTERFERENCJA ELEKTROMAGNETYCZNA

Wdrożenie mechanizmów kryptograficznych, które osiągają [*Realizacja: poziom ochrony zdefiniowany przez organizację*] przed skutkami zamierzonych zakłóceń elektromagnetycznych.

Omówienie: Wdrożenie kryptograficznych mechanizmów ochrony przed zakłóceniami elektromagnetycznymi chroni systemy przed celowym zagłuszaniem,

które może uniemożliwić lub utrudnić komunikację, zapewniając, że bezprzewodowe, fale widma rozproszonego wykorzystywane do ochrony przed zagłuszaniem nie są przewidywalne przez osoby nieupoważnione. Wdrożenie mechanizmów kryptograficznych może również pośrednio złagodzić skutki niezamierzonego zagłuszania spowodowanego zakłóceniami ze strony legalnych nadajników korzystających z tego samego widma. Wymagania operacyjne, przewidywane zagrożenia, koncepcja operacji oraz przepisy prawne, zarządzenia, dyrektywy, rozporządzenia, polityki i standardy określają poziomy dostępności łącza bezprzewodowego, wymaganej wydajności i kryptografii.

Zabezpieczenia powiązane: PE-21, SC-12, SC-13.

(2) OCHRONA ŁĄCZA BEZPRZEWODOWEGO | REDUKCJA POTENCJALNEJ DETEKCJI

Wdrożenie mechanizmów kryptograficznych w celu zmniejszenia potencjału wykrywania połączeń bezprzewodowych do [***Realizacja: poziom redukcji określony przez organizację***]**.**

Omówienie: Implementacja mechanizmów kryptograficznych w celu zmniejszenia możliwości wykrycia jest stosowana do komunikacji niejawnej oraz do ochrony nadajników bezprzewodowych przed geolokalizacją. Zapewnia to również, że rozkład fal widma wykorzystywany do osiągnięcia niskiego prawdopodobieństwa wykrycia nie jest możliwy do przewidzenia przez osoby nieupoważnione. Wymagania operacyjne, przewidywane zagrożenia, koncepcja operacji oraz obowiązujące przepisy, zarządzenia, dyrektywy, rozporządzenia, polityki i standardy określają poziom niewykrywalności łączy bezprzewodowych.

Zabezpieczenia powiązane: SC-12, SC-13.

(3) OCHRONA ŁĄCZA BEZPRZEWODOWEGO | NAŚLADOWCZE LUB MANIPULACYJNE OSZUSTWO TELEKOMUNIKACYJNE

Implementowanie mechanizmów kryptograficznych w celu identyfikowania i odrzucania transmisji bezprzewodowych, które są celowymi próbami

uwierzytelnienia oszustwa opartego na naśladownictwie lub manipulacji parametrami sygnału.

Omówienie: Zastosowanie kryptograficznych mechanizmów identyfikacji i odrzucania komunikacji naśladującej lub manipulacyjnej zapewnia, że parametry sygnału transmisji bezprzewodowej nie są przewidywalne przez osoby niepowołane. Taka nieprzewidywalność zmniejsza prawdopodobieństwo naśladowania lub zmanipulowania komunikacji opartej wyłącznie na parametrach sygnału.

Zabezpieczenia powiązane: SC-12, SC-13, SI-4.

(4) OCHRONA ŁĄCZA BEZPRZEWODOWEGO | IDENTYFIKACJA PARAMETRÓW SYGNAŁU

Zaimplementowanie mechanizmów kryptograficznych uniemożliwiających identyfikację [Realizacja: *zdefiniowane przez organizację nadajniki bezprzewodowe*] poprzez wykorzystanie parametrów sygnału nadajnika.

Omówienie: Wdrożenie mechanizmów kryptograficznych uniemożliwiających identyfikację nadajników bezprzewodowych chroni przed jednoznaczną identyfikacją nadajników bezprzewodowych na potrzeby analizy wywiadowczej poprzez zapewnienie, że zmiany parametrów sygnału z wykorzystaniem metody zapobiegającej tworzeniu odcisków cyfrowych (ang. anti-fingerprinting) nie są możliwe do przewidzenia przez osoby niepowołane. Zapewnia to również anonimowość. Techniki identyfikacji radiowych odcisków cyfrowych identyfikują unikalne parametry sygnału nadajników w celu pobrania odcisków tych nadajników dla celów śledzenia i identyfikacji misji lub użytkownika.

Zabezpieczenia powiązane: SC-12, SC-13.

Referencje: Brak.

SC-41 DOSTĘP DO PORTÓW I URZĄDZEŃ WEJŚCIA / WYJŚCIA

Zabezpieczenie podstawowe: [*Wybór: Fizyczne; Logicznie*] wyłączenie lub usunięcie [*Realizacja: zdefiniowane przez organizację porty połączeniowe lub urządzenia wejścia/wyjścia*] w następujących systemach lub komponentach systemu: [*Realizacja: zdefiniowane przez organizację systemy lub komponenty systemu*].

Omówienie: Porty połączeniowe obejmują Universal Serial Bus (USB), Thunderbolt i Firewire (IEEE 1394). Urządzenia wejścia/wyjścia (*ang. I/O*) obejmują napędy płyt kompaktowych CD oraz uniwersalne cyfrowe napędy dyskowe DVD. Wyłączenie lub usunięcie takich portów połączeniowych i urządzeń wejścia/wyjścia pomaga zapobiegać przenikaniu informacji z systemów i wprowadzaniu złośliwego kodu przez te porty lub urządzenia. Fizyczne wyłączenie lub usunięcie portów i/lub urządzeń jest działaniem bardziej skutecznym.

Zabezpieczenia powiązane: AC-20, MP-7.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

SC-42 CZUJNIKI

Zabezpieczenie podstawowe:

a. Zakazanie [*Wybór (jednego lub więcej): stosowania urządzeń posiadających* [*Realizacja: zdolność wykrywania środowiska zdefiniowaną przez organizację*] *w* [*Realizacja: obiekty, obszary lub systemy zdefiniowane przez organizację*]*; zdalnego uruchamiania zdolności wykrywania środowiska w systemach lub komponentach systemu, z następującymi wyjątkami:* [Realizacja: *zdefiniowane przez organizację wyjątki zezwalające na zdalne uruchamianie czujników*]]*;* oraz

b. Wyraźne wskazanie użycia czujnika przez [*Realizacja: zdefiniowana przez organizację grupa użytkowników*].

Omówienie: Możliwości i dane z czujników odnoszą się do typów systemów lub komponentów systemowych scharakteryzowanych jako urządzenia mobilne, takie jak telefony komórkowe, smartfony i tablety. Urządzenia mobilne często zawierają czujniki, które mogą gromadzić i rejestrować dane dotyczące środowiska, w którym system jest używany. Czujniki włączane w urządzeniach mobilnych obejmują mikrofony, aparaty fotograficzne, mechanizmy globalnego systemu pozycjonowania (GPS) oraz akceleratory. O ile czujniki umieszczone w urządzeniach przenośnych pełnią ważną funkcję, o tyle w przypadku ich ukrytej aktywacji urządzenia takie mogą potencjalnie stanowić dla przeciwników środek do zdobywania cennych informacji o osobach i organizacjach. Na przykład, zdalna aktywacja funkcji GPS w urządzeniu przenośnym może zapewnić przeciwnikowi możliwość śledzenia ruchów danej osoby. Organizacje mogą zabronić osobom wnoszenia telefonów komórkowych lub aparatów cyfrowych do niektórych wyznaczonych obiektów lub stref kontrolowanych w obiektach, w których przechowywane są informacje niejawne lub odbywają się wrażliwe rozmowy.

Zabezpieczenia powiązane: SC-15.

Zabezpieczenia rozszerzone:

(1) CZUJNIKI | RAPORTOWANIE DO UPOWAŻNIONYCH OSÓB LUB RÓL

Sprawdzanie, czy system jest skonfigurowany w taki sposób, że dane lub informacje zbierane przez [***Realizacja: czujniki zdefiniowane przez organizację***] **są zgłaszane tylko upoważnionym osobom lub rolom.**

Omówienie: W sytuacjach, gdy czujniki są aktywowane przez osoby upoważnione, nadal istnieje możliwość, że dane lub informacje zebrane przez czujniki zostaną przesłane do osób nieupoważnionych.

Zabezpieczenia powiązane: Brak.

(2) CZUJNIKI | AUTORYZOWANE UŻYCIE

Stosowanie następujących środków zapewniających, że dane lub informacje zbierane przez [***Realizacja: czujniki zdefiniowane przez organizację***] ***są*** **wykorzystywane wyłącznie do dozwolonych celów: [Realizacja:** ***środki zdefiniowane przez organizację***].

Omówienie: Informacje zbierane przez czujniki w określonym, autoryzowanym celu mogą zostać niewłaściwie wykorzystane do jakiegoś nieautoryzowanego celu. Na przykład czujniki GPS, które są wykorzystywane do wspomagania nawigacji drogowej, mogą być niewłaściwie wykorzystywane do śledzenia ruchów osób. Środki łagodzące takie działania obejmują dodatkowe szkolenia pomagające upewnić się, że upoważnione osoby nie nadużywają swoich uprawnień oraz ograniczenia umowne dotyczące wykorzystywania takich danych w przypadku, gdy dane z czujników są przechowywane przez strony zewnętrzne.

Zabezpieczenia powiązane: PT-2.

(3) CZUJNIKI | ZABRONIONE WYKORZYSTANIE URZĄDZEŃ

[Wycofane: Włączone do SC-42].

(4) CZUJNIKI | POWIADOMIENIE O ZBIERANIU DANYCH

Zastosowanie następujących środków mających na celu zwiększenie świadomości danej osoby, że dane osobowe są zbierane przez [***Realizacja: czujniki zdefiniowane przez organizację***]***:*** **[Realizacja:** ***środki określone przez organizację***]***:***

Omówienie: Świadomość, że czujniki organizacyjne gromadzą dane, umożliwia osobom bardziej efektywne zaangażowanie się w zarządzanie swoją prywatnością. Środki te mogą obejmować konwencjonalne pisemne powiadomienia i konfiguracje czujników, które bezpośrednio lub pośrednio, poprzez inne urządzenia, uświadamiają osobom, że czujnik gromadzi informacje za pośrednictwem innych urządzeń. Ważnymi czynnikami są użyteczność i skuteczność powiadomienia.

Zabezpieczenia powiązane: PKT-1, PT-4, PT-5.

(5) CZUJNIKI | MINIMALIZACJA GROMADZENIA DANYCH

Stosowanie [*Realizacja: czujniki zdefiniowane przez organizację*] skonfigurowanych tak, aby ograniczać do minimum zbieranie informacji o osobach.

Omówienie: Chociaż zasady kontroli autoryzowanego użycia mogą być stosowane do informacji już zgromadzonych, minimalizacja gromadzenia informacji, które nie są potrzebne, zmniejsza ryzyko naruszenia prywatności w momencie wprowadzenia do systemu i zmniejsza ryzyko niepowodzenia polityki kontroli. Konfiguracje czujników obejmują maskowanie elementów wyglądu człowieka, takie jak rozmycie lub pikselizacja odcieni ciała.

Zabezpieczenia powiązane: SA-8, SI-12.

Referencje: [OMB A-130], [NIST SP 800-124].

SC-43 OGRANICZENIA UŻYCIA

Zabezpieczenie podstawowe:

a. Ustanowienie ograniczeń w użytkowaniu i wytycznych wdrożeniowych dotyczących następujących komponentów systemu: [*Realizacja: zdefiniowane przez organizację komponenty systemu*]; oraz

b. Autoryzacja, monitorowanie i kontrolowanie wykorzystania tych komponentów w systemie.

Omówienie: Ograniczenia w użytkowaniu mają zastosowanie do wszystkich komponentów systemu, w tym między innymi do kodów mobilnych, urządzeń przenośnych, dostępu bezprzewodowego oraz przewodowych i bezprzewodowych urządzeń peryferyjnych (np. kopiarek, drukarek, skanerów, urządzeń optycznych i innych podobnych technologii). Ograniczenia w użytkowaniu i wytyczne dotyczące wdrażania są oparte na potencjale komponentów systemu do spowodowania uszkodzenia systemu i pomagają zapewnić, że będzie on używany tylko przez osoby upoważnione.

Zabezpieczenia powiązane: AC-18, AC-19, CM-6, SC-7, SC-18.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [NIST SP 800-124].

SC-44 KOMORY DETONACYJNE

Zabezpieczenie podstawowe: Wykorzystanie możliwości komory detonacyjnej w ramach [*Realizacja: system zdefiniowany przez organizację, komponent systemu lub lokalizacja*].

Omówienie: Komory detonacyjne, znane również jako dynamiczne środowiska wykonawcze, pozwalają organizacjom otwierać załączniki do wiadomości e-mail, uruchamiać niezaufane lub podejrzane aplikacje oraz wykonywać żądania ujednoliconych formatów adresowania (ang. Universal Resource Locator - URL) w bezpiecznym, izolowanym środowisku lub zwirtualizowanej piaskownicy (ang. virtualized sandbox). Chronione i izolowane środowiska wykonawcze zapewniają środki do określenia, czy powiązane załączniki lub aplikacje zawierają złośliwy kod. Mimo, że jest to związane z koncepcją sieci przechwytujących, wykorzystanie komór detonacyjnych nie ma na celu utrzymania długoterminowego środowiska, w którym mogą działać przeciwnicy, a ich działania mogą być obserwowane. Komory detonacyjne mają raczej na celu szybkie zidentyfikowanie złośliwego kodu i albo zmniejszenie prawdopodobieństwa, że kod ten zostanie rozprzestrzeniony do środowisk operacyjnych użytkowników, albo całkowite uniemożliwienie takiego rozprzestrzeniania.

Zabezpieczenia powiązane: SC-7, SC-18, SC-25, SC-26, SC-30, SC-35, SC-39, SI-3, SI-7.

Zabezpieczenia rozszerzone: Brak.

Referencje: [NIST SP 800-177].

SC-45 SYNCHRONIZACJA CZASU SYSTEMOWEGO

Zabezpieczenie podstawowe: Synchronizowanie zegarów systemowych w ramach oraz pomiędzy systemami i komponentami systemu.

Omówienie: Synchronizacja czasu zegarów systemowych jest niezbędna do prawidłowego wykonywania wielu usług systemowych, w tym procesów identyfikacji i uwierzytelniania, które wykorzystują certyfikaty i ograniczenia czasowe jako część kontroli dostępu. Odmowa świadczenia usług lub brak możliwości odrzucenia wygasłych poświadczeń może być skutkiem braku prawidłowej synchronizacji zegarów w obrębie systemów i komponentów systemu oraz pomiędzy nimi. Czas jest powszechnie wyrażany w uniwersalnym czasie koordynowanym (*ang.* Universal Time Coordinated - *UTC*), współczesnej kontynuacji czasu uniwersalnego Greenwich (*ang. Greenwich Mean Time - GMT*), lub w czasie lokalnym z przesunięciem w stosunku do czasu UTC. Dokładność pomiaru czasu odnosi się do dokładności synchronizacji pomiędzy zegarami systemu i zegarami odniesienia, np. zegary synchronizują się z dokładnością do setek milisekund lub dziesiątek milisekund. Organizacje mogą definiować różne granulacje czasu dla poszczególnych komponentów systemu. Funkcje usług czasowych mogą być krytyczne dla innych funkcji bezpieczeństwa - takich jak kontrola dostępu oraz identyfikacja i uwierzytelnianie - w zależności od charakteru mechanizmów wykorzystywanych do wspierania tych funkcji.

Zabezpieczenia powiązane: AC-3, AU-8, IA-2, IA-8.

Zabezpieczenia rozszerzone:

(1) SYNCHRONIZACJA CZASU SYSTEMOWEGO | SYNCHRONIZACJA Z AUTORYZOWANYM ŹRÓDŁEM CZASU ODNIESIENIA

a) Porównywanie wewnętrznych zegarów systemowych [***Realizacja: częstotliwość zdefiniowana przez organizację***] ***z*** [***Realizacja: wiarygodne źródło czasu zdefiniowane przez organizację***]***;*** **oraz**

(b) Synchronizowanie wewnętrznych zegarów systemowych z wiarygodnym źródłem czasu, gdy różnica czasu jest większa niż [***Realizacja: jednostka czasu określona przez organizację***]**.**

Omówienie: Synchronizacja wewnętrznych zegarów systemowych z autorytatywnym źródłem czasu zapewnia jednolitość znaczników czasu w systemach z wieloma zegarami systemowymi i systemach połączonych poprzez sieć.

Zabezpieczenia powiązane: Brak.

(2) SYNCHRONIZACJA CZASU SYSTEMOWEGO | WTÓRNE ŹRÓDŁO CZASU ODNIESIENIA

(a) Określenie wtórnego miarodajnego źródła czasu, które znajduje się w innym regionie geograficznym niż główne wiarygodne źródło czasu; oraz

(b) Synchronizowanie wewnętrznych zegarów systemowych z wtórnym miarodajnym źródłem czasu, jeśli podstawowe wiarygodne źródło czasu jest niedostępne.

Omówienie: Może okazać się konieczne wykorzystanie informacji geolokalizacyjnych w celu ustalenia, że wtórne miarodajne źródło czasu znajduje się w innym regionie geograficznym.

Zabezpieczenia powiązane: Brak.

Referencje: [IETF 5905].

SC-46 EGZEKWOWANIE POLITYKI MIĘDZYDOMENOWEJ

Zabezpieczenie podstawowe: Wdrożenie mechanizmu [*Wybór: fizyczny; logiczny*] egzekwowania polityki międzydomenowej pomiędzy fizycznymi i/lub sieciowymi interfejsami do łączenia domen bezpieczeństwa.

Omówienie: W przypadku mechanizmów logicznego egzekwowania polityki, organizacje unikają tworzenia logicznej ścieżki między interfejsami, aby zapobiec możliwości ominięcia mechanizmu egzekwowania polityki. W przypadku fizycznych mechanizmów egzekwowania zasad konieczne może być zapewnienie trwałej izolacji fizycznej zapewnianej przez fizyczne wdrożenie egzekwowania polityki w celu wykluczenia obecności ukrytych kanałów logicznych przenikających do domeny bezpieczeństwa.

Zabezpieczenia powiązane: AC-4, SC-7.

Zabezpieczenia rozszerzone: Brak.

Referencje: [NIST SP 800-160-1].

SC-47 ALTERNATYWNE ŚCIEŻKI KOMUNIKACYJNE

Zabezpieczenie podstawowe: Ustanowienie [*Realizacja: zdefiniowane przez organizację alternatywne ścieżki komunikacyjne*] do zarządzania i kontroli operacji systemowych.

Omówienie: Incydent, niezależnie od tego, czy ma podłoże agresywne czy nie, może zakłócić ustalone ścieżki komunikacyjne wykorzystywane do operacji systemowych oraz zarządzania i kontroli organizacji. Alternatywne ścieżki komunikacyjne zmniejszają ryzyko, że wszystkie ścieżki komunikacyjne zostaną naruszone przez ten sam incydent. Aby spotęgować problem, nieuzyskanie przez personel organizacyjny na czas informacji o zakłóceniach lub nieudzielenie na czas wskazówek jednostkom operacyjnym po incydencie związanym ze ścieżkami komunikacji, może wpłynąć na zdolność organizacji do reagowania na takie incydenty w odpowiednim czasie. Ustanowienie alternatywnych ścieżek łączności dla celów zarządzania i kontroli, w tym wyznaczenie alternatywnych decydentów, jeśli główne osoby decyzyjne są niedostępne oraz ustalenie zakresu i ograniczeń ich działań, może znacznie ułatwić zdolność organizacji do kontynuowania operacji i podejmowania odpowiednich działań podczas incydentu.

Zabezpieczenia powiązane: CP-2, CP-8.

Zabezpieczenia rozszerzone: Brak.

Referencje: [NIST SP 800-34], [NIST SP 800-61], [NIST SP 800-160-2].

SC-48 ROZMIESZCZENIE CZUJNIKÓW

Zabezpieczenie podstawowe: Rozmieszczenie [*Realizacja: czujniki i zasoby monitorowania określone przez organizację*] w [*Realizacja: lokalizacja określona przez organizację*] *w* następujących warunkach lub okolicznościach: [*Realizacja: warunki lub okoliczności określone przez organizację*].

Omówienie: Adwersarze mogą podążać różnymi ścieżkami i stosować różne podejścia, gdy "przedostając się bokiem" do organizacji (w tym do jej systemów) próbują dotrzeć do celu lub próbują eksfiltrować informacje z organizacji. Organizacja często dysponuje jedynie ograniczonym zestawem możliwości monitorowania i wykrywania, które mogą być skoncentrowane na krytycznych lub prawdopodobnych ścieżkach infiltracji lub eksfiltracji. Wykorzystując ścieżki komunikacyjne, których organizacja zazwyczaj nie monitoruje, przeciwnik może zwiększyć swoje szanse na osiągnięcie zamierzonych celów. Przenosząc swoje czujniki lub potencjał monitorowania w nowe miejsca, organizacja może utrudnić przeciwnikowi osiągnięcie jego celów. Przeniesienie czujników lub zasobów monitorujących może być dokonane na podstawie informacji o zagrożeniach, które organizacja zdobyła lub przeprowadzane losowo, aby zmylić przeciwnika i utrudnić mu przejście boczne przez system lub organizację.

Zabezpieczenia powiązane: AU-2, SC-7, SI-4.

Zabezpieczenia rozszerzone:

(1) RELOKACJA CZUJNIKA | DYNAMICZNE PRZEMIESZCZANIE CZUJNIKÓW LUB URZĄDZEŃ MONITORUJĄCYCH

Dynamiczne przemieszczanie [***Realizacja: czujniki i zasoby monitorowania określone przez organizację***] **do** [***Realizacja: lokalizacja określona przez organizację***] ***w*** **następujących warunkach lub okolicznościach:** [***Realizacja: warunki lub okoliczności określone przez organizację***]**.**

Omówienie: Brak.

Zabezpieczenia powiązane: Brak.

Referencje: [NIST SP 800-160-2].

SC-49 EGZEKWOWANIE SEPARACJI SPRZĘTOWEJ / POLITYKA EGZEKWOWANIA

Zabezpieczenie podstawowe: Wdrożenie sprzętowych mechanizmów separacji i egzekwowania polityki pomiędzy [*Realizacja: zdefiniowane przez organizację domeny bezpieczeństwa*].

Omówienie: Właściciele systemów mogą potrzebować dodatkowej siły mechanizmów zapewniających rozdzielenie domen i egzekwowanie polityki w odniesieniu do konkretnych rodzajów zagrożeń i środowisk działania. Separacja i egzekwowanie polityk za pomocą sprzętu zapewnia większą siłę mechanizmu niż separacja i egzekwowanie polityk za pomocą oprogramowania.

Zabezpieczenia powiązane: AC-4, SA-8, SC-50.

Zabezpieczenia rozszerzone: Brak.

Referencje: [NIST SP 800-160-1].

SC-50 EGZEKWOWANIE SEPARACJI PROGRAMOWEJ / POLITYKA EGZEKWOWANIA

Zabezpieczenie podstawowe: Wdrożenie wymuszonych programowo mechanizmów separacji i egzekwowania polityk pomiędzy [*Realizacja: zdefiniowane przez organizację domeny bezpieczeństwa*].

Omówienie: Właściciele systemów mogą potrzebować dodatkowej siły mechanizmów zapewniających rozdzielenie domen i egzekwowanie polityki w odniesieniu do konkretnych rodzajów zagrożeń i środowisk działania.

Zabezpieczenia powiązane: AC-3, AC-4, SA-8, SC-2, SC-3, SC-49.

Zabezpieczenia rozszerzone: Brak.

Referencje: [NIST SP 800-160-1].

SC-51 OCHRONA SPRZĘTOWA

Zabezpieczenie podstawowe:

a. Stosowanie sprzętowej ochrony przed zapisem w oprogramowaniu układowym (firmware) [*Realizacja: elementy oprogramowania układowego systemu zdefiniowane przez organizację*]; oraz

b. Wdrożenie określonych procedur dla personelu [*Realizacja: osoby upoważnione zdefiniowane przez organizację*], umożliwiających ręczne wyłączanie sprzętowej ochrony przed zapisem w przypadku modyfikacji oprogramowania układowego i ponowne włączanie ochrony przed zapisem przed powrotem systemu do trybu operacyjnego.

Omówienie: Brak.

Zabezpieczenia powiązane: Brak.

Zabezpieczenia rozszerzone: Brak.

KATEGORIA SI – INTEGRALNOŚĆ SYSTEMU I INFORMACJI

SI-1 POLITYKA I PROCEDURY

Zabezpieczenie podstawowe:

a. Opracowywanie, dokumentowanie i rozpowszechnianie wśród [Realizacja: *personel lub role określone przez organizację*]:

   1. [*Wybór (jeden lub więcej): poziom organizacji; poziom misji/procesu biznesowego; poziom systemu*] polityki integralności systemu i informacji, która:

      (a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami; oraz

      (b) Jest zgodna z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi; oraz

   2. Procedur ułatwiających wdrożenie polityki integralności systemu i informacji oraz powiązanych zabezpieczeń w zakresie integralności systemu i informacji;

b. Wyznaczanie [Realizacja: *osoba wyznaczona przez organizację*] do zarządzania rozwojem, dokumentacją i rozpowszechnianiem polityki i procedur integralności systemu i informacji; oraz

c. Przeglądanie i aktualizacja bieżącej:

   1. Polityki integralności systemu i informacji z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*]; oraz

   2. Procedur integralności systemu i informacji z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*].

Omówienie: Polityka i procedury w zakresie integralności systemu i informacji dotyczą zabezpieczeń w kategorii *Integralność systemu i informacji* (SI), które są wdrażane w ramach systemów i organizacji. Strategia zarządzania ryzykiem jest ważnym czynnikiem przy tworzeniu takich polityk i procedur. Polityki i procedury przyczyniają się do zapewnienia bezpieczeństwa i ochrony prywatności. Dlatego ważne jest, aby programy bezpieczeństwa i ochrony prywatności były opracowywane wspólnie przy kształtowaniu polityki i procedur integralności systemu i informacji. Polityki i procedury dotyczące programów bezpieczeństwa i ochrony prywatności na poziomie organizacji są ogólnie rzecz biorąc preferowane i mogą eliminować potrzeby tworzenia polityk i procedur specyficznych dla danej misji lub systemu. Polityka może być włączona jako część ogólnej polityki bezpieczeństwa i ochrony prywatności lub reprezentowana przez wiele polityk odzwierciedlających złożony charakter organizacji. Procedury mogą być ustanowione dla programów bezpieczeństwa i ochrony prywatności, dla misji lub procesów biznesowych oraz dla systemów, jeśli to konieczne. Procedury opisują sposób wdrażania zasad lub zabezpieczeń i mogą być skierowane do osoby lub roli, która jest przedmiotem procedury. Procedury mogą być udokumentowane w planach bezpieczeństwa i ochrony prywatności systemu w jednym lub kilku oddzielnych dokumentach.

Zdarzenia, które mogą spowodować konieczność aktualizacji polityki i procedur integralności systemu i informacji, obejmują wyniki oceny lub audytu, incydenty lub naruszenia bezpieczeństwa, lub zmiany w przepisach prawa, zarządzeniach, dyrektywach, rozporządzeniach, zasadach, standardach i wytycznych.

Oświadczenie o wprowadzeniu zabezpieczeń nie jest równoznaczne z ustanowieniem polityki lub procedury organizacyjnej.

Zabezpieczenia powiązane: PM-9, PS-8, SA-8, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [NIST SP 800-12], [NIST SP 800-100].

SI-2 USUWANIE USTEREK

Zabezpieczenie podstawowe:

a. Identyfikowanie, zgłaszanie i korygowanie niedoskonałości systemu;

b. Testowanie, przed instalacją, aktualizacji aplikacji i oprogramowania układowego związanego z usuwaniem usterek pod kątem skuteczności tych aktualizacji i potencjalnych skutków ubocznych;

c. Instalowanie aktualizacji aplikacji i oprogramowania układowego związanych z bezpieczeństwem w ciągu [*Realizacja: okres czasu określony przez organizację*] od momentu wydania aktualizacji; oraz

d. Włączenie usuwania usterek do procesu zarządzania konfiguracją organizacji.

Omówienie: Konieczność usuwania wad systemowych dotyczy wszystkich rodzajów aplikacji i oprogramowania układowego. Organizacje identyfikują systemy, w których występują błędy w oprogramowaniu, w tym potencjalne podatności wynikające z tych błędów i zgłaszają te informacje wyznaczonym pracownikom organizacji odpowiedzialnym za bezpieczeństwo i prywatność informacji. Aktualizacje istotne dla bezpieczeństwa obejmują poprawki, dodatki Service Pack i sygnatury złośliwych kodów. Organizacje zajmują się również błędami wykrytymi podczas ocen, ciągłego monitorowania, reagowania na incydenty i obsługi błędów systemowych. Dzięki włączeniu naprawiania błędów do procesów zarządzania konfiguracją, wymagane działania naprawcze mogą być śledzone i weryfikowane.

Określone przez organizację okresy aktualizacji aplikacji i oprogramowania układowego istotnych z punktu widzenia bezpieczeństwa mogą się różnić w zależności od różnych czynników ryzyka, w tym kategorii bezpieczeństwa systemu, krytyczności aktualizacji (tj. wagi podatności związanej z odkrytą wadą), tolerancji ryzyka organizacji, misji obsługiwanej przez system lub środowiska zagrożeń. Niektóre sposoby usuwania błędów mogą wymagać przeprowadzenia większej liczby testów niż inne ich rodzaje. Organizacje określają rodzaj testów wymaganych dla

konkretnego typu rozważanych działań naprawczych oraz rodzaje zmian, które są zarządzane przez konfigurację. W niektórych sytuacjach organizacje mogą stwierdzić, że testowanie aktualizacji aplikacji lub oprogramowania układowego nie jest konieczne lub praktyczne, np. w przypadku wdrażania prostych aktualizacji sygnatur złośliwych kodów. Przy podejmowaniu decyzji o testowaniu organizacje biorą pod uwagę, czy istotne dla bezpieczeństwa aktualizacje aplikacji lub oprogramowania układowego są uzyskiwane z autoryzowanych źródeł i posiadają odpowiednie podpisy cyfrowe.

Zabezpieczenia powiązane: CA-5, CM-3, CM-4, CM-5, CM-6, CM-8, MA-2, RA-5, SA-8, SA-10, SA-11, SI-3, SI- 5, SI-7, SI-11.

Zabezpieczenia rozszerzone:

(1) USUWANIE USTEREK | ZARZĄDZANIE CENTRALNE

[Wycofane: Włączone do PL-9].

(2) USUWANIE USTEREK | ZAUTOMATYZOWANE USUWANIE USTEREK

Ustalanie przy użyciu [Realizacja: mechanizmy automatyczne zdefiniowane przez organizację] z częstotliwością [Realizacja: częstotliwość zdefiniowana przez organizację], czy komponenty systemu mają zainstalowane stosowne, istotne z punktu widzenia bezpieczeństwa aktualizacje aplikacji i oprogramowania układowego.

Omówienie: Zautomatyzowane mechanizmy mogą śledzić i określać stan zidentyfikowanych usterek komponentów systemu.

Zabezpieczenia powiązane: CA-7, SI-4.

(3) USUWANIE USTEREK | CZAS DO USUNIĘCIA USTERKI / STANDARDY DZIAŁAŃ NAPRAWCZYCH

(a) Mierzenie czasu pomiędzy identyfikacją usterki, a jej usunięciem; oraz

(b) Ustanowienie wzorców do podejmowania działań korygujących [*Realizacja: standardy zdefiniowane przez organizację*] w celu podjęcia działań naprawczych.

Omówienie: Organizacje określają średni czas potrzebny na usunięcie błędów systemowych od momentu ich zidentyfikowania, a następnie ustalają standardy organizacyjne (tj. ramy czasowe) pozwalające na podjęcie działań naprawczych. Wzorce mogą być ustalane na podstawie typu usterki lub wagi potencjalnej podatności, jeśli dana usterka może zostać wykorzystana.

Zabezpieczenia powiązane: Brak.

(4) USUWANIE USTEREK | AUTOMATYCZNE ŚCIEŻKI ZARZĄDZANIA NARZĘDZIAMI

Wykorzystanie zautomatyzowanych ścieżek zarządzania narzędziami umożliwiającymi usuwanie błędów w następujących komponentach systemu: [Realizacja: komponenty systemu zdefiniowane przez organizację].

Omówienie: Stosowanie zautomatyzowanych narzędzi wspomagających zarządzanie poprawkami pomaga zapewnić terminowość i kompleksowość wprowadzania poprawek do systemu.

Zabezpieczenia powiązane: Brak.

(5) USUWANIE USTEREK | AUTOMATYCZNE AKTUALIZACJE APLIKACJI / OPROGRAMOWANIA UKŁADOWEGO

Automatyczne instalowanie [*Realizacja: zdefiniowane przez organizację aktualizacje aplikacji i oprogramowania układowego istotne dla bezpieczeństwa*] w [*Realizacja: zdefiniowane przez organizację komponenty systemu*].

Omówienie: Ze względu na kwestie związane z integralnością i dostępnością systemu, organizacje uwzględniają metodologię wykonywania automatycznych aktualizacji. Organizacje równoważą potrzebę zapewnienia, że aktualizacje są instalowane tak szybko, jak to możliwe, z potrzebą utrzymania zarządzania

konfiguracją i zabezpieczeniami z uwzględnieniem wpływu na misję lub operacje, jaki mogą mieć automatyczne aktualizacje.

Zabezpieczenia powiązane: Brak.

(6) USUWANIE USTEREK | USUWANIE POPRZEDNICH WERSJI APLIKACJI / OPROGRAMOWANIA UKŁADOWEGO

Usuwanie poprzednich wersje [***Realizacja: zdefiniowane przez organizację aplikacje i składniki oprogramowania układowego***] **po zainstalowaniu zaktualizowanych wersji.**

Omówienie: Wcześniejsze wersje oprogramowania lub komponentów oprogramowania układowego, które nie zostaną usunięte z systemu po zainstalowaniu aktualizacji, mogą zostać wykorzystane przez osoby niepowołane. Niektóre produkty mogą automatycznie usuwać poprzednie wersje oprogramowania i oprogramowania sprzętowego z systemu.

Zabezpieczenia powiązane: Brak.

Referencje: [OMB A-130], [FIPS 140-3], [FIPS 186-4], [NIST SP 800-39], [NIST SP 800-40], [NIST SP 800-128], [IR 7788].

SI-3 ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM

Zabezpieczenie podstawowe:

a. Wdrożenie [*Wybór (jeden lub więcej): sygnaturowych; niesygnaturowych*] mechanizmów ochrony przed złośliwym kodem w punktach wejścia i wyjścia do/z systemu, w celu wykrywania i wyeliminowania złośliwego kodu;

b. Automatyczna aktualizacja mechanizmów ochrony przed złośliwym kodem w miarę pojawiania się nowych wersji, zgodnie z polityką i procedurami zarządzania konfiguracją organizacyjną;

c. Konfigurowanie mechanizmów ochrony przed złośliwym kodem poprzez:

   1. Wykonywanie okresowych skanów systemu [*Realizacja: częstotliwość zdefiniowana przez organizację*] oraz skanowanie w czasie rzeczywistym plików ze źródeł zewnętrznych w punkcie [*Wybór (jeden lub więcej): punkt końcowy; punkty wejścia i wyjścia z sieci*] *podczas* pobierania, otwierania lub wykonywania plików zgodnie z polityką organizacyjną; oraz

   2. [*Wybór (jeden lub więcej): blokowanie złośliwego kodu; poddawanie złośliwego kodu kwarantannie; podejmowanie* [*Realizacja: działania określone przez organizację*]]*;* oraz wysłanie ostrzeżenia do [*Realizacja: personel lub role określone przez organizację*] w odpowiedzi na wykrycie złośliwego kodu; oraz

d. Rozwiązywanie problemów otrzymywania fałszywych alarmów podczas wykrywania i usuwania złośliwego kodu oraz wynikającego z tego potencjalnego wpływu na dostępność systemu.

Omówienie: Punkty wejścia i wyjścia do/z systemu obejmują zapory sieciowe, serwery zdalnego dostępu, stacje robocze, serwery poczty elektronicznej, serwery WWW, serwery proxy, notebooki i urządzenia mobilne. Złośliwy kod obejmuje wirusy, robaki, konie trojańskie i oprogramowanie szpiegujące. Złośliwy kod może być również zakodowany w różnych formatach zawartych w skompresowanych lub

ukrytych plikach lub zamaskowany w plikach przy użyciu technik takich jak steganografia[101]. Złośliwy kod może zostać wprowadzony do systemów na różne sposoby, w tym za pośrednictwem poczty elektronicznej, sieci WWW oraz przenośnych nośników danych. Wprowadzanie złośliwego kodu odbywa się poprzez wykorzystywanie podatności systemu na ataki. Istnieje wiele technologii i metod mających na celu ograniczenie lub wyeliminowanie skutków działania złośliwego kodu.

Mechanizmy ochrony przed złośliwym kodem obejmują zarówno technologie oparte na sygnaturach, jak i nieoparte na sygnaturach. Mechanizmy wykrywania nieoparte na sygnaturach obejmują techniki sztucznej inteligencji, które wykorzystują metody i techniki heurystyczne[102] do wykrywania, analizowania i opisywania cech lub zachowania złośliwego kodu oraz do zabezpieczania przed takim kodem, dla którego nie istnieją jeszcze sygnatury lub dla którego istniejące sygnatury mogą nie być skuteczne. Złośliwy kod, dla którego aktywne sygnatury jeszcze nie istnieją lub mogą być nieskuteczne, obejmuje złośliwy kod polimorficzny (tj. kod, który zmienia sygnatury podczas replikacji). Mechanizmy nieoparte na sygnaturach obejmują również technologie oparte na reputacji. Oprócz powyższych technologii, skuteczne w zapobieganiu wykonywania nieautoryzowanego kodu może być wszechobecne zarządzanie konfiguracją, kompleksowe kontrole integralności oprogramowania oraz oprogramowanie zapobiegające wyłudzaniu danych. Złośliwy kod może być obecny w dostępnym na rynku oprogramowaniu, jak również w oprogramowaniu tworzonym

[101] Nauka o komunikacji w taki sposób, by obecność komunikatu nie mogła zostać wykryta. W odróżnieniu od kryptografii (gdzie obecność komunikatu nie jest negowana, natomiast jego treść jest niejawna) steganografia próbuje ukryć fakt prowadzenia komunikacji. Techniki steganograficzne stosowane są także do znakowania danych cyfrowych.

[102] Ogół sposobów i reguł postępowania służących podejmowaniu najwłaściwszych decyzji w skomplikowanych sytuacjach, wymagających analizy dostępnych informacji, a także przewidywania zjawisk przyszłych; oparte na twórczym myśleniu i kombinacjach logicznych.

na zamówienie i może zawierać bomby logiczne, furtki (ang. back doors) i inne rodzaje ataków, które mogą wpływać na misję organizacji i jej funkcje biznesowe.

W sytuacjach, w których złośliwy kod nie może zostać wykryty za pomocą metod lub technologii wykrywania, organizacje polegają na innych rodzajach zabezpieczeń, w tym na praktykach bezpiecznego kodowania, zarządzaniu i zabezpieczaniu konfiguracji, zaufanych procesach zamówień oraz praktykach monitorowania w celu zapewnienia, że oprogramowanie nie wykonuje funkcji innych niż zamierzone. Organizacje mogą określić, że w odpowiedzi na wykrycie złośliwego kodu uzasadnione jest podjęcie zróżnicowanych działań. Na przykład, organizacje mogą zdefiniować działania w odpowiedzi na wykrycie złośliwego kodu podczas okresowego skanowania, wykrycie złośliwego pobierania plików lub wykrycie działania złośliwego podczas próby otwarcia lub wykonania plików.

Zabezpieczenia powiązane: AC-4, AC-19, CM-3, CM-8, IR-4, MA-3, PL-9, RA-5, SC-7, SC-23, SC-26, SC- 28, SC-44, SI-2, SI-4, SI-7, SI-8, SI-15.

Zabezpieczenia rozszerzone:

(1) ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | ZARZĄDZANIE CENTRALNE

[Wycofane: Włączone do PL-9].

(2) ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | AUTOMATYCZNE AKTUALIZACJE

[Wycofane: Włączone do SI-3].

(3) ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | NIEUPRZYWILEJOWANI UŻYTKOWNICY

[Wycofane: Włączone do AC-6(10)].

(4) ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | AKTUALIZACJE WYŁĄCZNIE PRZEZ UPRAWNIONYCH UŻYTKOWNIKÓW

Aktualizowanie mechanizmów ochrony przed złośliwym kodem tylko na polecenie personelu wyznaczonego przez kierownika jednostki organizacyjnej.

Omówienie: Mechanizmy ochrony przed złośliwym kodem są zazwyczaj klasyfikowane, jako oprogramowanie związane z bezpieczeństwem i jako takie są aktualizowane wyłącznie przez personel organizacji posiadający odpowiednie uprawnienia dostępu.

Zabezpieczenia powiązane: CM-5.

(5) ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | PRZENOŚNE URZĄDZENIA MAGAZYNUJĄCE

[Wycofane: Włączone do MP-7].

(6) ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | TESTOWANIE I WERYFIKACJA

(a) Testowanie mechanizmów ochrony przed złośliwym kodem [*Realizacja: częstotliwość zdefiniowana przez organizację*] poprzez wprowadzenie znanego łagodnego, nierozprzestrzeniającego się przypadku testowego do systemu; oraz

(b) Włączanie wyników analizy złośliwego kodu do organizacyjnych procesów reagowania na incydenty i usuwania wad.

Omówienie: Brak.

Zabezpieczenia powiązane: CA-2, CA-7, RA-5.

(7) ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | WYKRYWANIE BEZSYGNATUROWE

[Wycofane: Włączone do SI-3].

(8) ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | WYKRYWANIE NIEAUTORYZOWANYCH KOMEND

(a) Wykrywanie następujących nieautoryzowanych poleceń systemu operacyjnego za pośrednictwem interfejsu programowania aplikacji jądra[103]

[103] Aplikacja kernel.

w [***Realizacja: zdefiniowane przez organizację komponenty sprzętowe systemu***]***:*** [***Realizacja: zdefiniowane przez organizację nieautoryzowane polecenia systemu operacyjnego***]**; oraz**

(b) [***Wybór (jeden lub więcej): wydawanie ostrzeżeń; kontrolowanie wykonania polecenia; uniemożliwianie wykonania polecenia***]**.**

Omówienie: Wykrywanie nieautoryzowanych poleceń może być stosowane do krytycznych interfejsów innych niż oparte na jądrze, w tym interfejsów z maszynami wirtualnymi i aplikacjami uprzywilejowanymi. Nieautoryzowane polecenia systemu operacyjnego obejmują polecenia dla funkcji jądra z procesów systemowych, które nie są zaufane do inicjowania takich poleceń, a także polecenia dla funkcji jądra, które są podejrzane, mimo, że polecenia tego typu są uzasadnione dla procesów, które mają być inicjowane. Organizacje mogą definiować złośliwe polecenia, które mają być wykrywane przez kombinację typów poleceń, klas poleceń lub określonych instancji poleceń. Organizacje mogą również zdefiniować komponenty sprzętowe według typu komponentów, klas komponentów, lokalizacji komponentów w sieci lub ich kombinacji. Organizacje mogą wybrać różne akcje dla różnych typów, klas lub przykładów złośliwych poleceń.

Zabezpieczenia powiązane: AU-2, AU-6, AU-12.

(9) ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | ZDALNE POLECENIA AUTENTYFIKACYJNE

[Wycofane: Włączone do AC-17(10)].

(10) ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | ANALIZA KODU ZŁOŚLIWEGO

(a) Stosowanie następujących narzędzi i technik analizy charakterystyki i zachowania złośliwego kodu: [***Realizacja: narzędzia i techniki zdefiniowane przez organizację***]***;*** **oraz**

(b) Włączenie wyników analizy złośliwego kodu do organizacyjnych procesów reagowania na incydenty i usuwania wad.

Omówienie: Wykorzystanie narzędzi do analizy złośliwego kodu zapewnia organizacjom bardziej dogłębne zrozumienie rzemiosła przeciwników (tj. taktyki, technik i procedur) oraz funkcjonalności i przeznaczenia konkretnych przypadków złośliwego kodu. Zrozumienie charakterystyki złośliwego kodu ułatwia organizacjom skuteczne reagowanie na obecne i przyszłe zagrożenia. Organizacje mogą przeprowadzać analizy złośliwego kodu stosując techniki inżynierii wstecznej lub monitorując zachowanie wykonującego się kodu.

Zabezpieczenia powiązane: Brak.

Referencje: [NIST SP 800-83], [NIST SP 800-125B], [NIST SP 800-177].

SI-4 MONITOROWANIE SYSTEMU

Zabezpieczenie podstawowe:

a. Monitowanie systemu w celu wykrywania:

   1. Ataków i wskaźników potencjalnych ataków zgodnie z następującymi celami monitoringu: [*Realizacja: cele monitoringu określone przez organizację*]*;* oraz

   2. Nieautoryzowanych połączeń lokalnych, sieciowych i zdalnych;

b. Identyfikowanie nieuprawnionego korzystania z systemu poprzez wykorzystywanie następujących technik i metod: [*Realizacja: techniki i metody zdefiniowane przez organizację*]*;*

c. Uruchamianie wewnętrznych funkcji monitorowania lub wdrażanie urządzeń monitorujących:

   1. Długofalowo, w celu gromadzenia istotnych informacji ustalonych przez organizację; oraz

   2. W lokalizacjach doraźnych, w celu śledzenia określonych rodzajów transakcji będących przedmiotem zainteresowania organizacji;

d. Analizowanie wykrytych zdarzeń i anomalii;

e. Dostosowywanie poziomu aktywności monitorowania systemu w przypadku zmiany ryzyka dotyczącego operacji i aktywów organizacji, osób, innych organizacji lub Państwa;

f. Uzyskiwanie opinii prawnych dotyczących działań związanych z monitorowaniem systemu; oraz

g. Dostarczanie [*Realizacja: zdefiniowane przez organizację informacje dotyczące monitorowania systemu*] do [*Realizacja: personel lub role zdefiniowane przez organizację*] [*Wybór (jeden lub więcej): w miarę potrzeb*; [*Realizacja: częstotliwość zdefiniowana przez organizację*]]

Omówienie: Monitorowanie systemu obejmuje monitorowanie zarówno zewnętrzne, jak i wewnętrzne. Monitorowanie zewnętrzne obejmuje obserwację zdarzeń zachodzących na zewnętrznych interfejsach systemu. Monitorowanie wewnętrzne obejmuje obserwację zdarzeń zachodzących wewnątrz systemu. Organizacje monitorują systemy poprzez obserwację działań audytowych w czasie rzeczywistym lub poprzez obserwację innych cech systemu, takich jak wzorce dostępu, charakterystyka dostępu i inne działania. Cele monitorowania wyznaczają kierunek i wskazują sposób określania zdarzeń. Możliwości monitorowania systemu są osiągane za pomocą różnych narzędzi i technik, w tym systemów wykrywania i zapobiegania włamaniom, oprogramowania do ochrony przed złośliwym kodem, narzędzi skanujących, oprogramowania do monitorowania zapisów audytu oraz oprogramowania do monitorowania sieci.

W zależności od architektury bezpieczeństwa, rozmieszczenie i konfiguracja urządzeń monitorujących może mieć wpływ na przepustowość na kluczowych granicach wewnętrznych i zewnętrznych, a także w innych lokalizacjach w sieci, ze względu na wprowadzenie opóźnień w przepustowości sieci. Jeśli zarządzanie przepustowością jest wymagane, takie urządzenia są strategicznie rozmieszczone i wdrożone, jako część ustalonej architektury bezpieczeństwa w całej organizacji. Strategiczne lokalizacje urządzeń monitorujących obejmują wybrane lokalizacje brzegowe oraz w pobliżu kluczowych serwerów i grup serwerów, które obsługują krytyczne aplikacje. Urządzenia monitorujące są zwykle instalowane na zarządzanych interfejsach powiązanych z zabezpieczeniami SC-7 i AC-17. Zbierane informacje są funkcją organizacyjnych celów monitorowania oraz zdolności systemów do wspierania tych celów. Szczególne rodzaje operacji będące przedmiotem zainteresowania obejmują protokół przesyłania dokumentów hipertekstowych (ang. Hypertext Transfer Protocol - HTTP), który omija serwery proxy HTTP. Monitorowanie systemu jest integralną częścią organizacyjnych programów ciągłego monitorowania i reagowania na incydenty, a dane wyjściowe z monitorowania systemu służą jako dane wejściowe do tych programów. Wymagania dotyczące monitorowania systemu,

w tym zapotrzebowanie na określone rodzaje monitorowania systemu, znajdują odniesienie w innych zabezpieczeniach (np. AC-2g, AC-2(7), AC-2(12)(a), AC-17(1), AU-13, AU-13(1), AU-13(2), CM-3f, CM-6d, MA-3a, MA-4a, SC-5(3)(b), SC-7a, SC-7(24)(b), S.C.-18b, SC-43b). Dostosowanie poziomów monitorowania systemu opiera się na informacjach pochodzących od organów ścigania, informacjach wywiadowczych lub innych źródłach informacji. Legalność działań związanych z monitorowaniem systemu opiera się na obowiązujących przepisach, rozporządzeniach, dyrektywach, politykach, standardach i wytycznych.

Zabezpieczenia powiązane: AC-2, AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, AU-13, AU-14, CA-7, CM-3, CM-6, CM-8, CM-11, IA-10, IR-4, MA-3, MA-4, PL-9, PM-12, RA-5, RA-10, SC-5, SC-7, SC-18, SC-26, SC-31, SC-35, SC-36, SC-37, SC-43, SI-3, SI-6, SI-7, SR-9, SR-10.

Zabezpieczenia rozszerzone:

(1) MONITOROWANIE SYSTEMU | SYSTEM WYKRYWANIA WŁAMAŃ

Skonfigurowanie i podłączenie poszczególnych narzędzi w system wykrywania włamań obejmujący cały systemu informatyczny.

Omówienie: Połączenie poszczególnych narzędzi do wykrywania włamań w jeden system wykrywania włamań zapewnia dodatkowy zasięg i skuteczne możliwości wykrywania. Informacje zawarte w jednym narzędziu do wykrywania włamań mogą być rozpowszechniane w całej organizacji, dzięki czemu możliwości wykrywania w całym systemie są bardziej niezawodne i wydajne.

Zabezpieczenia powiązane: Brak.

(2) MONITOROWANIE SYSTEMU | AUTOMATYCZNE NARZĘDZIA I MECHANIZMY ANALIZY W CZASIE RZECZYWISTYM

Stosowanie zautomatyzowanych narzędzi i mechanizmów wspomagających analizę zdarzeń w czasie zbliżonym do rzeczywistego.

Omówienie: Zautomatyzowane narzędzia i mechanizmy obejmują narzędzia i mechanizmy monitorowania zdarzeń występujących w hoście, w sieci, podczas transportu lub przechowywaniu lub też technologie zarządzania informacjami i zdarzeniami związanymi z bezpieczeństwem (*ang. security information and event management - SIEM*), które zapewniają analizę w czasie rzeczywistym alarmów i powiadomień generowanych przez systemy organizacyjne. Zautomatyzowane techniki monitorowania mogą powodować niezamierzone zagrożenia prywatności, ponieważ zautomatyzowane środki bezpieczeństwa mogą łączyć się z zewnętrznymi lub w inny sposób niepowiązanymi systemami. Dopasowywanie zapisów między tymi systemami może tworzyć powiązania powodujące niezamierzone konsekwencje. Organizacje oceniają i dokumentują te zagrożenia w swojej ocenie wpływu na prywatność i podejmują decyzje zgodne z planem programu ochrony prywatności.

Zabezpieczenia powiązane: PM-23, PM-25.

(3) MONITOROWANIE SYSTEMU | AUTOMATYCZNA INTEGRACJA NARZĘDZI I MECHANIZMÓW

Stosowanie zautomatyzowanych narzędzi i mechanizmów do integracji narzędzi i mechanizmów wykrywania włamań z mechanizmami kontroli dostępu i kontroli przepływu.

Omówienie: Wykorzystanie zautomatyzowanych narzędzi i mechanizmów do integracji narzędzi i mechanizmów wykrywania włamań z mechanizmami kontroli dostępu i przepływu ułatwia szybką reakcję na ataki poprzez umożliwienie rekonfiguracji mechanizmów wspierających izolację i eliminację ataków.

Zabezpieczenia powiązane: PM-23, PM-25.

(4) MONITOROWANIE SYSTEMU | WEJŚCIOWY / WYJŚCIOWY RUCH TELEKOMUNIKACYJNY

(a) Określenie kryteriów dla nietypowych lub nieautoryzowanych działań lub warunków dla przychodzącego i wychodzącego ruchu telekomunikacyjnego;

(b) Monitorowanie telekomunikacyjnego ruchu przychodzącego i wychodzącego [Realizacja: *zdefiniowana przez organizację częstotliwość*] pod kątem [*Realizacja: zdefiniowane przez organizację nietypowe lub nieautoryzowane działania lub warunki*].

Omówienie: Nietypowe lub nieautoryzowane działania lub warunki związane z telekomunikacyjnym ruchem przychodzącym i wychodzącym do/z systemu obejmują ruch wewnętrzny, który wskazuje na obecność złośliwego kodu lub na nieautoryzowane użycie dozwolonego kodu lub danych uwierzytelniających w systemach organizacyjnych lub rozprzestrzeniających się między komponentami systemu; wymianę sygnalizacji z systemami zewnętrznymi; oraz nieuprawniony eksport informacji. Dowody obecności złośliwego kodu lub nieuprawnionego użycia legalnego kodu lub danych uwierzytelniających są wykorzystywane do identyfikacji potencjalnie zagrożonych systemów lub komponentów systemu.

Zabezpieczenia powiązane: Brak.

(5) MONITOROWANIE SYSTEMU | ALERTY SYSTEMOWE

Ostrzeganie [*Realizacja: zdefiniowany przez organizację personel lub role*] w przypadku wystąpienia następujących oznak naruszenia lub potencjalnego naruszenia: [*Realizacja: wskaźniki naruszenia zdefiniowane przez organizację*].

Omówienie: Alerty mogą być generowane z różnych źródeł, w tym z zapisów audytowych lub danych wejściowych pochodzących z mechanizmów ochrony przed złośliwym kodem, mechanizmów wykrywania lub zapobiegania włamaniom lub urządzeń brzegowych, takich jak zapory ogniowe, bramy i routery. Alerty

mogą być zautomatyzowane i mogą być przekazywane telefonicznie, za pomocą poczty elektronicznej lub wiadomości tekstowych. Personel organizacyjny znajdujący się na liście powiadomień o alarmach może obejmować administratorów systemów, właścicieli misji lub firm, właścicieli systemów, właścicieli informacji/władających informacją, SAISO, SAOP, SSO lub SPO.[104] W przeciwieństwie do alertów generowanych przez system, alerty generowane przez organizację (patrz: zabezpieczenie rozszerzone SI-4(12)) koncentrują się na źródłach informacji spoza systemu, takich jak raporty o podejrzanych działaniach i raporty o potencjalnych zagrożeniach wewnętrznych.

Zabezpieczenia powiązane: AU-4, AU-5, PE-6.

(6) MONITOROWANIE SYSTEMU | OGRANICZANIE NIEUPRZYWILEJOWANYCH UŻYTKOWNIKÓW

[Wycofane: Włączone do AC-6(10)].

(7) MONITOROWANIE SYSTEMU | AUTOMATYCZNA ODPOWIEDŹ NA PODEJRZANE ZDARZENIA

(a) Powiadamianie o wykrytych podejrzanych zdarzeniach [***Realizacja: zdefiniowany przez organizację personel reagowania na incydenty (zidentyfikowany na podstawie nazwy i/lub roli)***]**; oraz**

(b) Podejmowanie następujących działań po wykryciu: [*Realizacja: zdefiniowane przez organizację działania najmniej zakłócające pracę systemu, realizowane w celu wyeliminowania podejrzanych zdarzeń*].

Omówienie: Działania najmniej zakłócające pracę obejmują inicjowanie żądań powodujących reakcje personelu.

Zabezpieczenia powiązane: Brak.

[104] Patrz: NSC 800-37; NSC 7298.

(8) MONITORING SYSTEMU | OCHRONA INFORMACJI MONITORUJĄCYCH

[Wycofane: Włączone do SI-4].

(9) MONITOROWANIE SYSTEMU | TESTOWANIE NARZĘDZI I MECHANIZMÓW MONITORUJĄCYCH

Testowanie narzędzi i mechanizmów do monitorowania włamań [***Realizacja: częstotliwość określona przez organizację***]**.**

Omówienie: Testowanie narzędzi i mechanizmów do monitorowania włamań jest niezbędne do zapewnienia prawidłowego ich działania oraz dalszej realizacji celów monitoringu organizacji. Częstotliwość i zakres testowania zależy od rodzaju stosowanych przez organizacje narzędzi i mechanizmów oraz metod ich wdrażania.

Zabezpieczenia powiązane: Brak.

(10) MONITOROWANIE SYSTEMU | INSPEKCJA ZASZYFROWANYCH KOMUNIKATÓW

Zapewnienie, że [*Realizacja: zdefiniowany przez organizację zaszyfrowany ruch telekomunikacyjny*] jest widoczny przez [*Realizacja: narzędzia monitorowania systemu informatycznego zdefiniowane przez organizację*].

Omówienie: Organizacje równoważą potrzebę szyfrowania ruchu telekomunikacyjnego w celu ochrony poufności danych z potrzebą utrzymania widoczności takiego ruchu z perspektywy monitorowania. Organizacje określają, czy wymóg widoczności dotyczy wewnętrznego ruchu zaszyfrowanego, ruchu zaszyfrowanego kierowanego do zewnętrznych miejsc docelowych, czy określonego podzbioru typów ruchu.

Zabezpieczenia powiązane: Brak.

(11) MONITOROWANIE SYSTEMU | ANALIZA ANOMALII RUCHU TELEKOMUNIKACYJNEGO

Analizowanie telekomunikacyjnego ruch wychodzącego na zewnętrznych interfejsach systemu i wybranych [***Realizacja: zdefiniowane przez organizację punkty wewnętrzne w systemie***] **w celu wykrycia anomalii.**

Omówienie: Zdefiniowane organizacyjnie punkty wewnętrzne obejmują podsieci i podsystemy. Anomalie w systemach organizacyjnych obejmują duże transfery plików, długotrwające połączenia, próby dostępu do informacji z nieznanych lokalizacji, stosowanie nietypowych protokołów i portów, stosowanie niemonitorowanych protokołów sieciowych (np. korzystanie z IPv6 podczas przejścia na IPv4) oraz próby komunikacji z podejrzanymi złośliwymi adresami zewnętrznymi.

Zabezpieczenia powiązane: Brak.

(12) MONITOROWANIE SYSTEMU | AUTOMATYCZNE ALERTY GENEROWANE PRZEZ ORGANIZACJĘ

Ostrzeganie [***Realizacja: personel lub role określone przez organizację***] ***przy*** **użyciu** [***Realizacja: zautomatyzowane mechanizmy określone przez organizację***] ***w*** **przypadku wystąpienia następujących niewłaściwych lub nietypowych działań mających wpływ na bezpieczeństwo lub prywatność:** [***Realizacja: czynności określone przez organizację, które powodują uruchomienie alarmu***]**.**

Omówienie: Personel organizacyjny znajdujący się na liście powiadomień alarmowych systemu obejmuje administratorów systemu, właścicieli misji lub firm, właścicieli systemu, SAISO, SAOP, SSO lub SPO.[105] Automatyczne alerty to alerty bezpieczeństwa generowane przez organizacje i przekazywane za pomocą

[105] Patrz: NSC 800-37; NSC 7298.

środków automatycznych. Źródła alertów generowanych przez organizację opierają się na innych elementach, takich jak raporty o podejrzanych działaniach i raporty o potencjalnych zagrożeniach wewnętrznych. W przeciwieństwie do alertów generowanych przez organizację, alerty generowane przez system (patrz: zabezpieczenie rozszerzone SI-4(5)) koncentrują się na źródłach informacji, znajdujących się wewnątrz systemów, takich jak zapisy audytowe.

Zabezpieczenia powiązane: Brak.

(13) MONITOROWANIE SYSTEMU | ANALIZA MODELU RUCHU / ZDARZEŃ TELEKOMUNIKACYJNYCH

(a) Analizowanie ruchu telekomunikacyjnego i schematów zdarzeń danego systemu;

(b) Opracowywanie profili reprezentujących typowe wzorce ruchu i zdarzeń; oraz

(c) Wykorzystywanie profili ruchu / zdarzeń do przystosowywania urządzeń monitorujących system, celem zmniejszenia liczby fałszywych i rzeczywistych alarmów.

Omówienie: Identyfikacja i zrozumienie wspólnych wzorców ruchu telekomunikacyjnego i zdarzeń pomaga organizacjom w dostarczaniu użytecznych informacji do urządzeń monitorujących system, co pozwala na bardziej efektywne identyfikowanie podejrzanego lub anomalnego ruchu i zdarzeń w momencie ich wystąpienia. Takie informacje mogą pomóc w zmniejszeniu liczby fałszywych pozytywów i fałszywych negatywów podczas monitorowania systemu.

Zabezpieczenia powiązane: Brak.

(14) MONITOROWANIE SYSTEMU | WYKRYWANIE ATAKÓW BEZPRZEWODOWYCH

Stosowanie bezprzewodowego systemu wykrywania włamań i napadów do identyfikowania nieautoryzowanych urządzeń bezprzewodowych oraz wykrywania prób ataków i potencjalnych zagrożeń / naruszeń systemu.

Omówienie: Sygnały bezprzewodowe mogą promieniować poza obiekty organizacji. Organizacje proaktywnie wyszukują nieautoryzowane połączenia bezprzewodowe, w tym przeprowadzają dokładne skanowanie w poszukiwaniu nieautoryzowanych punktów dostępu bezprzewodowego. Skanowanie bezprzewodowe nie ogranicza się tylko do obszarów w obrębie obiektów zawierających systemy, ale obejmuje również obszary poza obiektami. Ma to na celu sprawdzenia, czy nieuprawnione punkty dostępu bezprzewodowego nie są podłączone do systemów organizacji.

Zabezpieczenia powiązane: AC-18, IA-3.

(15) MONITOROWANIE SYSTEMU | TELEKOMUNIKACJA BEZPRZEWODOWA / PRZEWODOWA

Stosowanie systemu wykrywania włamań do monitorowania ruchu telekomunikacyjnego generowanego przez urządzenia bezprzewodowe i nawiązywania połączeń z sieci bezprzewodowych do przewodowych.

Omówienie: Sieci bezprzewodowe są z natury mniej bezpieczne niż sieci przewodowe. Na przykład sieci bezprzewodowe są bardziej podatne na podsłuchy lub analizę ruchu niż sieci przewodowe. W przypadku komunikacji między sieciami bezprzewodowymi i przewodowymi, sieć bezprzewodowa może stać się portem wejścia do sieci przewodowej. Biorąc pod uwagę większe możliwości nieautoryzowanego dostępu do sieci za pośrednictwem punktów dostępu bezprzewodowego w porównaniu z nieautoryzowanym dostępem do sieci przewodowej z fizycznych granic systemu, może zaistnieć konieczność dodatkowego monitorowania ruchu przechodzącego między sieciami bezprzewodowymi i przewodowymi w celu wykrycia szkodliwych działań.

Wykorzystanie systemów wykrywania włamań do monitorowania ruchu w sieciach bezprzewodowych pomaga upewnić się, że ruch ten nie zawiera złośliwego kodu przed przejściem do sieci przewodowej.

Zabezpieczenia powiązane: AC-18.

(16) MONITOROWANIE SYSTEMU | KORELOWANIE INFORMACJI MONITORUJĄCYCH

Korelowanie informacji z poszczególnych narzędzi monitorowania stosowanych w całym systemie.

Omówienie: Korelacja informacji z różnych narzędzi i mechanizmów monitorowania systemu może zapewnić bardziej kompleksowy obraz aktywności systemu. Powiązanie narzędzi i mechanizmów monitorowania systemu, które zazwyczaj działają w oderwaniu od siebie - w tym oprogramowania zabezpieczającego przed złośliwym kodem, monitorowania hostów i monitorowania sieci - może zapewnić obraz monitorowania w całej organizacji i może ujawnić niewidoczne w inny sposób wzorce ataku. Zrozumienie możliwości i ograniczeń różnych narzędzi i mechanizmów monitorujących oraz sposobów maksymalnego wykorzystania informacji generowanych przez te narzędzia i mechanizmy może pomóc organizacji w opracowaniu, obsłudze i utrzymaniu skutecznych programów monitorujących. Korelacja informacji z monitoringu jest szczególnie istotna przy przechodzeniu ze starszych do nowszych technologii (np. przejście z protokołów sieciowych IPv4 na IPv6).

Zabezpieczenia powiązane: AU-6.

(17) MONITORING SYSTEMU | ZINTEGROWANA ŚWIADOMOŚĆ SYTUACYJNA

Korelowanie informacji z monitorowania działań fizycznych, cyberprzestrzeni i powiązanych z łańcuchem dostaw w celu osiągnięcia zintegrowanej świadomości sytuacyjnej w całej organizacji.

Omówienie: Korelacja informacji pochodzących z monitorowania bardziej zróżnicowanego zbioru źródeł informacji pomaga w osiągnięciu zintegrowanej

świadomości sytuacyjnej. Zintegrowana świadomość sytuacyjna wynikająca z połączenia działań w zakresie monitorowania fizycznego, cyberprzestrzeni i łańcucha dostaw zwiększa zdolność organizacji do szybszego wykrywania wyrafinowanych ataków oraz badania metod i technik wykorzystywanych do przeprowadzania takich ataków. W przeciwieństwie do zabezpieczenia rozszerzonego SI-4(16), które koreluje różne informacje dotyczące monitorowania cyberprzestrzeni, zintegrowana świadomość sytuacyjna ma na celu korelację monitorowania poza cyberdomeną. Korelacja informacji monitorujących pochodzących z wielu działań może pomóc w ujawnieniu ataków na organizacje, które działają w oparciu o wiele wektorów ataku.

Zabezpieczenia powiązane: AU-16, PE-6, SR-2, SR-4, SR-6.

(18) MONITOROWANIE SYSTEMU | ANALIZA RUCHU / ZAPOBIEGANIE EKSFILTRACJI

Analizowanie telekomunikacyjnego ruch wychodzącego na urządzeniach brzegowych systemu (tj. na obrzeżach systemu) oraz w następujących punktach wewnętrznych w celu wykrycia ukrytej eksfiltracji informacji: [***Realizacja: zdefiniowane przez organizację punkty wewnętrzne w systemie***]**.**

Omówienie: Zdefiniowane organizacyjnie punkty wewnętrzne obejmują podsieci i podsystemy. Ukryte środki, które mogą być wykorzystane do wyprowadzenia informacji, obejmują steganografię.

Zabezpieczenia powiązane: Brak.

(19) MONITOROWANIE SYSTEMU | RYZYKO ZE STRONY OSÓB

Wdrożenie [***Realizacja: zdefiniowany przez organizację dodatkowe monitorowanie***] **osób, które zostały zidentyfikowane przez** [***Realizacja: zdefiniowane przez organizację źródła***]**, jako stwarzające zwiększony poziom ryzyka.**

Omówienie: Oznaki zwiększonego ryzyka ze strony osób można uzyskać z różnych źródeł, w tym z rejestrów osobowych, agencji wywiadowczych, organów ścigania

i innych. Monitorowanie osób jest koordynowane z kierownictwem, radcą prawnym, personelem ds. bezpieczeństwa, prywatności i zasobów ludzkich, którzy prowadzą taki monitoring. Monitorowanie jest prowadzone zgodnie z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi.

Zabezpieczenia powiązane: Brak.

(20) MONITOROWANIE SYSTEMU | UPRZYWILEJOWANI UŻYTKOWNICY

Wdrożenie do monitorowania uprzywilejowanych użytkowników następującego dodatkowego zabezpieczenia: [***Realizacja: zdefiniowane przez organizację dodatkowe monitorowanie***]**.**

Omówienie: Użytkownicy uprzywilejowani mają dostęp do informacji bardziej wrażliwych, w tym informacji związanych z bezpieczeństwem, niż ogół populacji użytkowników. Dostęp do takich informacji oznacza, że uprzywilejowani użytkownicy mogą potencjalnie wyrządzić większe szkody systemom i organizacjom niż nieuprzywilejowani użytkownicy. W związku z tym wdrożenie dodatkowego monitorowania uprzywilejowanych użytkowników pomaga zapewnić, że organizacje będą mogły jak najszybciej zidentyfikować złośliwe działania i podjąć odpowiednie środki zaradcze.

Zabezpieczenia powiązane: AC-18.

(21) MONITOROWANIE SYSTEMU | OKRESY PRÓBNE

Wdrożenie następującego dodatkowego monitoringu osób podczas [***Realizacja: zdefiniowany przez organizację okres próbny***]**:** ***[Realizacja: określony przez organizację dodatkowy monitoring]*.**

Omówienie: W okresie próbnym pracownicy nie mają statusu stałego zatrudnienia w organizacji. Bez takiego statusu lub dostępu do informacji, które znajdują się w systemie, dodatkowy monitoring może pomóc w identyfikacji wszelkich potencjalnie złośliwych działań lub niewłaściwych zachowań.

Zabezpieczenia powiązane: AC-18.

(22) MONITOROWANIE SYSTEMU | NIEAUTORYZOWANE USŁUGI SIECIOWE

(a) Wykrywanie usług sieciowych, które nie zostały autoryzowane lub zatwierdzone przez [***Realizacja: procesy autoryzacji lub zatwierdzania zdefiniowane przez organizację***]***;*** **oraz**

(b) W przypadku wykrycia nieautoryzowanych usług sieciowych [Wybór (jeden lub więcej): Przeprowadzenie audytu; Alarmowanie [Realizacja: zdefiniowany przez organizację personel lub role]].

Omówienie: Nieautoryzowane lub niezatwierdzone usługi sieciowe obejmują usługi w architekturach zorientowanych na usługi, którym brakuje organizacyjnej weryfikacji lub walidacji i które w związku z tym mogą być zawodne lub służyć, jako złośliwe zagrożenia dla obowiązujących usług.

Zabezpieczenia powiązane: CM-7.

(23) MONITOROWANIE SYSTEMU | KOMPUTER GŁÓWNY (HOST)

Wdrożenie następujących mechanizmów monitorowania opartych na hostach w [***Realizacja: zdefiniowane przez organizację komponenty systemu***]**: [Realizacja: zdefiniowane przez** ***organizację mechanizmy monitorowania oparte na hostach***]

Omówienie: Monitorowanie oparte na komputerze głównym zbiera informacje o hoście (lub systemie, w którym się znajduje). Komponenty systemu, w których może być zaimplementowane monitorowanie oparte na hoście, obejmują serwery, notebooki i urządzenia mobilne. Organizacje mogą rozważyć zastosowanie mechanizmów monitorowania hosta pochodzących od wielu producentów lub dostawców.

Zabezpieczenia powiązane: AC-18, AC-19.

(24) MONITOROWANIE SYSTEMU | WSKAŹNIKI RYZYKA

Odkrywanie, gromadzenie i dystrybuowanie do [***Realizacja: personel lub role określone*** **przez organizację] wskaźników ryzyka dostarczanych przez** [***Realizacja: źródła określone przez organizację***]**.**

Omówienie: Wskaźniki ryzyka (*ang. indicators of compromise - IOC*) to kryminalistyczne artefakty pochodzące z włamań, które są identyfikowane w systemach organizacyjnych na poziomie hosta lub sieci. IOC dostarczają cennych informacji o systemach, które zostały naruszone. Wskaźniki IOC mogą obejmować tworzenie kluczowych wartości rejestru. IOC dla ruchu sieciowego obejmują ujednolicone formaty adresowania (*ang. Universal Resource Locator – URL*) lub elementy protokołu, które wskazują na złośliwe serwery poleceń i zabezpieczeń kodu. Szybka dystrybucja i przyjęcie IOC może poprawić bezpieczeństwo informacji poprzez skrócenie czasu, w którym systemy i organizacje są podatne na ten sam atak lub wykorzystanie istniejących luk. Wskaźniki zagrożenia, podpisy, taktyka, techniki, procedury i inne wskaźniki ujawnienia mogą być dostępne za pośrednictwem wspólnot rządowych i pozarządowych (Forum of Incident Response and Security Teams, United States Computer Emergency Readiness Team, Defense Industrial Base Cybersecurity Information Sharing Program oraz CERT Coordination Center) i sektorowych CSIRT.

Zabezpieczenia powiązane: AC-18.

(25) MONITOROWANIE SYSTEMU | ANALIZY OPTYMALIZACJI RUCHU SIECIOWEGO

Zapewnienie dostępu do informacji o ruchu sieciowym na zewnętrznych i kluczowych wewnętrznych interfejsach systemowych w celu optymalizacji skuteczności urządzeń monitorujących.

Omówienie: Ruch szyfrowany, asymetryczne architektury routingu, ograniczenia przepustowości i opóźnień oraz przechodzenie ze starszych na nowsze technologie (np. przejście z protokołu sieciowego IPv4 na IPv6) mogą powodować, że podczas analizy ruchu sieciowego organizacje mogą znaleźć się

w „martwych punktach". Zbieranie, odszyfrowywanie, wstępne przetwarzanie i dystrybucja tylko istotnego ruchu do urządzeń monitorujących może usprawnić wydajność i wykorzystanie urządzeń oraz zoptymalizować analizę ruchu.

Zabezpieczenia powiązane: Brak.

Referencje: [OMB A-130], [FIPS 140-3], [NIST SP 800-61], [NIST SP 800-83], [NIST SP 800-92], [NIST SP 800-94], [NIST SP 800-137].

SI-5 ALERTY BEZPIECZEŃSTWA, PORADY I DYREKTYWY

Zabezpieczenie podstawowe:

a. Otrzymywanie na bieżąco alarmów, porad i wytycznych dotyczących bezpieczeństwa systemu od [*Realizacja: zdefiniowane organizacje zewnętrzne*];

b. Generowanie wewnętrznych alarmów, porad i dyrektyw dotyczących bezpieczeństwa, jeśli zostanie to uznane za konieczne;

c. Rozpowszechnianie alertów bezpieczeństwa, porad i dyrektyw wśród: [*Wybór (jeden lub więcej):* [*Realizacja: personel lub role określone przez organizację*]; [*Realizacja: elementy organizacyjne określone przez organizację*]; [*Realizacja: zewnętrzne organizacje określone przez organizację*]]; oraz

d. Wdrożenie dyrektyw bezpieczeństwa zgodnie z ustalonymi ramami czasowymi lub powiadomienie organizacji wydającej o stopniu niezgodności.

Omówienie: CSIRT sektorowe generują alerty dotyczące bezpieczeństwa i zalecenia w celu utrzymania świadomości sytuacyjnej w cyberprzestrzeni. Dyrektywy dotyczące bezpieczeństwa są wydawane przez stosowne instytucje rządowe lub inne wyznaczone organizacje, które są odpowiedzialne i upoważnione do wydawania takich dyrektyw. Zgodność z dyrektywami bezpieczeństwa jest niezbędna ze względu na krytyczny charakter wielu z nich oraz potencjalne (natychmiastowe) negatywne skutki dla operacji organizacyjnych i majątku, osób, innych organizacji i Państwa, jeśli dyrektywy nie zostaną wdrożone w odpowiednim czasie. Do organizacji zewnętrznych należą partnerzy z łańcucha dostaw, misji zewnętrznych lub partnerzy biznesowi, zewnętrzni dostawcy usług oraz inne organizacje partnerskie lub wspierające.

Zabezpieczenia powiązane: PM-15, RA-5, SI-2.

Zabezpieczenia rozszerzone:

(1) ALERTY BEZPIECZEŃSTWA, PORADY I DYREKTYWY | AUTOMATYCZNE ALERTY I PORADY

Stosowanie zautomatyzowanych mechanizmów udostępniających alerty bezpieczeństwa i informacje doradcze w całej organizacji przy użyciu [***Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację***]**.**

Omówienie: Znacząca liczba wprowadzanych zmian w systemach organizacyjnych i środowiskach działania wymusza rozpowszechnianie informacji związanych z bezpieczeństwem wśród różnych jednostek organizacyjnych, które są bezpośrednio zaangażowane w realizację misji i funkcji biznesowych organizacji. Na podstawie informacji dostarczanych przez alerty i powiadomienia dotyczące bezpieczeństwa, zmiany mogą być wymagane na jednym lub więcej z trzech poziomów związanych z zarządzaniem ryzykiem, w tym na poziomie zarządzania, na poziomie misji i procesów biznesowych oraz na poziomie systemu informatycznego.

Zabezpieczenia powiązane: Brak.

Referencje: [NIST SP 800-40].

SI-6 WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Zabezpieczenie podstawowe:

a. Sprawdzanie poprawności działania [*Realizacja: funkcje bezpieczeństwa i ochrony prywatności zdefiniowane przez organizację*];

b. Dokonywanie weryfikacji funkcji określonych w zabezpieczeniu SI-6a [*Wybór (jedna lub więcej)*]: [*Realizacja: stany przejściowe systemu zdefiniowane przez organizację*]; *na polecenie użytkownika z odpowiednimi uprawnieniami;* [*Realizacja: częstotliwość określona przez organizację*]];

c. Powiadamianie [*Realizacja: personel lub role określone przez organizację*] o nieudanych testach weryfikacji bezpieczeństwa i ochrony prywatności; oraz

d. [*Wybór (jeden lub więcej): Wyłączenie systemu; Ponowne uruchomienie systemu;* [*Realizacja: działania alternatywne zdefiniowane przez organizację*]] w przypadku wykrycia anomalii.

Omówienie: Stany przejściowe systemów obejmują uruchomienie, restart, wyłączenie i przerwanie pracy systemu. Powiadomienia systemowe obejmują sygnalizacyjne lampki kontrolne w sprzęcie, elektroniczne alerty kierowane do administratorów systemu oraz komunikaty na lokalnych konsolach komputerowych. W przeciwieństwie do weryfikacji funkcji bezpieczeństwa, weryfikacja funkcji ochrony prywatności zapewnia, że funkcje ochrony prywatności działają zgodnie z oczekiwaniami i są zatwierdzone przez SAOP[106] lub że atrybuty ochrony prywatności są stosowane lub wykorzystywane zgodnie z oczekiwaniami.

Zabezpieczenia powiązane: CA-7, CM-4, CM-6, SI-7.

[106] Tamże.

Zabezpieczenia rozszerzone:

(1) WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | POWIADOMIENIE O NIEUDANYCH TESTACH BEZPIECZEŃSTWA

[Wycofane: Włączone do SI-6].

(2) WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | WSPARCIE AUTOMATYZACYJNE BADAŃ ROZPROSZONYCH

Wdrożenie zautomatyzowanych mechanizmów wspierających zarządzanie rozproszonymi testami funkcji bezpieczeństwa i ochrony prywatności.

Omówienie: Wykorzystanie zautomatyzowanych mechanizmów wspomagających zarządzanie rozproszonymi testami funkcjonalnymi pomaga zapewnić integralność, terminowość, kompletność i skuteczność takich testów.

Zabezpieczenia powiązane: SI-2.

(3) WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | RAPORT Z WYNIKÓW WERYFIKACJI

Zgłaszanie wyników weryfikacji funkcji bezpieczeństwa i ochrony prywatności do [***Realizacja: personel lub role określone przez organizację***]**.**

Omówienie: Personel organizacyjny, który powinien być zapoznawany z wynikami weryfikacji funkcji bezpieczeństwa i ochrony prywatności obejmuje SSO, SAISO, oraz SAOP.[107]

Zabezpieczenia powiązane: SI-4, SR-4, SR-5.

Referencje: [OMB A-130].

[107] Tamże.

SI-7 APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI

Zabezpieczenie podstawowe:

a. Wykorzystywanie narzędzi weryfikacji integralności w celu wykrycia nieautoryzowanych zmian w poniższym oprogramowaniu, oprogramowaniu układowym i informacjach: [*Realizacja: oprogramowanie, oprogramowanie układowe i informacje zdefiniowane przez organizację*]; oraz

b. Podejmowanie następujących działań w przypadku wykrycia nieautoryzowanych zmian w oprogramowaniu, oprogramowaniu układowym i informacjach: [*Realizacja: działania zdefiniowane przez organizację*].

Omówienie: Nieautoryzowane zmiany w oprogramowaniu, oprogramowaniu układowym i informacjach mogą być spowodowane błędami lub złośliwym działaniem. Oprogramowanie obejmuje systemy operacyjne (z kluczowymi komponentami wewnętrznymi, takimi jak jądra lub sterowniki), oprogramowanie pośredniczące i aplikacje. Interfejsy oprogramowania układowego (*ang. firmware*) obejmują interfejs pomiędzy systemem operacyjnym, a firmware (*ang. Unified Extensible Firmware Interface - UEFI*) oraz podstawowy system wejścia/wyjścia (*ang. Basic Input/Output System - BIOS*). Informacje obejmują dane osobowe i metadane, które zawierają atrybuty bezpieczeństwa i ochrony prywatności związane z informacjami. Mechanizmy zabezpieczeń integralności - w tym zabezpieczenia parzystości, cykliczne zabezpieczenia nadmiarowości, kryptograficzne skróty i powiązane narzędzia - umożliwiają automatyczne monitorowanie integralności systemów i hostowanych aplikacji.

Zabezpieczenia powiązane: AC-4, CM-3, CM-7, CM-8, MA-3, MA-4, RA-5, SA-8, SA-9, SA-10, SC-8, SC-12, SC-13, SC-28, SC-37, SI-3, SR-3, SR-4, SR-5, SR-6, SR-9, SR-10, SR-11.

Zabezpieczenia rozszerzone:

(1) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | KONTROLE INTEGRALNOŚCI

Sprawdzanie integralności [***Realizacja: określone przez organizację oprogramowanie, oprogramowanie układowe i informacje***] [***Wybór (jeden lub więcej):*** **podczas uruchamianiu; w** [***Realizacja: stany przejściowe określone przez organizację lub zdarzenia istotne dla bezpieczeństwa***]; [***Realizacja: częstotliwość określona przez organizację***]].

Omówienie: Istotne dla bezpieczeństwa zdarzenia obejmują identyfikację nowych zagrożeń, na które podatne są systemy organizacyjne oraz instalację nowego sprzętu, oprogramowania lub firmware'u. Stany przejściowe obejmują uruchomienie, restart, wyłączenie i przerwanie pracy systemu.

Zabezpieczenia powiązane: Brak.

(2) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | AUTOMATYCZNE POWIADOMIENIA O NARUSZENIACH INTEGRALNOŚCI

Stosowanie zautomatyzowanych narzędzi, które powiadamiają [***Realizacja: personel lub role określone przez organizację***] **po wykryciu rozbieżności podczas weryfikacji integralności.**

Omówienie: Zastosowanie zautomatyzowanych narzędzi do zgłaszania naruszeń integralności systemu i informacji oraz powiadamiania personelu organizacji w odpowiednim czasie, ma zasadnicze znaczenie dla skutecznej reakcji na ryzyko. Personel powiadamiany o naruszeniu integralności systemów i informacji obejmuje właścicieli misji i firm, właścicieli systemów, SAISO, SAOP, administratorów systemów, programistów, integratorów systemów, oraz SPO. [108]

Zabezpieczenia powiązane: Brak.

[108] Tamże.

(3) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | NARZĘDZIA DO CENTRALNEGO ZARZĄDZANIA INTEGRALNOŚCIĄ

Stosowanie centralnie zarządzanych narzędzi weryfikacji integralności.

Omówienie: Centralnie zarządzane narzędzia weryfikacji integralności zapewniają większą spójność w stosowaniu takich narzędzi i mogą ułatwić bardziej kompleksowe ujęcie działań w zakresie weryfikacji integralności.

Zabezpieczenia powiązane: AU-3, SI-2, SI-8.

(4) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | OCHRONA PRZED NARUSZENIAMI

[Wycofane: Włączone do SR-9].

(5) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | AUTOMATYCZNA ODPOWIEDŹ NA NARUSZENIA INTEGRALNOŚCI

Automatycznie [***Wybór (jeden lub więcej): zamyka system; ponownie uruchomienia systemu; wdraża*** [***Realizacja: zabezpieczenia zdefiniowane przez organizację***]] **po wykryciu naruszeń integralności.**

Omówienie: Organizacje mogą definiować różne reakcje sprawdzania integralności według typu informacji, specyficznych informacji lub kombinacji obu. Typy informacji obejmują oprogramowanie sprzętowe, oprogramowanie i dane użytkownika. Specyficzne informacje obejmują oprogramowanie rozruchowe dla określonych typów maszyn. Automatyczne wdrażanie zabezpieczeń w systemach organizacyjnych obejmuje odwracanie zmian, zatrzymywanie systemu lub wyzwalanie alarmów audytowych w przypadku wystąpienia nieautoryzowanych modyfikacji krytycznych plików zabezpieczeń.

Zabezpieczenia powiązane: Brak.

(6) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | OCHRONA KRYPTOGRAFICZNA

Implementowanie mechanizmów kryptograficzne w celu wykrywania nieautoryzowanych zmian w oprogramowaniu, oprogramowaniu układowym i informacjach.

Omówienie: Mechanizmy kryptograficzne stosowane do ochrony integralności obejmują podpisy cyfrowe oraz wyliczanie i stosowanie podpisanych „haszy" z wykorzystaniem kryptografii asymetrycznej, chroniącej poufność klucza użytego do wygenerowania „haszy" oraz wykorzystującej klucz publiczny do weryfikacji informacji o „haszu". Organizacje, które stosują mechanizmy kryptograficzne, rozważają również wprowadzenie rozwiązań w zakresie zarządzania kluczami kryptograficznymi.

Zabezpieczenia powiązane: SC-12, SC-13.

(7) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | INTEGRACJA WYKRYWANIA I ODPOWIEDZI

Włączenie wykrywania następujących nieautoryzowanych zmian do zdolności reagowania na incydenty organizacyjne: [***Realizacja: zdefiniowane przez organizację zmiany istotne z punktu widzenia bezpieczeństwa w systemie***]**.**

Omówienie: Zintegrowanie wykrywania i reagowania pomaga zapewnić, że wykryte zdarzenia są śledzone, monitorowane, korygowane i dostępne do celów archiwalnych. Zachowanie zapisów archiwalnych jest ważne, aby móc zidentyfikować i rozróżnić działania przeciwnika w dłuższym okresie czasu oraz w celu podjęcia ewentualnych kroków prawnych. Zmiany istotne z punktu widzenia bezpieczeństwa obejmują nieuprawnione zmiany ustalonych ustawień konfiguracyjnych lub nieuprawnione podniesienie uprawnień systemowych.

Zabezpieczenia powiązane: AU-2, AU-6, IR-4, IR-5, SI-4.

(8) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | ZDOLNOŚĆ AUDYTU ISTOTNYCH ZDARZEŃ

Po wykryciu potencjalnego naruszenia integralności, zapewnienie możliwości przeprowadzenia audytu zdarzenia i zainicjowania następujących działań: [***Wybór (jeden lub więcej): wygenerowanie zapisu z audytu; ostrzeżenie aktualnego użytkownika; ostrzeżenie*** [***Realizacja: personel lub role określone przez organizację***]***;*** [***Realizacja: inne działania określone przez organizację***]**].**

Omówienie: Organizacje podejmują działania na podstawie typów oprogramowania, poszczególnych programów lub informacji, które mogą naruszać integralność..

Zabezpieczenia powiązane: AU-2, AU-6, AU-12.

(9) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | WERYFIKACJA PROCESU URUCHAMIANIA

Sprawdzanie integralności procesu uruchamiania następujących komponentów systemu: [***Realizacja: zdefiniowane przez organizację komponenty systemu***]**.**

Omówienie: Zapewnienie integralności procesów rozruchowych jest krytyczne dla uruchomienia komponentów systemu w znanych, wiarygodnych stanach. Mechanizmy weryfikacji integralności zapewniają poziom pewności, że tylko zaufany kod jest wykonywany podczas uruchamiania procesów.

Zabezpieczenia powiązane: SI-6.

(10) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | OCHRONA URUCHAMIANIA OPROGRAMOWANIA UKŁADOWEGO

Zaimplementowanie następujących mechanizmów ochrony integralności oprogramowania układowego w [Realizacja: ***komponenty systemu zdefiniowane przez organizację*****]: [Realizacja:** ***mechanizmy zdefiniowane przez organizację*****].**

Omówienie: Nieautoryzowane modyfikacje uruchamiania oprogramowania układowego mogą wskazywać na wyrafinowany, celowy atak. Tego typu ukierunkowane ataki mogą skutkować trwałym odrzuceniem usługi lub trwałym występowaniem złośliwego kodu. Takie sytuacje mogą mieć miejsce, gdy oprogramowanie firmware jest uszkodzone lub gdy złośliwy kod jest wbudowany w oprogramowanie firmware. Komponenty systemu mogą chronić integralność firmware'u rozruchowego w systemach organizacyjnych, weryfikując integralność i autentyczność wszystkich aktualizacji firmware'u przed wprowadzeniem zmian w komponencie systemu i uniemożliwiając nieautoryzowanym procesom modyfikowanie firmware'u rozruchowego.

Zabezpieczenia powiązane: SI-6.

(11) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | ZAMKNIĘTE ŚRODOWISKO Z OGRANICZONYMI UPRAWNIENIAMI

[Wycofane: Włączone do CM-7(6)].

(12) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | WERYFIKACJA INTEGRALNOŚCI

Wymaganie, aby przed wykonaniem zweryfikować integralność następującego zainstalowanego przez użytkownika oprogramowania: [***Realizacja: zdefiniowane przez organizację oprogramowanie instalowane przez użytkownika***]**.**

Omówienie: Organizacje weryfikują integralność oprogramowania zainstalowanego przez użytkownika przed jego wykonaniem w celu zmniejszenia prawdopodobieństwa wykonania złośliwego kodu lub programów zawierających błędy wynikające z nieautoryzowanych modyfikacji. Organizacje biorą pod uwagę praktyczność podejścia do weryfikacji integralności oprogramowania, w tym dostępność wiarygodnych sum zabezpieczeń od twórców i dostawców oprogramowania.

Zabezpieczenia powiązane: CM-11.

(13) OPROGRAMOWANIE, FIRMWARE I INTEGRALNOŚĆ INFORMACJI | WYKONANIE KODU W ŚRODOWISKACH CHRONIONYCH

[Wycofane: Włączone do CM-7(7)].

(14) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | KOD WYKONYWALNY BINARNY LUB MASZYNOWY

[Wycofane: Włączone do CM-7(8)].

(15) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | AUTORYZACJA KODU

Przed instalacją należy zaimplementować mechanizmy kryptograficzne w celu uwierzytelnienia następujących składników oprogramowania lub oprogramowania układowego: [***Realizacja: składniki oprogramowania lub oprogramowania układowego zdefiniowane przez organizację***]**.**

Omówienie: Uwierzytelnianie kryptograficzne obejmuje weryfikację, czy składniki oprogramowania lub firmware'u zostały podpisane cyfrowo przy użyciu certyfikatów uznanych i zatwierdzonych przez organizację. Podpisywanie kodu jest skuteczną metodą ochrony przed złośliwym kodem. Organizacje, które stosują mechanizmy kryptograficzne, rozważają również rozwiązania z zakresu zarządzania kluczami kryptograficznymi.

Zabezpieczenia powiązane: CM-5, SC-12, SC-13.

(16) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | LIMIT CZASU NA WYKONANIE PROCESU BEZ NADZORU

Zakazanie wykonywania procesów bez nadzoru przez okres dłuższy niż [***Realizacja: okres czasu określony przez organizację***]**.**

Omówienie: Wprowadzenie limitu czasowego na wykonanie procesu bez nadzoru ma zastosowanie do procesów, dla których można określić typowe lub normalne okresy wykonania oraz do sytuacji, w których organizacje przekroczą te okresy. Nadzorowane są timery na systemach operacyjnych, odpowiedzi automatyczne

oraz ręczny nadzór i reagowanie w przypadku wystąpienia anomalii procesów systemowych.

Zabezpieczenia powiązane: Brak.

(17) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | SAMOOCHRONA APLIKACJI ŚRODOWISKA WYKONAWCZEGO

Implementowanie [***Realizacja: zabezpieczenia zdefiniowane przez organizację***] **umożliwiające samoochronę aplikacji w czasie działania.**

Omówienie: Samoochrona aplikacji w czasie rzeczywistym wykorzystuje oprzyrządowanie uruchomieniowe do wykrywania i blokowania podatności oprogramowania poprzez wykorzystywanie informacji pochodzących z wykonującego się oprogramowania. Zapobieganie nadużyciom w czasie rzeczywistym różni się od tradycyjnych zabezpieczeń opartych o ochronę obwodową, takich jak bariery i zapory sieciowe, które mogą wykrywać i blokować ataki tylko na podstawie informacji sieciowych bez znajomości kontekstu. Technologia samoochrony aplikacji w czasie rzeczywistym może zmniejszyć podatność oprogramowania na ataki poprzez monitorowanie danych wejściowych i blokowanie tych danych, które mogłyby umożliwić ataki. Może również pomóc w ochronie środowiska uruchomieniowego przed niepożądanymi zmianami i manipulacją. W przypadku wykrycia zagrożenia, technologia samoochrony aplikacji działających w trybie uruchomieniowym, może zapobiec wykorzystaniu zagrożenia i podjąć inne działania (np. wysłać komunikat ostrzegawczy do użytkownika, zakończyć sesję użytkownika, zakończyć działanie aplikacji lub wysłać ostrzeżenie do personelu organizacyjnego). Rozwiązania samoochrony aplikacji działających w czasie rzeczywistym mogą być wdrażane w trybie monitorowania lub ochrony.

Zabezpieczenia powiązane: SI-16.

Referencje: [OMB A-130], [FIPS 140-3], [FIPS 180-4], [FIPS 186-4], [FIPS 202], [NIST SP 800-70], [NIST SP 800-147].

SI-8 OCHRONA PRZED SPAMEM

Zabezpieczenie podstawowe:

a. Stosowanie mechanizmów ochrony przed spamem w punktach wejścia/wyjścia do/z systemu w celu wykrywania i reagowania na niechciane wiadomości; oraz

b. Aktualizacja mechanizmów ochrony antyspamowej po pojawieniu się nowych wersji zgodnie z polityką i procedurami zarządzania konfiguracją organizacji.

Omówienie: Punkty wejścia i wyjścia do/z systemu obejmują zapory ogniowe, serwery zdalnego dostępu, serwery poczty elektronicznej, serwery internetowe, serwery proxy, stacje robocze, notebooki i urządzenia mobilne. Spam może być transportowany za pomocą różnych środków, w tym poczty elektronicznej, załączników do poczty elektronicznej i dostępu do Internetu. Mechanizmy ochrony przed spamem zawierają definicje podpisów.

Zabezpieczenia powiązane: PL-9, SC-5, SC-7, SC-38, SI-3, SI-4.

Zabezpieczenia rozszerzone:

(1) OCHRONA PRZED SPAMEM | ZARZĄDZANIE CENTRALNE

[Wycofane: Włączone do PL-9].

(2) OCHRONA PRZED SPAMEM | AUTOMATYCZNE AKTUALIZACJE

Automatyczne aktualizowanie mechanizmów ochrony przed spamem [***Realizacja: częstotliwość określona przez organizację***]**.**

Omówienie: Używanie automatycznych mechanizmów do aktualizacji mechanizmów ochrony przed spamem pomaga zapewnić, że aktualizacje odbywają się regularnie i dostarczają najnowszych treści i możliwości ochrony.

Zabezpieczenia powiązane: Brak.

(3) OCHRONA PRZED SPAMEM | CIĄGŁA ZDOLNOŚĆ DO NAUKI

Wdrożenie mechanizmów ochrony przed spamem z możliwością uczenia się w celu skuteczniejszej identyfikacji legalnego ruchu telekomunikacyjnego.

Omówienie: Mechanizmy uczenia się obejmują „filtry bayesowskie", które reagują na dane wprowadzane przez użytkowników, identyfikując konkretny ruch, jako legalny lub jako spam, poprzez aktualizację parametrów algorytmów, a tym samym dokładniejsze oddzielenie rodzajów ruchu.

Zabezpieczenia powiązane: Brak.

Referencje: [NIST SP 800-45], [NIST SP 800-177].

SI-9 OGRANICZENIA WPROWADZANIA INFORMACJI

[Wycofane: Włączone do AC-2, AC-3, AC-5 i AC-6].

SI-10 WERYFIKACJA WPROWADZANYCH INFORMACJI

Zabezpieczenie podstawowe: Sprawdzanie prawidłowości wprowadzania następujących danych informacyjnych: [*Realizacja: zdefiniowane przez organizację wejściowe dane informacyjne do systemu*].

Omówienie: Sprawdzanie poprawności składni i semantyki danych wprowadzanych do systemu - w tym zestawu znaków, długości, zakresu liczbowego i dopuszczalnych wartości - umożliwia weryfikację, czy dane wejściowe są zgodne z określonymi definicjami formatu i treści. Na przykład, jeżeli organizacja określa, że wartości liczbowe w zakresie 1-100 są jedynymi dopuszczalnymi danymi wejściowymi dla pola w danej aplikacji, dane wejściowe "387", "abc" lub "%K%" są nieprawidłowe i nie są akceptowane, jako dane wejściowe do systemu. Prawidłowe dane wejściowe mogą się różnić w zależności od pola w aplikacji oprogramowania. Aplikacje zazwyczaj korzystają z dobrze zdefiniowanych protokołów, które używają ustrukturyzowanych wiadomości (tj. poleceń lub zapytań) do komunikacji między modułami oprogramowania lub komponentami systemu. Wiadomości ustrukturyzowane mogą zawierać surowe lub nieustrukturyzowane dane przeplatane metadanymi lub informacjami kontrolnymi. Jeśli aplikacje oprogramowania wykorzystają dane wejściowe wprowadzone przez atakującego do skonstruowania wiadomości strukturalnych bez odpowiedniego kodowania takich wiadomości, wówczas atakujący może wstawić złośliwe polecenia lub znaki specjalne, które mogą spowodować, że dane zostaną zinterpretowane, jako informacje kontrolne lub metadane. W konsekwencji, moduł lub komponent, który otrzyma uszkodzone dane wyjściowe, wykona niewłaściwe operacje lub w inny sposób nieprawidłowo zinterpretuje dane. Wstępne sprawdzanie danych wejściowych przed przekazaniem ich do interpreterów zapobiega niezamierzonej interpretacji treści, jako poleceń. Walidacja danych wejściowych zapewnia dokładne i poprawne dane wejściowe i zapobiega atakom takim jak XSS (*ang. cross-site scripting*) oraz różnym atakom typu „injection".

Zabezpieczenia powiązane: Brak.

Zabezpieczenia rozszerzone:

(1) WERYFIKACJA WPROWADZANYCH INFORMACJI | RĘCZNE ZASTĘPOWANIE

(a) Zapewnienie możliwości ręcznego zastąpienia procedury sprawdzania poprawności następujących danych wejściowych: [***Realizacja: dane wejściowe zdefiniowane przez organizację w zabezpieczeniu podstawowym (SI-10)***]**;**

(b) Używanie funkcji ręcznego zastępowania tylko przez [***Realizacja: osoby upoważnione zdefiniowane przez organizację***]**; oraz**

(c) Kontrolowanie wykorzystania funkcji ręcznego zastępowania.

Omówienie: W niektórych sytuacjach, np. podczas zdarzeń zdefiniowanych w planach awaryjnych, może być konieczne ręczne zastępowanie funkcji weryfikacji danych wejściowych. Ręczne zastępowanie jest stosowane tylko w ograniczonych okolicznościach i przy danych wejściowych zdefiniowanych przez organizację.

Zabezpieczenia powiązane: AC-3, AU-2, AU-12.

(2) WERYFIKACJA WPROWADZANYCH INFORMACJI | PRZEGLĄD / USUWANIE BŁĘDÓW

Sprawdzanie i rozwiązywanie błędów walidacji danych wejściowych w ciągu [***Realizacja: okres czasu określony przez organizację***]**.**

Omówienie: Rozwiązywanie błędów walidacji danych wejściowych obejmuje korektę systemowych przyczyn błędów oraz ponowne przedstawienie sprawy z poprawionymi danymi wejściowymi. Błędy walidacji danych wejściowych to błędy związane z danymi wejściowymi zdefiniowanymi przez organizację w zabezpieczeniu podstawowym (SI-10).

Zabezpieczenia powiązane: Brak.

(3) WERYFIKACJA WPROWADZANYCH INFORMACJI | PRZEWIDYWALNE ZACHOWANIE

Sprawdzanie, czy system zachowuje się w przewidywalny i udokumentowany sposób, odzwierciedlający cele organizacyjne i systemowe, po otrzymaniu nieprawidłowych danych wejściowych.

Omówienie: Powszechną podatnością systemu organizacyjnego jest nieprzewidywalne zachowanie w przypadku otrzymania nieprawidłowych danych wejściowych. Weryfikacja przewidywalności systemu pomaga zapewnić, że w przypadku otrzymania nieprawidłowych danych wejściowych system zachowa się zgodnie ze stawianymi przed nim oczekiwaniami. Następuje to poprzez określenie reakcji systemu, które pozwalają mu na przejście do znanych stanów bez niepożądanych, niezamierzonych skutków ubocznych. Nieprawidłowe dane wejściowe są powiązane z danymi wejściowymi zdefiniowanymi przez organizację w zabezpieczeniu podstawowym (SI-10).

Zabezpieczenia powiązane: Brak.

(4) WERYFIKACJA WPROWADZANYCH INFORMACJI | INTERAKCJE CZASOWE

Uwzględnianie interakcji czasowych pomiędzy komponentami systemu przy określaniu odpowiednich reakcji na nieprawidłowe dane wejściowe..

Omówienie: W adresowaniu nieprawidłowych danych wejściowych systemu otrzymywanych przez interfejsy protokołów, interakcje czasowe stają się istotne, kiedy jeden protokół musi uwzględnić wpływ błędu na reakcje innych protokołów w stosie protokołów. Na przykład, protokoły sieci bezprzewodowych standardu 802.11 nie współdziałają poprawnie z protokołami sterowania transmisją (*ang. Transmission Control Protocols - TCP*), gdy pakiety są tracone (co może być spowodowane nieprawidłowym pakietem wejściowym). TCP zakłada, że utrata pakietów jest spowodowana przeciążeniem, podczas gdy pakiety tracone przez łącza 802.11 są zazwyczaj tracone z powodu zakłóceń lub kolizji na łączu. Jeśli TCP reaguje na przeciążenie, podejmuje błędne działanie w odpowiedzi na zdarzenie kolizji. Adwersarze mogą być w stanie wykorzystać to, co wydaje się być

akceptowalnym indywidualnym zachowaniem protokołów w celu osiągnięcia niekorzystnych efektów poprzez odpowiednie skonstruowanie nieprawidłowych danych wejściowych. Nieprawidłowe dane wejściowe są powiązane z danymi wejściowymi zdefiniowanymi przez organizację w zabezpieczeniu podstawowym (SI-10).

Zabezpieczenia powiązane: Brak.

(5) WERYFIKACJA WPROWADZANYCH INFORMACJI | OGRANICZANIE DANYCH WEJŚCIOWYCH DO ZAUFANYCH ŹRÓDEŁ I ZATWIERDZONYCH FORMATÓW

Ograniczanie korzystanie z informacji wejściowych do [***Realizacja: zaufane źródła zdefiniowane przez organizację***] **i/lub** [***Realizacja: formaty zdefiniowane przez organizację***]**.**

Omówienie: Ograniczenie korzystania z danych wejściowych pochodzących z zaufanych źródeł i zapisanych w zaufanych formatach odnosi się do stosowania koncepcji autoryzowanego lub dozwolonego oprogramowania do dostarczanych danych wejściowych. Określanie znanych zaufanych źródeł do wprowadzania danych i akceptowalnych formatów dla tych danych, może zmniejszyć prawdopodobieństwo złośliwego działania. Dane wejściowe są zdefiniowane przez organizację w zabezpieczeniu podstawowym (SI-10).

Zabezpieczenia powiązane: AC-3, AC-6.

(6) WERYFIKACJA WPROWADZANYCH INFORMACJI | ZAPOBIEGANIE WSTRZYKIWANIU NIEZAUFANYCH DANYCH

Zapobieganie wstrzykiwaniu niezaufanych danych.

Omówienie: Wstrzykiwanie niezaufanych danych może być uniemożliwiane za pomocą parametryzowanego interfejsu lub zapobiegania wyprowadzania danych wyjściowych (kodowania danych wyjściowych). Parametryzowane interfejsy oddzielają dane od kodu, tak, że wstrzyknięcie złośliwych lub niezamierzonych danych nie może zmienić semantyki wysyłanych poleceń. Kodowanie danych

wyjściowych wykorzystuje określone znaki, aby poinformować analizator składni, czy dane są zaufane. Zapobieganie wstrzyknięciom niezaufanych danych dotyczy wejść informacji zdefiniowanych przez organizację w zabezpieczeniu podstawowym (SI-10).

Zabezpieczenia powiązane: AC-3, AC-6.

Referencje: [OMB A-130].

SI-11 OBSŁUGA BŁĘDÓW

Zabezpieczenie podstawowe:

a. Generowanie komunikatów o błędach, które dostarczają informacji niezbędnych do działań naprawczych, bez ujawniania informacji, które mogłyby zostać wykorzystane przez przeciwników; oraz

b. Wyświetlanie komunikatów o błędach tylko zdefiniowanemu [*Realizacja: personel lub role zdefiniowane przez organizację*].

Omówienie: Organizacje biorą pod uwagę strukturę i treść komunikatów o błędach. Zakres, w jakim systemy mogą obsługiwać błędne zachowania, jest określony przez politykę organizacyjną i wymagania operacyjne. Podatne informacje zawierają zapisy stosu (*ang. stack traces*) i szczegóły implementacji; błędne próby logowania z hasłami omyłkowo wprowadzonymi jako nazwa użytkownika; informacje o misji lub działalności, które mogą być wyprowadzone z zarejestrowanych informacji, jeśli nie są one jednoznacznie określone; oraz informacje umożliwiające identyfikację osób, takie jak numery kont, numery PESEL i numery kart bankowych. Komunikaty o błędach mogą również stanowić ukryty kanał przekazywania informacji.

Zabezpieczenia powiązane: AU-2, AU-3, SC-31, SI-2, SI-15.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

SI-12 ZARZĄDZANIE I RETENCJA DANYCH

Zabezpieczenie podstawowe: Zarządzanie i retencja danych przetwarzanych w systemie informatycznym oraz informacji wyjściowe z systemu zgodnie z obowiązującymi przepisami, zarządzeniami wykonawczymi, dyrektywami, politykami, przepisami, standardami i wymaganiami operacyjnymi.

Omówienie: Wymogi dotyczące zarządzania informacjami i ich retencji obejmują pełny cykl życia informacji, w niektórych przypadkach wykraczający poza utylizację systemu. Informacje, które mają być zatrzymywane, mogą również obejmować polityki, procedury, plany, sprawozdania, dane uzyskane w wyniku realizacji zabezpieczeń oraz inne rodzaje informacji administracyjnych. Np. Krajowa Administracja Archiwów i Rejestrów (*ang. National Archives and Records Administration - NARA*) zapewnia politykę i wytyczne dotyczące przechowywania rejestrów i harmonogramów. Jeżeli organizacje posiadają biuro zarządzania dokumentacją, należy rozważyć koordynację z personelem zarządzającym dokumentacją. Dokumentacja sporządzona na podstawie wyników przeprowadzonych zabezpieczeń, które mogą wymagać zarządzania i przechowywania, obejmuje między innymi, ale nie jest do nich ograniczona: wszystkie zabezpieczenia XX-1, AC-6(9), AT-4, AU-12, CA-2, CA-3, CA-5, CA-6, CA-7, CA-8, CA-9, CM-2, CM-3, CM-4, CM-6, CM-8, CM-9, CM-12, CM-13, CP-2, IR-6, IR-8, MA-2, MA-4, PE-2, PE-8, PE-16, PE-17, PL-2, PL-4, PL-7, PL-8, PM-5, PM-8, PM-9, PM-18, PM-21, PM-27, PM-28, PM-30, PM-31, PS-2, PS-6, PS-7, PT-2, PT-3, PT-7, RA-2, RA-3, RA-5, RA-8, SA-4, SA-5, SA-8, SA-10, SI-4, SR-2, SR-4, SR-8.

Zabezpieczenia powiązane: Wszystkie zabezpieczenia XX-1, AC-16, AU-5, AU-11, CA-2, CA-3, CA-5, CA-6, CA-7, CA-9, CM- 5, CM-9, CP-2, IR-8, MP-2, MP-3, MP-4, MP-6, PL-2, PL-4, PM-4, PM-8, PM-9, PS-2, PS-6, PT-2, PT- 3, RA-2, RA-3, SA-5, SA-8, SR-2.

Zabezpieczenia rozszerzone:

(1) ZARZĄDZANIE I RETENCJA DANYCH | OGRANICZANIE ELEMENTÓW DANYCH OSOBOWYCH

Ograniczanie informacji umożliwiających identyfikację osoby przetwarzanych w cyklu życia informacji do następujących elementów danych osobowych: [***Realizacja: określone przez organizację elementy danych osobowych umożliwiające identyfikację osoby***]**.**

Omówienie: Ograniczenie wykorzystania informacji umożliwiających identyfikację osób w całym cyklu życia informacji, jeżeli informacje te nie są potrzebne do celów operacyjnych, pomaga zmniejszyć poziom zagrożenia prywatności powodowanego przez system. Cykl życia informacji obejmuje tworzenie, gromadzenie, wykorzystywanie, przetwarzanie, przechowywanie, utrzymywanie, rozpowszechnianie, ujawnianie i usuwanie informacji. Oceny ryzyka, a także obowiązujące przepisy, regulacje i polityki mogą stanowić użyteczny wkład w określanie, które elementy danych osobowych mogą stwarzać ryzyko.

Zabezpieczenia powiązane: PM-25, PKT-2, PKT-3, RA-3.

(2) ZARZĄDZANIE I RETENCJA DANYCH | MINIMALIZOWANIE WYKORZYSTYWANIA DANYCH OSOBOWYCH PODCZAS TESTÓW, SZKOLEŃ I BADAŃ

Stosowanie następujących technik w celu zminimalizowania wykorzystania danych osobowych do badań, testów lub szkoleń: [*Realizacja: techniki zdefiniowane przez organizację*].

Omówienie: Organizacje mogą zminimalizować ryzyko naruszenia prywatności osoby, stosując takie techniki jak deidentyfikacja lub dane syntetyczne. Ograniczenie wykorzystania informacji umożliwiających identyfikację osoby w całym cyklu życia informacji, gdy nie są one potrzebne do badań, testów lub szkoleń, pozwala zmniejszyć poziom ryzyka utraty prywatności powodowanego przez system. Oceny ryzyka, a także obowiązujące przepisy, regulacje i polityki mogą dostarczyć przydatnych informacji przy określaniu, jakie techniki należy zastosować i kiedy należy je stosować.

Zabezpieczenia powiązane: PM-22, PM-25, SI-19.

(3) ZARZĄDZANIE I RETENCJA DANYCH | USUWANIE INFORMACJI

Stosowanie następujących techniki usuwania, niszczenia lub kasowania informacji po upływie retencji danych: [***Realizacja: techniki określone przez organizację***]**.**

Omówienie: Organizacje mogą zminimalizować zarówno zagrożenia dla bezpieczeństwa, jak i prywatności, usuwając informacje, gdy ich zachowanie nie jest już wymagane. Usuwanie lub niszczenie informacji dotyczy zarówno oryginałów, jak i kopii i archiwalnych zapisów, w tym dzienników systemowych, które mogą zawierać dane osobowe.

Zabezpieczenia powiązane: MP-6.

Referencje: [USC 2901], [OMB A-130].

SI-13 PRZEWIDYWANIE AWARII

Zabezpieczenie podstawowe:

a. Określanie średniego czasu między awariami (*ang. mean time to failure – MTTF*) w określonych środowiskach działania odnoszącego się do: *[Realizacja: elementy systemu teleinformatycznego zdefiniowane przez organizację]; oraz*

b. Zapewnianie zastępczych komponentów systemu oraz środków do wymiany aktywnych i rezerwowych komponentów zgodnie z poniższymi kryteriami: [*Realizacja: określone przez organizację kryteria substytucji MTTF*].

Omówienie: Podczas gdy MTTF jest przede wszystkim kwestią niezawodności, przewidywalne zapobieganie awariom ma na celu przeciwdziałanie potencjalnym awariom komponentów systemu zapewniających funkcje bezpieczeństwa. Wskaźniki awaryjności odzwierciedlają uwarunkowania specyficzne dla danej instalacji, a nie średnią dla całej branży. Organizacje określają kryteria substytucji komponentów systemu w oparciu o wartość MTTF z uwzględnieniem potencjalnych szkód wynikających z awarii komponentów. Przeniesienie odpowiedzialności pomiędzy komponentami aktywnymi i pozostającymi w gotowości nie wpływa negatywnie na bezpieczeństwo, gotowość operacyjną lub możliwości ochrony. Zachowanie zmiennych stanu systemu jest również krytyczne dla zapewnienia udanego procesu transferu. Komponenty w stanie gotowości pozostają dostępne przez cały czas, z wyjątkiem sytuacji związanych z konserwacją lub trwającymi procesami przywracania sprawności.

Zabezpieczenia powiązane: CP-2, CP-10, CP-13, MA-2, MA-6, SA-8, SC-6.

Zabezpieczenia rozszerzone:

(1) PRZEWIDYWANIE AWARII | PRZENIESIENIE ODPOWIEDZIALNOŚCI KOMPONENTÓW

Wyłączanie komponentów systemu z eksploatacji poprzez przeniesienie rozliczalności za komponenty na części zastępujące nie później niż [***Realizacja:***

zdefiniowany przez organizację ułamek lub procent] **średniego czasu między awariami.**

Omówienie: Przenoszenie odpowiedzialności za podstawowe komponenty systemu na inne komponenty zastępcze jeszcze przed wystąpieniem awarii komponentu podstawowego jest ważne dla zmniejszenia ryzyka pogorszenia lub osłabienia misji lub funkcji biznesowych. Dokonywanie takich przeniesień w oparciu o procent średniego czasu między awariami pozwala organizacjom na proaktywne działania w oparciu o ich tolerancję ryzyka. Jednakże przedwczesna wymiana komponentów systemu może spowodować wzrost kosztów jego eksploatacji.

Zabezpieczenia powiązane: Brak.

(2) PRZEWIDYWANIE AWARII | LIMIT CZASU NA WYKONANIE PROCESU BEZ NADZORU

[Wycofane: Włączone do SI-7(16)].

(3) PRZEWIDYWANIE AWARII | RĘCZNY TRANSFER MIĘDZY SKŁADNIKAMI

Inicjowanie ręcznego transferu pomiędzy aktywnymi i rezerwowymi komponentami systemu, gdy użycie komponentu aktywnego osiągnie [***Realizacja: zdefiniowany przez organizację procent***] **średniego czasu między awariami (MTTF).**

Omówienie: Na przykład, jeśli MTTF dla komponentu systemu wynosi 100 dni, a procent MTTF zdefiniowany przez organizację wynosi 90 procent, ręczny transfer miałby miejsce po 90 dniach.

Zabezpieczenia powiązane: Brak.

(4) PRZEWIDYWANIE AWARII | INSTALACJA KOMPONENTÓW Z LISTY REZERWOWEJ / POWIADOMIENIE

W przypadku wykrycia awarii komponentów systemu:

(a) Zapewnienie, że komponenty rezerwowe zostaną pomyślnie i przejrzyście zainstalowane w ciągu [***Realizacja: okres czasu określony przez organizację***]***;*** **oraz**

(b) [***Wybór (jeden lub więcej): Aktywacja*** [***Realizacja: alarm zdefiniowany przez organizację***]***; Automatyczne wyłączenie systemu;*** [***Realizacja: działanie zdefiniowane przez organizację***]]]**.**

Omówienie: Automatyczne lub ręczne przejście komponentów z trybu czuwania do trybu aktywnego może nastąpić po wykryciu awarii komponentów.

Zabezpieczenia powiązane: Brak.

(5) PRZEWIDYWANIE AWARII | PRZEŁĄCZANIE AWARYJNE

Udostępnienie [***Wybór: w czasie rzeczywistym; w czasie zbliżonym do rzeczywistego akceptowanym przez organizację***] [***Realizacja: zdefiniowana przez organizację zdolność do przełączania awaryjnego***] ***systemu*****.**

Omówienie: Tryb awaryjny (*ang. failover*) odnosi się do automatycznego przełączania na system alternatywny w przypadku awarii systemu podstawowego. Zdolność przełączania awaryjnego obejmuje włączenie lustrzanych operacji systemowych w alternatywnych miejscach przetwarzania lub okresowe odtwarzanie danych w regularnych odstępach czasu określonych przez okresy odzyskiwania danych w organizacjach.

Zabezpieczenia powiązane: CP-6, CP-7, CP-9.

Referencje: Brak.

SI-14 ZAPOBIEGANIE ZAAWANSOWANYM DŁUGOTRWAŁYM ATAKOM TYPU APT

Zabezpieczenie podstawowe: Wdrożenie tzw. nietrwałości [*Realizacja: zdefiniowane przez organizację komponenty systemu i usług*], które są inicjowane w znanym stanie i zakończone [*Wybór (jeden lub więcej): po zakończeniu sesji użytkowania; okresowo przy* [*Realizacja: zdefiniowana przez organizację częstotliwość*]].

Omówienie: Wdrożenie nietrwałości komponentów i usług zmniejsza ryzyko związane z zaawansowanymi trwałymi zagrożeniami typu APT (*ang. advanced persistent threat*) poprzez redukcję możliwości ukierunkowania ataku (tj. ograniczenie zakresu i powierzchni ataku) w celu inicjowania i przeprowadzania ataków przez przeciwników. Wdrożenie koncepcji nietrwałości wybranych komponentów systemu pozwala organizacjom na dostarczanie zaufanych zasobów obliczeniowych o znanym stanie przez określony czas, który nie daje adwersarzom wystarczającej ilości czasu na wykorzystanie luk w systemach organizacyjnych lub środowiskach operacyjnych. Ponieważ APT to zagrożenie zaawansowane technologicznie, mające wyrafinowane możliwości, zamiary i cele, organizacje zakładają, że w dłuższym okresie czasu pewien odsetek ataków zakończy się sukcesem. Nietrwałość komponentów i usług systemowych jest aktywowana w miarę potrzeb przy użyciu chronionych informacji i kończone okresowo lub po zakończeniu sesji. Nietrwałość zwiększa współczynnik pracy przeciwników próbujących naruszyć lub złamać systemy organizacyjne.

Nietrwałość może być osiągnięta poprzez odświeżanie komponentów systemowych, okresowe ponowne obrazowanie komponentów lub wykorzystanie różnych popularnych technik wirtualizacji. Usługi nietrwałe mogą być zaimplementowane poprzez użycie technik wirtualizacji, jako część maszyn wirtualnych lub jako nowe instancje procesów na maszynach fizycznych (zarówno trwałych jak i nietrwałych). Zaletą okresowego odświeżania komponentów i usług systemowych jest to, że nie wymaga ono od organizacji wcześniejszego określenia, czy doszło do kompromitacji komponentów lub usług (co często może być trudne do określenia). Odświeżanie

wybranych komponentów systemu i usług odbywa się z częstotliwością wystarczającą do zapobiegania rozprzestrzenianiu się lub zamierzonym skutkom ataków, ale nie z taką częstotliwością, która powodowałaby niestabilność systemu. Odświeżanie krytycznych komponentów i usług może być wykonywane okresowo, aby utrudnić adwersarzom wykorzystanie optymalnych okien podatności.

Zabezpieczenia powiązane: SC-30, SC-34, SI-21.

Zabezpieczenia rozszerzone:

(1) ZAPOBIEGANIE ZAAWANSOWANYM DŁUGOTRWAŁYM ATAKOM TYPU APT | ODŚWIEŻANIE Z ZAUFANYCH ŹRÓDEŁ

Uzyskiwanie oprogramowania i danych wykorzystywanych podczas odświeżania komponentów systemu i usług z następujących zaufanych źródeł: [***Realizacja: zdefiniowane przez organizację zaufane źródła***]**.**

Omówienie: Do zaufanych źródeł zalicza się oprogramowanie i dane z nośników typu "write-once", "read-only" lub z wybranych bezpiecznych nośników offline.

Zabezpieczenia powiązane: Brak.

(2) ZAPOBIEGANIE ZAAWANSOWANYM DŁUGOTRWAŁYM ATAKOM TYPU APT | ZMIENNOŚĆ INFORMACJI

(a) [***Wybór: Odświeżanie*** [***Realizacja: informacje określone przez organizację***] [***Realizacja: częstotliwość określona przez organizację***]***; Generowanie na żądanie*** [***Realizacja: informacje określone przez organizację***]**]; oraz**

(b) Usuwanie niewykorzystywanych informacji.

Omówienie: Retencja informacji dłużej niż jest to konieczne sprawia, że informacje te stają się potencjalnym celem dla zaawansowanych przeciwników wyszukujących aktywów o wysokiej wartości, które mogą zostać narażone na nieupoważnione ujawnienie, nieupoważnioną modyfikację lub eksfiltrację. W przypadku informacji związanych z systemem, nieuzasadnione przetrzymywanie

informacji dostarcza zaawansowanym przeciwnikom informacji, które mogą pomóc w rozpoznaniu i bocznym przepływie przez system.

Zabezpieczenia powiązane: Brak.

(3) ZAPOBIEGANIE ZAAWANSOWANYM DŁUGOTRWAŁYM ATAKOM TYPU APT | ZMIENNOŚĆ POŁĄCZEŃ

Nawiązywanie połączeń z systemem na żądanie i zakańczanie sesji po [*Wybór: wykonanie żądania; okres nieużywania*].

Omówienie: Trwałe połączenia z systemami mogą zapewnić zaawansowanym adwersarzom ścieżki do bocznego przechodzenia przez systemy i potencjalnego pozycjonowania się bliżej aktywów o wysokiej wartości. Ograniczenie dostępności takich połączeń ogranicza zdolność adwersarza do swobodnego poruszania się w systemach organizacyjnych.

Zabezpieczenia powiązane: SC-10.

Referencje: Brak.

SI-15 FILTROWANIE INFORMACJI WYJŚCIOWYCH

Zabezpieczenie podstawowe: Weryfikowanie danych wyjściowych z programów i/lub aplikacji w celu upewnienia się, że informacje są zgodne z oczekiwaną zawartością: [*Realizacja: programy i/lub aplikacje zdefiniowane przez organizację*].

Omówienie: Niektóre typy ataków, w tym wstrzykiwanie kodu SQL, generują wyniki wyjściowe, które są nieoczekiwane lub niespójne z wynikami wyjściowymi, jakich można oczekiwać od programów lub aplikacji. Filtrowanie danych wyjściowych koncentruje się na wykrywaniu obcych treści, zapobieganiu ich wyświetlania, a następnie powiadamianiu narzędzi monitorujących o wykryciu anomalii.

Zabezpieczenia powiązane: SI-3, SI-4, SI-11.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

SI-16 OCHRONA PAMIĘCI

Zabezpieczenie podstawowe: Zaimplementowanie następujących środków bezpieczeństwa w celu ochrony pamięci systemu przed nieautoryzowanym wykonaniem kodu: [*Realizacja: zabezpieczenia zdefiniowane przez organizację*].

Omówienie: Niektórzy przeciwnicy przeprowadzają ataki z zamiarem wykonania kodu w niewykonalnych regionach pamięci lub w miejscach pamięci, które są zabronione. Zabezpieczenia stosowane w celu ochrony pamięci obejmują zapobieganie wykonywaniu danych oraz randomizację układu przestrzeni adresowej. Zabezpieczenia przed wykonywaniem danych mogą być wymuszane sprzętowo lub programowo, przy czym wymuszanie sprzętowe zapewnia większą siłę mechanizmu.

Zabezpieczenia powiązane: AC-25, SC-3, SI-7.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

SI-17 PROCEDURY TESTOWANIA AWARYJNEGO „FAIL-SAFE”

Zabezpieczenie podstawowe: Wdrożenie procedur bezpieczeństwa w przypadku wystąpienia awarii: [*Realizacja: określony przez organizację wykaz warunków wystąpienia awarii i procedur bezpieczeństwa w przypadku wystąpienia awarii*].

Omówienie: Warunki awarii obejmują utratę łączności między krytycznymi komponentami systemu lub między komponentami systemu, a urządzeniami operacyjnymi. Procedury bezpieczeństwa w przypadku wystąpienia awarii obejmują ostrzeganie personelu obsługującego i dostarczanie szczegółowych instrukcji dotyczących kolejnych kroków, które należy podjąć. Kolejne kroki mogą obejmować niepodejmowanie żadnych działań, przywracanie ustawień systemu, wyłączanie procesów, ponowne uruchamianie systemu lub kontakt z wyznaczonym personelem organizacyjnym.

Zabezpieczenia powiązane: CP-12, CP-13, SC-24, SI-13.

Zabezpieczenia rozszerzone: Brak.

Referencje: Brak.

SI-18 OPERACJE SPRADZAJĄCE JAKOŚĆ DANYCH OSOBOWYCH

Zabezpieczenie podstawowe:

a. Sprawdzanie dokładności, przydatności, terminowości i kompletności informacji umożliwiających identyfikację osób w całym cyklu życia informacji [*Realizacja: częstotliwość określona przez organizację*]; oraz

b. Poprawianie lub usuwanie niedokładnych lub nieaktualnych danych osobowych.

Omówienie: Działania związane z jakością danych osobowych obejmują kroki, które organizacje podejmują w celu potwierdzenia dokładności i przydatności informacji osobowych w całym cyklu życia informacji. Cykl życia informacji obejmuje tworzenie, zbieranie, wykorzystywanie, przetwarzanie, przechowywanie, obsługę, rozpowszechnianie, ujawnianie i usuwanie informacji umożliwiających identyfikację osób. Operacje związane z jakością informacji umożliwiających identyfikację osób obejmują edycję i walidację adresów w miarę ich gromadzenia lub wprowadzania do systemów przy użyciu zautomatyzowanych interfejsów do programowania aplikacji służących do weryfikacji adresów. Sprawdzanie jakości informacji umożliwiających identyfikację osób obejmuje śledzenie aktualizacji lub zmian danych w czasie, co pozwala organizacjom dowiedzieć się, w jaki sposób i jakie dane osobowe zostały zmienione w przypadku zidentyfikowania błędnych informacji. Środki podejmowane w celu ochrony jakości danych osobowych opierają się na charakterze i kontekście informacji umożliwiających identyfikację osób, sposobie ich wykorzystania, sposobie ich uzyskania oraz ewentualnych zastosowanych metodach dezidentyfikacji. Środki podejmowane w celu weryfikacji dokładności informacji umożliwiających identyfikację osób, wykorzystywanych do ustalania praw, korzyści lub przywilejów osób objętych programami państwowymi, mogą być bardziej kompleksowe niż środki stosowane w celu weryfikacji informacji umożliwiających identyfikację osób wykorzystywanych do celów mniej wrażliwych.

Zabezpieczenia powiązane: PM-22, PM-24, PT-2, SI-4.

Zabezpieczenia rozszerzone:

(1) OPERACJE SPRAWDZAJĄCE JAKOŚĆ DANYCH OSOBOWYCH | AUTOMATYZACJA WSPARCIA

Poprawianie lub usuwanie informacji umożliwiających identyfikację osób, które są niedokładne lub nieaktualne, nieprawidłowo określone pod względem podatności lub nieprawidłowo zdezidentyfikowane przy użyciu [***Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację***]**.**

Omówienie: Wykorzystanie automatycznych mechanizmów do poprawy jakości danych może nieumyślnie stwarzać zagrożenie dla prywatności. Zautomatyzowane narzędzia mogą łączyć się z zewnętrznymi lub w inny sposób niepowiązanymi systemami, a dopasowanie zapisów między tymi systemami może tworzyć powiązania o niezamierzonych konsekwencjach. Organizacje oceniają i dokumentują te zagrożenia w swoich ocenach wpływu na prywatność oraz dokonują ustaleń zgodnych z ich planami programów ochrony prywatności.

Ponieważ dane są uzyskiwane i wykorzystywane w całym cyklu życia informacji, ważne jest, aby potwierdzić dokładność i znaczenie informacji umożliwiających identyfikację osób. Zautomatyzowane mechanizmy mogą poprawić istniejące procesy i procedury w zakresie jakości danych oraz umożliwić organizacji lepszą identyfikację i zarządzanie informacjami umożliwiającymi identyfikację osób w dużych systemach. Na przykład, zautomatyzowane narzędzia mogą znacznie poprawić wysiłki zmierzające do konsekwentnej normalizacji danych lub identyfikacji danych zniekształconych. Zautomatyzowane narzędzia mogą być również wykorzystywane do poprawy zabezpieczeń danych i wykrywania błędów, które mogą nieprawidłowo zmienić dane osobowe lub nieprawidłowo powiązać takie informacje z niewłaściwą osobą. Zautomatyzowane funkcje wspierają procesy i procedury w skali umożliwiającej bardziej precyzyjne wykrywanie i korygowanie błędów jakości danych.

Zabezpieczenia powiązane: PM-18, RA-8.

(2) OPERACJE SPRAWDZAJĄCE JAKOŚĆ DANYCH OSOBOWYCH | ZNACZNIKI DANYCH

Stosowanie znaczników danych w celu zautomatyzowania korygowania lub usuwania danych osobowych w całym cyklu życia informacji w systemach organizacyjnych.

Omówienie: Oznaczanie danych dotyczących informacji umożliwiających identyfikację osób obejmuje znaczniki, które wskazują zezwolenia na przetwarzanie, upoważnienie do przetwarzania, pozbawienie tożsamości, poziom wpływu, etap cyklu życia informacji oraz daty przechowywania lub ostatniej aktualizacji. Stosowanie znaczników danych w odniesieniu do informacji umożliwiających identyfikację osób może wspierać stosowanie zautomatyzowanych narzędzi do poprawiania lub usuwania odpowiednich informacji osobowych.

Zabezpieczenia powiązane: AC-3, AC-16, SC-16.

(3) OPERACJE SPRAWDZAJĄCE JAKOŚĆ DANYCH OSOBOWYCH |ZBIERANIE DANYCH

Zbieranie dane osobowych bezpośrednio od danej osoby.

Omówienie: Osoby lub ich wyznaczeni przedstawiciele mogą dostarczać prawidłowych informacji umożliwiających identyfikację osób. Organizacje biorą pod uwagę czynniki kontekstowe, które mogą zachęcać osoby do podawania poprawnych danych w celu uniknięcia podawania fałszywych. Dodatkowe kroki mogą być konieczne do zatwierdzenia zebranych informacji w zależności od charakteru i kontekstu informacji umożliwiających identyfikację osób, sposobu ich wykorzystania oraz sposobu ich uzyskania. Środki podejmowane w celu potwierdzenia dokładności danych osobowych służących do identyfikacji osób, wykorzystywanych do określania praw, korzyści lub przywilejów osób w ramach programów rządowych, mogą być bardziej wszechstronne niż środki podejmowane w celu potwierdzenia mniej wrażliwych danych osobowych.

Zabezpieczenia powiązane: Brak.

(4) OPERACJE SPRAWDZAJĄCE JAKOŚĆ DANYCH OSOBOWYCH | ZGŁOSZENIA USUNIĘCIA DANYCH

Korekta lub usuwanie danych osobowych na żądanie osób lub ich wyznaczonych przedstawicieli.

Omówienie: Nieprecyzyjne dane osobowe przechowywane przez organizacje mogą powodować problemy dotykające osoby, szczególnie w przypadku tych funkcji biznesowych, w których niedokładne informacje mogą skutkować niewłaściwymi decyzjami lub odmową świadczeń i usług dla osób. Nawet poprawne informacje, w pewnych okolicznościach, mogą powodować problemy odczuwane przez osoby, przewyższające korzyści z utrzymywania informacji przez organizację. Organizacje kierują się uznaniem przy określaniu, czy informacje umożliwiające identyfikację osób mają być poprawione lub usunięte, w oparciu o zakres wniosków, pożądane zmiany, wpływ zmian oraz prawo, przepisy i zasady. Personel organizacyjny konsultuje się z SAOP[109] i radcą prawnym w sprawie odpowiednich przypadków poprawiania lub usuwania informacji.

Zabezpieczenia powiązane: Brak.

(5) OPERACJE SPRAWDZAJĄCE JAKOŚĆ DANYCH OSOBOWYCH |ZAWIADOMIENIE O KOREKCIE LUB USUNIĘCIU

Powiadamianie [***Realizacja: zdefiniowani przez organizację odbiorcy danych osobowych***] **oraz osoby, że dane osobowe zostały poprawione lub usunięte.**

Omówienie: W przypadku skorygowania lub usunięcia danych osobowych, organizacje podejmują kroki w celu zapewnienia, że wszyscy upoważnieni odbiorcy takich informacji, a także osoba, z którą informacje są powiązane lub ich wyznaczeni przedstawiciele, są poinformowani o skorygowanych lub usuniętych danych.

[109] Tamże

Zabezpieczenia powiązane: Brak.

Referencje: [NIST SP 800-188], [IR 8112], [OMB M-19-15].

SI-19 DE-IDENTYFIKACJA

Zabezpieczenie podstawowe:

a. Usuwanie z zestawów danych następujących elementów informacji umożliwiających identyfikację osób: [*Realizacja: określone przez organizację elementy informacji umożliwiających identyfikację osób*]; oraz

b. Ocenianie [*Realizacja: częstotliwość zdefiniowana przez organizację*] skuteczności przeprowadzonej deidentyfikacji.

Omówienie: Deidentyfikacja to ogólny termin określający proces usuwania powiązań między zbiorem danych identyfikacyjnych, a osobą, której dane dotyczą. Wiele zbiorów danych zawiera informacje o osobach, które mogą być wykorzystane do rozróżnienia lub prześledzenia tożsamości osoby fizycznej, takie jak nazwisko, PESEL, data i miejsce urodzenia, nazwisko panieńskie matki lub dane biometryczne. Zbiory danych mogą również zawierać inne informacje, które są powiązane lub możliwe do powiązania z daną osobą, takie jak informacje medyczne, edukacyjne, finansowe i dotyczące zatrudnienia. Informacje umożliwiające identyfikację osób są usuwane ze zbiorów danych przez przeszkolone osoby, jeżeli informacje te nie są (lub przestały być) niezbędne do spełnienia wymogów przewidzianych dla tych danych. Na przykład, jeżeli zbiór danych jest wykorzystywany wyłącznie do tworzenia statystyk zbiorczych, identyfikatory, które nie są potrzebne do tworzenia tych statystyk, są usuwane. Usunięcie identyfikatorów poprawia ochronę prywatności, ponieważ usunięte informacje nie mogą być nieumyślnie ujawnione lub niewłaściwie wykorzystane. Organizacje mogą podlegać określonym definicjom lub metodom dezidentyfikacji zgodnie z obowiązującymi przepisami prawa, regulacjami lub zasadami. Ponowna identyfikacja jest ryzykiem szczątkowym w przypadku danych, które zostały zdeidentyfikowane. Ataki na ponowną identyfikację mogą być różne, w tym mogą obejmować łączenie nowych zbiorów danych lub inne usprawnienia w zakresie analizy danych. Utrzymanie świadomości potencjalnych ataków i ocena

skuteczności usuwania danych identyfikacyjnych w czasie, wspiera zarządzanie tym ryzykiem szczątkowym.

Zabezpieczenia powiązane: MP-6, PM-22, PM-23, PM-24, RA-2, SI-12.

Zabezpieczenia rozszerzone:

(1) DE-IDENTYFIKACJA | ZBIERANIE DANYCH

Pozbawienie zbioru danych możliwości identyfikacji poprzez nie gromadzenie informacji umożliwiających ustalenie osoby.

Omówienie: Jeżeli źródło danych zawiera informacje umożliwiające identyfikację osoby, ale informacje te nie będą wykorzystywane, zbiór danych w momencie tworzenia może zostać pozbawiony tożsamości (poddany deidentyfikacji) poprzez zaniechanie gromadzenia elementów danych, które zawierają informacje umożliwiające identyfikację osoby. Na przykład, jeżeli organizacja nie zamierza wykorzystywać numeru PESEL osoby ubiegającej się o pracę, wówczas formularze wniosków nie zawierają pytania o PESEL.

Zabezpieczenia powiązane: Brak.

(2) DE-IDENTYFIKACJA | ARCHIWIZACJA DANYCH

Zakazanie archiwizowania elementów informacji umożliwiających identyfikację osoby, jeżeli te elementy nie będą potrzebne po dokonaniu archiwizacji zbioru danych.

Omówienie: Zbiory danych mogą być archiwizowane z wielu powodów. Określa się przewidywane cele archiwizowanego zbioru danych, a jeżeli elementy informacji umożliwiających identyfikację osób nie są wymagane, elementy te nie są archiwizowane

Zabezpieczenia powiązane: Brak.

(3) DE-IDENTYFIKACJA | UJAWNIANIE DANYCH

Usuwanie elementów informacji umożliwiających identyfikację osób ze zbioru danych przed ich udostępnieniem, jeżeli te elementy zbioru danych nie muszą być częścią udostępniania danych.

Omówienie: Przed udostępnieniem zbioru danych, administrator danych rozważa zamierzone sposoby wykorzystania zbioru danych i określa, czy konieczne jest udostępnienie danych osobowych. Jeśli dane osobowe nie są konieczne, można je usunąć za pomocą technik dezidentyfikacji.

Zabezpieczenia powiązane: Brak.

(4) DE-IDENTYFIKACJA | USUWANIE, MASKOWANIE, SZYFROWANIE, HASZOWANIE LUB WYMIANA IDENTYFIKATORÓW BEZPOŚREDNICH

Usuwanie, maskowanie, szyfrowanie, haszowanie lub wymiana identyfikatorów bezpośrednich w zbiorze danych.

Omówienie: Istnieje wiele możliwych procesów usuwania identyfikatorów bezpośrednich ze zbioru danych. Kolumny w zbiorze danych, które zawierają identyfikator bezpośredni, mogą zostać usunięte. Podczas maskowania identyfikator bezpośredni jest przekształcany na powtarzający się znak, np. XXXXXX lub 999999. Identyfikatory mogą być szyfrowane lub haszowane tak, że połączone rekordy pozostają połączone. W przypadku szyfrowania lub haszowania stosowane są algorytmy, które wymagają użycia klucza, w tym symetryczny szyfr blokowy (*ang. Advanced Encryption Standard*) lub kod HMAC[110] (*ang. Hash-based Message Authentication Code*). Wdrożenia mogą używać tego samego klucza dla wszystkich identyfikatorów lub używać innego klucza dla każdego identyfikatora. Użycie innego klucza dla każdego identyfikatora zapewnia

[110] Kod uwierzytelniania wiadomości (ang. *message authentication code - MAC*) z wmieszanym kluczem tajnym zapewniający zarówno ochronę integralności jak i autentyczności danych.

wyższy stopień bezpieczeństwa i ochrony prywatności. Identyfikatory można alternatywnie zastąpić słowem kluczowym, przekształcając np. "George Washington" na "PATIENT" lub zastępując je wartością zastępczą, np. przekształcając "George Washington" na "Abraham Polk".

Zabezpieczenia powiązane: SC-12, SC-13.

(5) DE-IDENTYFIKACJA | ZABEZPIECZENIE UJAWNIANIA DANYCH STATYSTYCZNYCH

Manipulowanie danymi liczbowymi, tabelami kontyngencji i wynikami statystycznymi w taki sposób, aby wyniki analizy nie umożliwiały identyfikacji żadnej osoby ani organizacji.

Omówienie: Wiele rodzajów analiz statystycznych może prowadzić do ujawnienia informacji o osobach, nawet jeśli dostarczane są tylko informacje zbiorcze. Na przykład, jeśli szkoła, która publikuje comiesięczną tabelę z liczbą uczniów niepełnoletnich zapisanych do szkoły, podaje, że w styczniu ma 10-19 takich uczniów, a następnie podaje, że w marcu ma 20-29 takich uczniów, to można wywnioskować, że uczniowie, którzy zapisali się do szkoły w lutym, byli niepełnoletni.

Zabezpieczenia powiązane: Brak.

(6) DE-IDENTYFIKACJA |ZRÓŻNICOWANA PRYWATNOŚĆ

Zapobieganie ujawnianiu informacji umożliwiających identyfikację osób poprzez dodawanie niedeterministycznego szumu do wyników operacji matematycznych przed podaniem wyników.

Omówienie: Matematyczna definicja prywatności różnicowej zakłada, że wynik analizy zbioru danych powinien być w przybliżeniu taki sam przed i po dodaniu lub usunięciu pojedynczego rekordu danych (co do którego zakłada się, że są to dane pochodzące od pojedynczej osoby). W swojej najbardziej podstawowej formie, prywatność różnicowa ma zastosowanie jedynie do systemów zapytań online. Może być jednak również wykorzystywana do tworzenia statystycznych

klasyfikatorów uczących się maszynowo oraz danych syntetycznych. Różnicowanie prywatności odbywa się kosztem zmniejszonej dokładności wyników, co zmusza organizacje do określenia równowagi pomiędzy ochroną prywatności, a ogólną dokładnością, użytecznością i przydatnością zbioru danych pozbawionych identyfikacji. Szum niedeterministyczny (stochastyczny) może obejmować dodawanie małych, losowych wartości do wyników operacji matematycznych w analizie zbioru danych.

Zabezpieczenia powiązane: SC-12, SC-13.

(7) DE-IDENTYFIKACJA | ZATWIERDZONE ALGORYTMY I OPROGRAMOWANIE

Przeprowadzanie de-identyfikacji przy użyciu zatwierdzonych do wdrażania algorytmów i oprogramowania.

Omówienie: Algorytmy, które pozornie usuwają informacje umożliwiające identyfikację osób ze zbioru danych, mogą w rzeczywistości pozostawić informacje umożliwiające identyfikację osób lub dane umożliwiające ponowną identyfikację. Oprogramowanie, które rzekomo wdraża zatwierdzony algorytm, może zawierać błędy lub wdrażać inny algorytm. Oprogramowanie może pozbawiać tożsamości jeden typ danych, taki jak liczby całkowite, ale nie pozbawia tożsamości innego typu danych, takich jak liczby zmiennoprzecinkowe. Z tych powodów usuwanie danych identyfikacyjnych przeprowadza się przy użyciu zatwierdzonych algorytmów i oprogramowania.

Zabezpieczenia powiązane: Brak.

(8) DE-IDENTYFIKACJA | ZMOTYWOWANY INTRUZ

Przeprowadzenie testu zmotywowanego intruza na zbiorze danych pozbawionych cech identyfikacyjnych, w celu ustalenia czy pozostały dane zidentyfikowane lub czy dane pozbawione cech identyfikacyjnych mogą zostać ponownie zidentyfikowane.

Omówienie: Test zmotywowanego intruza jest testem, w którym osoba lub grupa otrzymuje dostęp do danych oraz określonych zasobów i próbuje ponownie zidentyfikować jedną lub więcej osób w zdezidentyfikowanym zbiorze danych. Testy takie określają zakres niezbędnej wiedzy własnej, zasobów obliczeniowych, środków finansowych, danych i umiejętności, jakie intruzi muszą posiadać, aby przeprowadzić próby włamania. Test zmotywowanego intruza pozwala określić, czy deidentyfikacja jest niedostatecznie skuteczna. Może on być również użytecznym narzędziem diagnostycznym do oceny, czy deidentyfikacja będzie prawdopodobnie wystarczająca. Jednakże sam test nie może udowodnić, że usuwanie danych jest wystarczające.

Zabezpieczenia powiązane: Brak.

Referencje: [OMB A-130], [NIST SP 800-188].

SI-20 SKAŻENIE

Zabezpieczenie podstawowe: Osadzenie danych lub funkcji w następujących systemach lub komponentach systemowych w celu określenia, czy dane organizacyjne zostały eksfiltrowane lub niewłaściwie usunięte z organizacji: [*Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację*].

Omówienie: Wiele cyberataków jest ukierunkowanych na informacje organizacyjne lub informacje, które organizacja przechowuje w imieniu innych podmiotów (np. informacje umożliwiające identyfikację osób), i powoduje eksfiltrację tych danych. Ponadto, ataki wewnętrzne i błędne procedury postępowania użytkowników mogą spowodować usunięcie z systemu informacji, co stanowi naruszenie zasad organizacyjnych. Metody skażenia mogą być zarówno pasywne, jak i aktywne. Pasywne podejście do skażenia może być tak proste, jak dodanie fałszywych nazw i adresów e-mail do wewnętrznej bazy danych. Jeśli organizacja otrzymuje wiadomości e-mail na jeden z fałszywych adresów e-mail, wie, że baza danych została naruszona. Co więcej, organizacja wie, że e-mail został wysłany przez nieautoryzowany podmiot, zatem wszelkie zawarte w nim pakiety mogą potencjalnie zawierać złośliwy kod, oraz że nieautoryzowany podmiot mógł potencjalnie uzyskać kopię bazy danych. Inne podejście do skażenia może obejmować osadzanie fałszywych danych lub danych steganograficznych w plikach, co umożliwia ich odnalezienie za pomocą analizy open-source. Wreszcie, aktywne podejście do skażenia może obejmować osadzanie w danych oprogramowania, które jest w stanie " zadzwonić do domu", ostrzegając w ten sposób organizację o ich "przechwyceniu", a być może także o ich lokalizacji i ścieżce, za pomocą której zostały one eksfiltrowane lub usunięte.

Zabezpieczenia powiązane: AU-13.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [NIST SP 800-160-2].

SI-21 ODŚWIEŻANIE INFORMACJI

Zabezpieczenie podstawowe: Odświeżanie [Realizacja: *informacje zdefiniowana przez organizację*] z [*Realizacja: częstotliwość zdefiniowana przez organizację*] lub generowanie informacji na żądanie i usuwanie niewykorzystywanych informacji.

Omówienie: Retencja informacji przez okres dłuższy niż jest to konieczne sprawia, że stają się one coraz cenniejszym i bardziej kuszącym celem dla przeciwników. Posiadanie informacji przez minimalny okres czasu niezbędny do wspierania misji organizacyjnych lub funkcji biznesowych ogranicza możliwość narażenia, przechwycenia i eksfiltracji tych informacji przez przeciwników.

Zabezpieczenia powiązane: SI-14.

Zabezpieczenia rozszerzone: Brak.

Referencje: [OMB A-130], [NIST SP 800-160-2].

SI-22 RÓŻNICOWANIE INFORMACJI

Zabezpieczenie podstawowe:

a. Zidentyfikowanie następujących alternatywnych źródeł informacji dla [Realizacja: zdefiniowane przez organizację podstawowe funkcje i usługi]: [Realizacja: alternatywne źródła informacji zdefiniowane przez organizację]; oraz

b. Wykorzystywanie alternatywnego źródła informacji do realizacji istotnych funkcji lub usług w [Realizacja: zdefiniowane przez organizację systemy lub komponenty systemu] w przypadku uszkodzenia lub niedostępności podstawowego źródła informacji..

Omówienie: Działania podejmowane przez usługę lub funkcję systemową często wynikają z uzyskiwanych przez nią informacji. Uszkodzenie, sfabrykowanie, zmodyfikowanie lub usunięcie tych informacji może wpłynąć na zdolność usługi do prawidłowego wykonywania zamierzonych działań. Posiadając wiele źródeł danych wejściowych, usługa lub funkcja może kontynuować działanie, jeżeli jedno źródło ulegnie uszkodzeniu lub przestanie być dostępne. Możliwe jest, że alternatywne źródła informacji mogą być mniej precyzyjne lub mniej dokładne niż podstawowe źródło informacji. Jednak posiadanie takich nieoptymalnych źródeł informacji może nadal zapewniać wystarczający poziom jakości, aby zasadnicza usługa lub funkcja mogła być realizowana, nawet w sposób obniżony lub osłabiony.

Zabezpieczenia powiązane: Brak.

Zabezpieczenia rozszerzone: Brak.

Referencje: [NIST SP 800-160-2].

SI-23 FRAGMENTACJA INFORMACJI

Zabezpieczenie podstawowe: W oparciu o [*Realizacja: okoliczności określone przez organizację*]*:*

a. Fragmentacja następujących informacji: [*Realizacja: informacje określone przez organizację*]*;* oraz

b. Dystrybuowanie podzielonej informacji pomiędzy następujące systemy lub komponenty systemu: [*Realizacja: zdefiniowane przez organizację systemy lub komponenty systemów*].

Omówienie: Jednym z celów zaawansowanych trwałych zagrożeń jest eksfiltracja cennych informacji. Po eksfiltracji, organizacja zazwyczaj nie ma możliwości odzyskania utraconych informacji. Dlatego też, organizacje mogą rozważyć podzielenie informacji na rozproszone elementy i rozmieszczenie tych elementów w wielu systemach lub komponentach i lokalizacjach. Takie działania zwiększą czynnik pracy przeciwnika w celu przechwycenia i eksfiltracji pożądanych informacji, a tym samym zwiększą prawdopodobieństwo wykrycia tego czynnika. Fragmentacja informacji wpływa na zdolność organizacji do uzyskania dostępu do informacji w odpowiednim czasie. Zakres fragmentacji jest podyktowany wpływem lub poziomem klasyfikacji (i wartością) informacji, otrzymanymi informacjami wywiadowczymi dotyczącymi zagrożeń oraz tym, czy stosowane jest skażenie danych (tj. informacje pochodzące ze skażenia danych dotyczące eksfiltracji niektórych informacji mogą spowodować fragmentację pozostałych informacji).

Zabezpieczenia powiązane: Brak.

Zabezpieczenia rozszerzone: Brak.

KATEGORIA SR - ZARZĄDZANIE RYZYKIEM W ŁAŃCUCHU DOSTAW

SR-1 POLITYKA I PROCEDURY

Zabezpieczenie podstawowe:

a. Opracowywanie, dokumentowanie i rozpowszechnianie wśród [Realizacja: *personel lub role określone przez organizację*]:

1. [*Wybór (jeden lub więcej): poziom organizacji; poziom misji/procesu biznesowego; poziom systemu*] polityki zarządzania ryzykiem w łańcuchu dostaw, która:

(a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami; oraz

(b) Jest zgodna z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi; oraz

2. Procedur ułatwiających wdrożenie polityki zarządzania ryzykiem w łańcuchu dostaw oraz powiązanych zabezpieczeń w zakresie zarządzania ryzykiem w łańcuchu dostaw;

b. Wyznaczanie [Realizacja: *osoba wyznaczona przez organizację*] do zarządzania rozwojem, dokumentacją i rozpowszechnianiem polityki i procedur zarządzania ryzykiem w łańcuchu dostaw; oraz

c. Przeglądanie i aktualizacja bieżącej:

1. Polityki zarządzania ryzykiem w łańcuchu dostaw z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*]; oraz

2. Procedur zarządzania ryzykiem w łańcuchu dostaw z [Realizacja: *częstotliwość określona przez organizację*] i następujących [Realizacja: *zdarzenia określone przez organizację*].

Omówienie: Polityka i procedury w zakresie zarządzania ryzykiem w łańcuchu dostaw dotyczą zabezpieczeń w kategorii *Zarządzanie ryzykiem w łańcuchu dostaw* (SR), które są wdrażane w ramach systemów i organizacji. Strategia zarządzania ryzykiem jest ważnym czynnikiem przy tworzeniu takich polityk i procedur. Polityki i procedury przyczyniają się do zapewnienia bezpieczeństwa i ochrony prywatności. Dlatego ważne jest, aby programy bezpieczeństwa i ochrony prywatności były opracowywane wspólnie przy kształtowaniu polityki i procedur zarządzania ryzykiem w łańcuchu dostaw. Polityki i procedury dotyczące programów bezpieczeństwa i ochrony prywatności na poziomie organizacji są ogólnie rzecz biorąc preferowane i mogą eliminować potrzeby tworzenia polityk i procedur specyficznych dla danej misji lub systemu. Polityka może być włączona, jako część ogólnej polityki bezpieczeństwa i ochrony prywatności lub reprezentowana przez wiele polityk odzwierciedlających złożony charakter organizacji. Procedury mogą być ustanowione dla programów bezpieczeństwa i ochrony prywatności, dla misji lub procesów biznesowych oraz dla systemów, jeśli to konieczne. Procedury opisują sposób wdrażania zasad lub zabezpieczeń i mogą być skierowane do osoby lub roli, która jest przedmiotem procedury. Procedury mogą być udokumentowane w planach bezpieczeństwa i ochrony prywatności systemu w jednym lub kilku oddzielnych dokumentach.

Zdarzenia, które mogą spowodować konieczność aktualizacji polityki i procedur zarządzania ryzykiem w łańcuchu dostaw, obejmują wyniki oceny lub audytu, incydenty lub naruszenia bezpieczeństwa, lub zmiany w przepisach prawa, zarządzeniach, dyrektywach, rozporządzeniach, zasadach, standardach i wytycznych.

Oświadczenie o wprowadzeniu zabezpieczeń nie jest równoznaczne z ustanowieniem polityki lub procedury organizacyjnej.

Zabezpieczenia powiązane: PM-9, PM-30, PS-8, SI-12.

Zabezpieczenia rozszerzone: Brak.

Referencje: [FASC18], [41 CFR 201], [EO 13873], [CNSSD 505], [NIST SP 800-12], [NIST SP 800-30], [NIST SP 800-39], [NIST SP 800- 100], [NIST SP 800-161].

SR-2 PLAN ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW

Zabezpieczenie podstawowe:

a. Opracowanie planu zarządzania ryzykiem związanym z łańcuchem dostaw w zakresie badań i rozwoju, projektowania, produkcji, nabywania, dostarczania, integracji, eksploatacji i konserwacji oraz utylizacji następujących systemów, komponentów systemu lub usług systemowych: [*Realizacja: określone przez organizację systemy, komponenty systemu lub usługi systemowe*];

b. Przeglądanie i aktualizacja planu zarządzania ryzykiem w łańcuchu dostaw [*Realizacja: częstotliwość określona przez organizację*] lub w razie potrzeby w celu uwzględnienia zagrożeń, zmian organizacyjnych lub środowiskowych; oraz

c. Ochrona planu zarządzania ryzykiem w łańcuchu dostaw przed nieautoryzowanym ujawnieniem i modyfikacją.

Omówienie: Zależność od produktów, systemów i usług pochodzących od zewnętrznych dostawców, jak również charakter relacji z tymi dostawcami, stwarzają coraz większe ryzyko dla organizacji. Działania zagrażające, które mogą zwiększyć ryzyko związane z bezpieczeństwem lub prywatnością, obejmują nieautoryzowaną produkcję, wprowadzanie lub stosowanie podróbek, manipulowanie, kradzież, wprowadzanie złośliwego oprogramowania i sprzętu oraz złe praktyki produkcyjne i rozwojowe w łańcuchu dostaw. Ryzyko związane z łańcuchem dostaw może mieć charakter endemiczny lub systemowy w obrębie elementu lub komponentu systemu, systemu, organizacji, sektora lub kraju. Zarządzanie ryzykiem w łańcuchu dostaw jest złożonym, wieloaspektowym przedsięwzięciem, które wymaga skoordynowanego wysiłku całej organizacji w celu budowania relacji zaufania i komunikacji z wewnętrznymi i zewnętrznymi interesariuszami. Działania związane z zarządzaniem ryzykiem w łańcuchu dostaw (ang. Supply chain risk management - SCRM) obejmują identyfikację i ocenę ryzyka, określanie odpowiednich działań w odpowiedzi na ryzyko, opracowywanie planów SCRM w celu udokumentowania działań w

odpowiedzi na ryzyko oraz monitorowanie wyników działań wynikających z tych planów. Plan SCRM (na poziomie systemu) jest specyficzny dla danego wdrożenia, zapewniając realizację polityki, wymagania, ograniczenia i implikacje. Może on być samodzielny lub włączony do planów bezpieczeństwa i ochrony prywatności systemu. Plan SCRM dotyczy zarządzania, wdrażania i monitorowania zabezpieczeń SCRM oraz rozwoju / utrzymania systemów w całym cyklu życia systemu (ang. System Development Life Cycle - SDLC) w ramach wspierania misji i funkcji biznesowych.

Ponieważ łańcuchy dostaw mogą się znacznie różnić w zależności od organizacji, plany SCRM są dostosowywane do poszczególnych programów, organizacji i kontekstów operacyjnych. Dostosowane plany SCRM stanowią podstawę do określenia, czy dana technologia, usługa, komponent systemu lub system jest dopasowany do celu, a w związku z tym zabezpieczenia muszą być odpowiednio dobrane. Dostosowane plany SCRM pomagają organizacjom skupić swoje zasoby na najbardziej krytycznych funkcjach misji i biznesu w oparciu o wymagania misji i biznesu oraz środowisko ryzyka. Plany zarządzania ryzykiem łańcucha dostaw zawierają określenie tolerancji na ryzyko łańcucha dostaw w danej organizacji; akceptowalne strategie lub mechanizmy bezpieczeństwa ograniczające ryzyko łańcucha dostaw; proces ciągłej oceny i monitorowania ryzyka łańcucha dostaw; metody wdrażania i ogłaszania planu; opis i uzasadnienie podjętych działań ograniczających ryzyko łańcucha dostaw oraz związane z tym role i obowiązki. Ponadto, plany zarządzania ryzykiem w łańcuchu dostaw uwzględniają wymagania dotyczące opracowywania godnych zaufania, bezpiecznych, chroniących prywatność i odpornych komponentów i systemów, w tym zastosowanie zasad projektowania bezpieczeństwa, wdrażanych jako część procesów inżynierii bezpieczeństwa systemów opartych na cyklu życia (patrz: zabezpieczenie SA-8).

Zabezpieczenia powiązane: CA-2, CP-4, IR-4, MA-2, MA-6, PE-16, PL-2, PM-9, PM-30, RA-3, RA-7, SA-8, SI-4.

Zabezpieczenia rozszerzone:

(1) PLAN ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW | POWOŁANIE ZESPOŁU ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW

Powołanie zespołu zarządzania ryzykiem w łańcuchu dostaw składającego się z [***Realizacja: określony przez organizację personel, role i obowiązki***]**,** ***który będzie*** **prowadził i wspierał następujące działania** ***związane z zarządzaniem ryzykiem w łańcuchu dostaw*** **(SCRM):** [***Realizacja: działania w zakresie zarządzania ryzykiem w łańcuchu dostaw określone przez organizację***]**.**

Omówienie: W celu wdrożenia planów zarządzania ryzykiem w łańcuchu dostaw organizacja ustanawia skoordynowane, oparte na pracy zespołowej podejście do identyfikacji i oceny ryzyk związanych z łańcuchem dostaw oraz zarządzania tymi ryzykami poprzez zastosowanie programowych i technicznych metod ograniczania ryzyka. Podejście zespołowe umożliwia organizacjom przeprowadzenie analizy własnego łańcucha dostaw, komunikację z wewnętrznymi i zewnętrznymi partnerami lub interesariuszami oraz uzyskanie szerokiego poparcia w kwestii odpowiednich zasobów dla SCRM. Zespół SCRM składa się z personelu organizacyjnego o różnych rolach i obowiązkach w zakresie prowadzenia i wspierania działań SCRM, w tym osób odpowiedzialnych za zarządzanie ryzykiem, technologię informacyjną, zamówienia, bezpieczeństwo informacji, prywatność, misję lub biznes, prawo, łańcuch dostaw i logistykę, zaopatrzenie, ciągłość działania i inne istotne funkcje. Członkowie zespołu SCRM są włączani w różne procesy SDLC i posiadają wiedzę i doświadczenie w zakresie procesów pozyskiwania, praktyk prawnych, podatności, zagrożeń i wektorów ataków, a także rozumieją techniczne aspekty i zależności systemów. Zespół SCRM może stanowić rozbudowaną część procesów zarządzania ryzykiem związanym z bezpieczeństwem i prywatnością lub być włączony, jako część organizacyjnego zespołu zarządzania ryzykiem.

Zabezpieczenia powiązane: Brak.

Referencje: [FASC18], [41 CFR 201], [EO 13873], [NIST SP 800-30], [NIST SP 800-39], [SP 800-160-1], [NIST SP 800-161], [NIST SP 800-181], [CNSSD 505], [IR 7622], [IR 8272].

SR-3 ZABEZPIECZENIA I PROCESY W ŁAŃCUCHU DOSTAW

Zabezpieczenie podstawowe:

a. Ustanowienie procesów służących do identyfikacji i eliminacji słabych punktów lub braków w elementach i procesach łańcucha dostaw [*Realizacja: zdefiniowany przez organizację system lub komponent systemu*] w koordynacji z [*Realizacja: zdefiniowany przez organizację personel łańcucha dostaw*];

b. Stosowanie następujących zabezpieczeń w celu ochrony przed ryzykiem powiązanym z łańcuchem dostaw systemu, komponentu systemu lub usługi systemowej oraz w celu ograniczenia szkód lub konsekwencji wynikających ze zdarzeń związanych z łańcuchem dostaw: [*Realizacja: określone przez organizację zabezpieczenia łańcucha dostaw*]; oraz

c. Dokumentowanie wybranych i wdrożonych procesów i zabezpieczeń łańcucha dostaw w [*Wybór: plan bezpieczeństwa i ochrony prywatności; plan zarządzania ryzykiem w łańcuchu dostaw;* [Realizacja: *dokument zdefiniowany przez organizację*]].

Omówienie: Elementy łańcucha dostaw obejmują organizacje, podmioty lub narzędzia wykorzystywane do badań i rozwoju, projektowania, produkcji, nabywania, dostarczania, integracji, eksploatacji i konserwacji oraz utylizacji systemów i komponentów systemu. Procesy łańcucha dostaw obejmują procesy opracowywania sprzętu, oprogramowania i firmware'u (oprogramowania układowego); procedury wysyłki i obsługi; bezpieczeństwo personelu i programy bezpieczeństwa fizycznego; narzędzia, techniki i środki zarządzania konfiguracją w celu zapewnienia autentyczności pochodzenia; lub inne programy, procesy lub procedury związane z opracowywaniem, nabyciem, utrzymaniem i usuwaniem systemów i komponentów systemów. Elementy i procesy łańcucha dostaw mogą być dostarczane przez organizacje, integratorów systemów lub dostawców zewnętrznych. Podatności lub braki w elementach lub procesach łańcucha dostaw stanowią potencjalne słabe punkty, które mogą zostać

wykorzystane przez przeciwników do wyrządzenia szkody organizacji i wpłynąć na jej zdolność do wykonywania podstawowych misji lub funkcji biznesowych. Personel łańcucha dostaw to osoby pełniące role i obowiązki w łańcuchu dostaw.

Zabezpieczenia powiązane: CA-2, MA-2, MA-6, PE-3, PE-16, PL-8, PM-30, SA-2, SA-3, SA-4, SA-5, SA-8, SA-9, SA-10, SA-15, SC-7, SC-29, SC-30, SC-38, SI-7, SR-6, SR-9, SR-11.

Zabezpieczenia rozszerzone:

(1) ZABEZPIECZENIA I PROCESY W ŁAŃCUCHU DOSTAW | ZRÓŻNICOWANA BAZA DOSTAW

Wykorzystywanie zróżnicowanych źródeł dostaw następujących komponentów systemu i usług: [***Realizacja: zdefiniowane przez organizację komponenty systemu i usługi***]**.**

Omówienie: Dywersyfikacja dostaw systemów, komponentów systemu i usług może zmniejszyć prawdopodobieństwo, że przeciwnicy z powodzeniem zidentyfikują i ukierunkują łańcuch dostaw oraz może zmniejszyć wpływ zdarzenia w łańcuchu dostaw lub kompromitacji. Zidentyfikowanie wielu dostawców komponentów zamiennych może zmniejszyć prawdopodobieństwo, że dany komponent zamienny stanie się niedostępny. Zatrudnienie zróżnicowanej grupy deweloperów lub dostawców usług logistycznych może zmniejszyć wpływ klęski żywiołowej lub innego zdarzenia w łańcuchu dostaw. Organizacje rozważają zaprojektowanie systemu w taki sposób, aby obejmował on różnorodne materiały i komponenty.

Zabezpieczenia powiązane: Brak.

(2) ZABEZPIECZENIA I PROCESY W ŁAŃCUCHU DOSTAW | OGRANICZANIE SZKODY

Stosowanie następujące zabezpieczeń w celu ograniczenia szkód wyrządzanych przez potencjalnych przeciwników, którzy identyfikują i ukierunkowują łańcuch

dostaw organizacji: [***Realizacja: zabezpieczenia zdefiniowane przez organizację***]**.**

Omówienie: Zabezpieczenia, które można wdrożyć w celu zmniejszenia prawdopodobieństwa pomyślnej identyfikacji i ukierunkowania przeciwników w łańcuchu dostaw obejmują: unikanie zakupu specjalnych lub niestandardowych konfiguracji, stosowanie zatwierdzonych list dostawców o ustalonej renomie w branży, przestrzeganie wcześniej uzgodnionych harmonogramów konserwacji oraz mechanizmów dostarczania aktualizacji i poprawek, utrzymywanie planu awaryjnego na wypadek zdarzenia w łańcuchu dostaw, stosowanie klauzul wykluczeń w zamówieniach, które zapewniają wyjątki od zobowiązań lub obowiązków, stosowanie zróżnicowanych tras dostaw oraz minimalizowanie czasu pomiędzy decyzją o zakupie a dostawą.

Zabezpieczenia powiązane: Brak.

(3) ZABEZPIECZENIA I PROCESY W ŁAŃCUCHU DOSTAW | PODWYKONAWCY

Zapewnienie, że zabezpieczenia zawarte w umowach z głównymi wykonawcami są również zawarte w umowach z podwykonawcami.

Omówienie: W celu skutecznego i wszechstronnego zarządzania ryzykiem w łańcuchu dostaw, ważne jest, aby organizacje uwzględniały zabezpieczenia zarządzania ryzykiem w łańcuchu dostaw na wszystkich szczeblach łańcucha. Obejmuje to zapewnienie, że wykonawcy pierwszego (głównego) szczebla wdrożyli procesy ułatwiające "przepływ" zabezpieczeń zarządzania ryzykiem w ramach łańcucha dostaw do wykonawców niższego szczebla. Zabezpieczenia podlegające procedurze "przepływu w dół" są określone w zabezpieczeniu podstawowym SR-3b.

Zabezpieczenia powiązane: SR-5, SR-8.

Referencje: [FASC18], [41 CFR 201], [EO 13873], [ISO 20243], [NIST SP 800-30], [NIST SP 800-161], [IR 7622].

SR-4 POCHODZENIE

Zabezpieczenie podstawowe: Dokumentowanie, monitorowanie i utrzymywanie autentyczności pochodzenia następujących systemów, komponentów systemu i związanych z nimi danych: [*Realizacja: określone przez organizację systemy, komponenty systemu i związane z nimi dane*].

Omówienie: Każdy system i komponent systemu ma swoje źródło i może być modyfikowane przez cały okres swojego istnienia. Pochodzenie to chronologia źródła, rozwoju, własności, lokalizacji oraz zmian w systemie lub komponencie systemu i związanych z nim danych. Może ono również obejmować personel i procesy wykorzystywane do interakcji z systemem, komponentem lub powiązanymi danymi lub do wprowadzania w nich zmian. Organizacje rozważają opracowanie procedur (patrz: zabezpieczenie SR-1) dotyczących podziału rozliczalności za tworzenie, utrzymanie i monitorowanie pochodzenia systemów i komponentów systemu; przekazywanie dokumentacji pochodzenia i rozliczalności pomiędzy organizacjami; oraz zapobieganie i monitorowanie nieautoryzowanych zmian w dokumentacji pochodzenia. Organizacje posiadają metody dokumentowania, monitorowania i utrzymywania aktualnych baz danych dotyczących pochodzenia systemów, komponentów systemu i związanych z nimi danych. Działania te pomagają śledzić, oceniać i dokumentować wszelkie zmiany w pochodzeniu, w tym zmiany w elementach łańcucha dostaw lub konfiguracji, oraz pomagają zapewnić niezaprzeczalność informacji o pochodzeniu i zapisów dokonywanych zmian w pochodzeniu. Kwestie związane z pochodzeniem są uwzględniane w całym cyklu życia systemu i w stosownych przypadkach włączane do umów i innych porozumień.

Zabezpieczenia powiązane: CM-8, MA-2, MA-6, RA-9, SA-3, SI-4.

Zabezpieczenia rozszerzone:

(1) POCHODZENIE | TOŻSAMOŚĆ

Ustanowienie i utrzymanie unikalnej identyfikacji następujących elementów łańcucha dostaw, procesów i personelu związanego ze zidentyfikowanym systemem i krytycznymi elementami systemu: [***Realizacja: zdefiniowane przez organizację elementy łańcucha dostaw, procesy i personel związany ze zdefiniowanymi przez organizację systemami i krytycznymi elementami systemu.***

Omówienie: Wiedza o tym, kto i co znajduje się w łańcuchach dostaw organizacji, jest krytyczna dla uzyskania przejrzystości działań w łańcuchu dostaw. Przejrzystość działań w łańcuchu dostaw jest również ważna dla monitorowania i identyfikowania zdarzeń i działań wysokiego ryzyka. Bez odpowiedniej znajomości elementów łańcucha dostaw, procesów i personelu, organizacjom bardzo trudno jest zrozumieć i zarządzać ryzykiem oraz zmniejszyć podatność na niekorzystne zdarzenia. Elementy łańcucha dostaw obejmują organizacje, podmioty lub narzędzia wykorzystywane do badań i rozwoju, projektowania, wytwarzania, pozyskiwania, dostarczania, integracji, eksploatacji, utrzymania i utylizacji systemów i ich komponentów. Procesy w łańcuchu dostaw obejmują procesy rozwojowe sprzętu, oprogramowania i oprogramowania układowego; procedury wysyłki i obsługi; narzędzia, techniki i środki zarządzania konfiguracją służące zapewnieniu pochodzenia; programy bezpieczeństwa osobowego i fizycznego; lub inne programy, procesy lub procedury związane z produkcją i dystrybucją elementów łańcucha dostaw. Personel łańcucha dostaw to osoby pełniące określone role i obowiązki związane z zabezpieczaniem badań i rozwoju, projektowania, produkcji, nabywania, dostarczania, integracji, eksploatacji i utrzymania oraz utylizacji systemu lub jego elementu. Metody identyfikacji umożliwiają wsparcie dochodzenia w przypadku zmiany w łańcuchu dostaw (np. w przypadku zakupu firmy dostawczej), naruszenia lub zdarzenia.

Zabezpieczenia powiązane: IA-2, IA-8, PE-16.

(2) POCHODZENIE | ŚLEDZENIE PRZESYŁEK

Ustanowienie i utrzymywanie unikalnej identyfikacji następujących systemów i krytycznych elementów systemu w celu śledzenia ich w całym łańcuchu dostaw: [***Realizacja: określone przez organizację systemy i krytyczne komponenty systemu***]**.**

Omówienie: Możliwość śledzenia unikalnej identyfikacji systemów i ich komponentów podczas działań związanych z rozwojem i transportem umożliwia ustalenie i zachowanie pochodzenia. Na przykład komponenty systemu mogą być oznaczane za pomocą etykiet z numerami seryjnymi lub tagowane za pomocą znaczników radiowych. Etykiety i znaczniki mogą pomóc w zapewnieniu lepszej widoczności pochodzenia systemu lub komponentu systemu. System lub komponent systemu może mieć więcej niż jeden niepowtarzalny identyfikator. Metody identyfikacji są wystarczające, aby wspomóc dochodzenie kryminalistyczne po naruszeniu łańcucha dostaw lub zdarzeniu z nim związanym.

Zabezpieczenia powiązane: IA-2, IA-8, PE-16, PL-2.

(3) POCHODZENIE |POTWIERDZANIE AUTENTYCZNOŚCI I NIEZMIENNOŚCI

Stosowanie następujących zabezpieczeń w celu potwierdzenia, że otrzymany system lub element systemu jest autentyczny i nie został zmieniony,: [***Realizacja: zabezpieczenia zdefiniowane przez organizację***]**.**

Omówienie: W przypadku wielu systemów i komponentów systemowych, zwłaszcza sprzętu komputerowego, istnieją środki techniczne umożliwiające ustalenie, czy elementy są oryginalne, czy też zostały zmienione. Są to np. znakowanie optyczne i nanotechnologiczne, funkcje fizycznie nieklonowalne, analiza bocznokanałowa, kryptograficzna weryfikacja haszu lub podpis cyfrowy oraz widoczne etykiety lub naklejki zabezpieczające przed manipulacją. Zabezpieczenia mogą również obejmować monitorowanie działania niezgodnego

ze specyfikacją, co może być wskaźnikiem manipulowania lub podróbek. Organizacje mogą wykorzystywać procesy dostawców i wykonawców do sprawdzania, czy system lub komponent jest autentyczny i nie został zmieniony oraz do zamiany podejrzanego systemu lub komponentu na nowy. Niektóre oznaki manipulacji mogą być widoczne i możliwe do wyeliminowania przed przyjęciem dostawy, np. nieodpowiednie opakowanie, zerwane plomby i nieprawidłowe etykiety. W przypadku podejrzenia, że system lub jego komponent został zmieniony lub podrobiony, dostawca, wykonawca lub producent oryginalnego sprzętu może być w stanie wymienić taki element lub zapewnić zdolność kryminalistyczną w celu ustalenia pochodzenia podrobionego lub zmienionego elementu. Organizacje mogą zapewnić szkolenia personelu w zakresie identyfikacji podejrzanych dostaw systemów lub komponentów.

Zabezpieczenia powiązane: AT-3, SR-9, SR-10, SR-11.

(4) POCHODZENIE | INTEGRALNOŚĆ ŁAŃCUCHA DOSTAW - POCHODZENIE

Stosowanie [***Realizacja: zdefiniowane przez organizację zabezpieczenia***] **i prowadzenie** [***Realizacja: zdefiniowana przez organizację analiza***] **w celu zapewnienia integralności systemu i jego komponentów poprzez walidację wewnętrznego składu i pochodzenia krytycznych lub istotnych technologii, produktów i usług.**

Omówienie: Wiarygodne informacje dotyczące wewnętrznego składu komponentów systemu oraz pochodzenia technologii, produktów i usług stanowią mocną podstawę zaufania. Weryfikacja wewnętrznego składu i pochodzenia technologii, produktów i usług jest określana mianem rodowodu. W przypadku mikroelektroniki obejmuje to skład materiałowy komponentów. W przypadku oprogramowania obejmuje to strukturę kodu open-source i kodu własnościowego, w tym wersję komponentu w danym punkcie w czasie. Rodowody zwiększają pewność, że roszczenia dostawców dotyczące wewnętrznego składu i pochodzenia dostarczanych przez nich produktów, usług

i technologii są uzasadnione. Weryfikacja wewnętrznego składu i pochodzenia może być osiągnięta poprzez różne artefakty dowodowe lub zapisy, które producenci i dostawcy tworzą podczas badań i rozwoju, projektowania, produkcji, nabywania, dostarczania, integracji, eksploatacji i utrzymania oraz utylizacji technologii, produktów i usług. Artefakty dowodowe obejmują, ale nie ograniczają się do znaczników identyfikacji oprogramowania (*ang. software identification - SWID*), wykazu komponentów oprogramowania, deklaracji producentów dotyczących atrybutów platformy (np. numerów seryjnych, wykazu komponentów sprzętu) oraz pomiarów (np. haszy firmware), które są ściśle związane z samym sprzętem.

Zabezpieczenia powiązane: RA-3.

Referencje: [FASC18], [41 CFR 201], [EO 13873], [ISO 27036], [ISO 20243], [NIST SP 800-160-1], [NIST SP 800-161], [IR 7622], [IR 8112], [IR 8272].

SR-5 STRATEGIE, NARZĘDZIA I METODY NABYCIA

Zabezpieczenie podstawowe: Stosowanie następujących strategii pozyskiwania, narzędzi zawierania umów i metod zaopatrzenia w celu ochrony przed ryzykiem związanym z łańcuchem dostaw, jego identyfikacji i ograniczania: [*Realizacja: określone przez organizację strategie nabywania, narzędzia kontraktowe i metody zaopatrzenia*].

Omówienie: Wykorzystanie procesu nabywania stanowi ważne narzędzie ochrony łańcucha dostaw. Dostępnych jest wiele użytecznych narzędzi i technik, w tym ukrycie końcowego przeznaczenia systemu lub jego komponentu, stosowanie zakupów w ciemno lub filtrowanych, wymaganie opakowań umożliwiających łatwe stwierdzenie ich naruszenia oraz stosowanie zaufanej lub kontrolowanej dystrybucji. Wyniki oceny ryzyka łańcucha dostaw mogą stanowić wskazówkę i źródło informacji na temat strategii, narzędzi i metod, które mają największe zastosowanie w danej sytuacji. Narzędzia i techniki mogą zapewnić ochronę przed nieuprawnioną produkcją, kradzieżą, manipulacją, wprowadzaniem podróbek, wprowadzaniem złośliwego oprogramowania lub "tylnych furtek" oraz złymi praktykami rozwojowymi w całym cyklu życia systemu. Organizacje rozważają również wprowadzenie zachęt dla dostawców, którzy wdrażają mechanizmy zabezpieczające, promują przejrzystość swoich procesów oraz praktyk w zakresie bezpieczeństwa i ochrony prywatności, wprowadzają zapisy w umowach dotyczące zakazu stosowania skażonych lub podrobionych komponentów oraz ograniczają zakupy od niegodnych zaufania dostawców. Organizacje rozważają zapewnienie szkoleń, kursów i programów uświadamiających personel w zakresie ryzyka związanego z łańcuchem dostaw, dostępnych strategii ograniczających oraz sytuacji, w których programy te powinny być stosowane. Metody przeglądania i ochrony planów rozwojowych, dokumentacji i dowodów są współmierne do wymagań bezpieczeństwa i ochrony prywatności organizacji. Kontrakty mogą określać wymagania dotyczące ochrony dokumentacji.

Zabezpieczenia powiązane: AT-3, SA-2, SA-3, SA-4, SA-5, SA-8, SA-9, SA-10, SA-15, SR-6, SR-9, SR-10, SR-11.

Zabezpieczenia rozszerzone:

(1) STRATEGIE, NARZĘDZIA I METODY NABYCIA | ODPOWIEDNIE ZAOPATRZENIE

Stosowanie następujących środki bezpieczeństwa w celu zapewnienia odpowiedniego zaopatrzenia [***Realizacja: zdefiniowane przez organizację krytyczne komponenty systemu***]**:** [***Realizacja: środki bezpieczeństwa zdefiniowane przez organizację***]**.**

Omówienie: Adwersarze mogą próbować utrudniać operacje organizacyjne poprzez zakłócanie dostaw krytycznych komponentów systemu lub zaburzanie działań dostawców. Organizacje mogą monitorować średni czas bezawaryjnej pracy systemów i komponentów, aby zminimalizować tymczasową lub stałą utratę funkcji systemu. Zabezpieczenia mające na celu zapewnienie odpowiednich dostaw krytycznych komponentów systemu obejmują korzystanie z wielu dostawców określonych krytycznych komponentów w całym łańcuchu dostaw, gromadzenie zapasowych komponentów w celu zapewnienia działania w czasie krytycznym oraz identyfikację funkcjonalnie identycznych lub podobnych komponentów możliwych do zastosowania w razie potrzeby.

Zabezpieczenia powiązane: RA-9.

(2) STRATEGIE, NARZĘDZIA I METODY NABYCIA | OCENY PRZED WYBOREM, AKCEPTACJĄ, MODYFIKACJĄ LUB AKTUALIZACJĄ

Dokonywanie oceny systemu, komponentu systemu lub usługi systemowej przed jego wyborem, akceptacją, modyfikacją lub aktualizacją.

Omówienie: Personel organizacyjny lub niezależne, zewnętrzne podmioty przeprowadzają oceny systemów, komponentów, produktów, narzędzi i usług w celu wykrycia dowodów ingerencji, niezamierzonych i celowych podatności lub dowodów braku zgodności z kontrolą łańcucha dostaw. Należą do

nich złośliwy kod, złośliwe procesy, wadliwe oprogramowanie, furtki oraz podróbki. Oceny mogą obejmować oszacowania, przeglądy propozycji projektowych; inspekcje wizualne lub fizyczne; analizy statyczne i dynamiczne; inspekcje wizualne, rentgenowskie, lub defotoskopię magnetyczną cząsteczek; symulacje, testy białej, szarej lub czarnej skrzynki; testy odporności na błędne dane; testy obciążenia i testy penetracyjne (patrz SR-6(1)). Dowody uzyskane podczas oceny są dokumentowane w celu podjęcia dalszych działań przez organizację. Dowody wygenerowane podczas organizacyjnych lub niezależnych ocen elementów łańcucha dostaw mogą być wykorzystane do doskonalenia procesów łańcucha dostaw i informowania o procesie zarządzania ryzykiem w łańcuchu dostaw. Dowody te mogą być wykorzystane w kolejnych ocenach. Dowody i inna dokumentacja mogą być udostępniane zgodnie z umowami organizacyjnymi.

Zabezpieczenia powiązane: CA-8, RA-5, SA-11, SI-7.

Referencje: [FASC18], [41 CFR 201], [EO 13873], [ISO 27036], [ISO 20243], [NIST SP 800-30], [NIST SP 800- 161], [IR 7622], [IR 8272].

SR-6 OCENY I RECENZJE DOSTAWCÓW

Zabezpieczenie podstawowe: Ocena i przegląd ryzyka związanego z łańcuchem dostaw, dotyczącego dostawców lub wykonawców oraz dostarczanego przez nich systemu, komponentu systemu lub usługi systemowej [*Realizacja: częstotliwość określona przez organizację*].

Omówienie: Ocena i przegląd ryzyka dostawcy obejmuje procesy zarządzania bezpieczeństwem i ryzykiem łańcucha dostaw; kontrolę lub wpływy kapitału zagranicznego (*ang. foreign ownership, control or influence - FOCI*); oraz zdolność dostawcy do skutecznego oceniania podległych dostawców i wykonawców drugiego i trzeciego szczebla. Przeglądy mogą być prowadzone przez organizację lub przez niezależną stronę trzecią. W przeglądach uwzględnia się udokumentowane procesy, udokumentowane zabezpieczenia, informacje pochodzące ze wszystkich źródeł oraz publicznie dostępne informacje dotyczące dostawcy lub wykonawcy. Organizacje mogą wykorzystywać informacje z otwartych źródeł do monitorowania oznak kradzieży danych, złych praktyk w zakresie rozwoju i kontroli jakości, wycieków informacji lub podróbek. W niektórych przypadkach może być właściwe lub wymagane udostępnienie wyników oceny i przeglądu innym organizacjom zgodnie z wszelkimi obowiązującymi zasadami, polityką lub umowami i porozumieniami międzyorganizacyjnymi.

Zabezpieczenia powiązane: SR-3, SR-5.

Zabezpieczenia rozszerzone:

(1) OCENY I RECENZJE DOSTAWCÓW | BADANIA I ANALIZY

Stosowanie [***Wybór (jeden lub więcej): analiza organizacyjna; niezależna analiza zewnętrzna; testy organizacyjne; niezależne testy zewnętrzne***] **następujących elementów łańcucha dostaw, procesów i podmiotów związanych z systemem, komponentem systemu lub usługą systemową:**

[Realizacja: *zdefiniowane przez organizację elementy, procesy i podmioty łańcucha dostaw*].

Omówienie: Pod uwagę brane są relacje pomiędzy podmiotami i procedurami w ramach łańcucha dostaw, w tym rozwój i dostawy. Elementy łańcucha dostaw obejmują organizacje, podmioty lub narzędzia, które są wykorzystywane do badań i rozwoju, projektowania, wytwarzania, nabywania, dostarczania, integracji, eksploatacji, utrzymania i utylizacji systemów, komponentów systemów lub usług systemowych. Procesy łańcucha dostaw obejmują programy zarządzania ryzykiem w łańcuchu dostaw; strategie i plany wdrożenia SCRM[111]; programy bezpieczeństwa osobowego i fizycznego; procesy rozwoju sprzętu, oprogramowania i firmware'u; narzędzia, techniki i środki zarządzania konfiguracją w celu zapewnienia pochodzenia; procedury wysyłki i obsługi; oraz programy, procesy lub procedury związane z produkcją i dystrybucją elementów łańcucha dostaw. Uczestnicy łańcucha dostaw to osoby pełniące określone role i obowiązki w łańcuchu dostaw. Dowody wygenerowane i zebrane podczas analiz i testów elementów łańcucha dostaw, procesów i aktorów są dokumentowane i wykorzystywane do informowania o działaniach i decyzjach w zakresie zarządzania ryzykiem organizacyjnym.

Zabezpieczenia powiązane: CA-8, SI-4.

Referencje: [FASC18], [41 CFR 201], [EO 13873], [ISO 27036], [ISO 20243], [FIPS 140-3], [FIPS 180-4], [FIPS 186-4], [FIPS 202], [NIST SP 800-30], [NIST SP 800-161], [IR 7622], [IR 8272].

[111] Patrz: NSC 800-37; NSC 7298.

SR-7 BEZPIECZEŃSTWO OPERACJI W RAMACH ŁAŃCUCHA DOSTAW

Zabezpieczenie podstawowe: Stosowanie następujących środki bezpieczeństwa operacyjnego (*ang. Operations Security - OPSEC*) w celu ochrony informacji powiązanych z łańcuchem dostaw systemu, komponentu systemu lub usługi systemowej: [*Realizacja: określone przez organizację zabezpieczenia w zakresie bezpieczeństwa operacyjnego (OPSEC)*].

Omówienie: Łańcuch dostaw OPSEC rozszerza zakres działania OPSEC o dostawców i potencjalnych dostawców. OPSEC jest procesem obejmującym identyfikację informacji krytycznych, analizę przyjaznych działań związanych z operacjami i innymi działaniami w celu zidentyfikowania czynności, które mogą być obserwowane przez potencjalnych przeciwników, określenie wskaźników, które potencjalni przeciwnicy mogą uzyskać, a które mogą być analizowane i łączone w celu uzyskania informacji w czasie wystarczającym do wyrządzenia szkód organizacjom, wdrożenie zabezpieczeń lub środków zaradczych w celu wyeliminowania lub zmniejszenia podatności i ryzyka do akceptowalnego poziomu oraz rozważenie, w jaki sposób zagregowane informacje mogą narazić użytkowników lub konkretne rodzaje wykorzystania łańcucha dostaw. Informacje dotyczące łańcucha dostaw obejmują tożsamość użytkowników, przeznaczenia systemów, komponentów systemów i usług systemowych, tożsamość dostawców, wymagania dotyczące bezpieczeństwa i prywatności, konfiguracje systemów i komponentów, procesy dostawców, specyfikacje projektowe oraz wyniki testów i ocen. OPSEC łańcucha dostaw może wymagać od organizacji nieujawniania dostawcom informacji dotyczących misji lub działalności i może obejmować wykorzystanie pośredników w celu nieujawnienia przeznaczenia lub użytkowników końcowych systemów, komponentów systemów lub usług systemowych.

Zabezpieczenia powiązane: SC-38.

Zabezpieczenia rozszerzone: Brak.

Referencje: [EO 13873], [NIST SP 800-30], [ISO 27036], [NIST SP 800-161], [IR 7622].

SR-8 UMOWY DOTYCZĄCE POWIADOMIEŃ

Zabezpieczenie podstawowe: Tworzenie umów i procedur z podmiotami uczestniczącymi w łańcuchu dostaw systemu, komponentu systemu lub usługi systemowej w celu przekazywania [*Wybór (jeden lub więcej): zawiadomienie o naruszeniach w łańcuchu dostaw; wyniki oceny lub audytu;* [*Realizacja: informacje określone przez organizację*]].

Omówienie: Ustanowienie umów i procedur ułatwia komunikację pomiędzy podmiotami z łańcucha dostaw. Wczesne powiadamianie o naruszeniach i potencjalnych ujawnieniach w łańcuchu dostaw, które mogą mieć lub miały negatywny wpływ na systemy organizacyjne lub komponenty systemu, jest niezbędne, aby organizacje mogły skutecznie reagować na takie zdarzenia. Wyniki ocen lub audytów mogą obejmować informacje pochodzące z otwartych źródeł, które przyczyniły się do podjęcia decyzji lub osiągnięcia wyniku i mogą zostać wykorzystane do pomocy jednostce obsługującej łańcuch dostaw w rozwiązaniu problemu lub udoskonaleniu jej procesów.

Zabezpieczenia powiązane: IR-4, IR-6, IR-8.

Zabezpieczenia rozszerzone: Brak.

Referencje: [FASC18], [41 CFR 201], [EO 13873], [ISO 27036], [NIST SP 800-30], [NIST SP 800-161], [IR 7622].

SR-9 ODPORNOŚĆ NA MANIPULACJE I WYKRYWANIE SABOTAŻU

Zabezpieczenie podstawowe: Wdrożenie programu zabezpieczającego przed manipulacją przy systemie, komponencie systemu lub usłudze systemowej.

Omówienie: Technologie, narzędzia i techniki przeciwdziałania manipulacjom zapewniają stosowny poziom ochrony systemów, komponentów systemu i usług przed wieloma zagrożeniami, w tym inżynierią odwrotną, modyfikacją i zastępowaniem. Silna identyfikacja połączona z odpornością na manipulacje i/lub wykrywaniem manipulacji ma zasadnicze znaczenie dla ochrony systemów i komponentów podczas dystrybucji i w trakcie użytkowania.

Zabezpieczenia powiązane: PE-3, PM-30, SA-15, SI-4, SI-7, SR-3, SR-5, SR-10, SR-11.

Zabezpieczenia rozszerzone:

(1) ODPORNOŚĆ NA MANIPULACJE I WYKRYWANIE SABOTAŻU | WIELOETAPOWY CYKL ŻYCIA SYSTEMU

Stosowanie technologii, narzędzi i technik antysabotażowych przez cały cykl życia systemu.

Omówienie: Cykl życia systemu obejmuje badania i rozwój, projektowanie, produkcję, pozyskiwanie, dostarczanie, integrację, eksploatację i utrzymanie oraz utylizację. Organizacje stosują połączenie technik sprzętowych i programowych w celu zapewnienia odporności na manipulacje i wykrywanie. Organizacje stosują zamaskowanie i samozabezpieczenie, aby utrudnić inżynierię odwrotną i modyfikacje, które są czasochłonne i kosztowne dla przeciwników. Dostosowywanie systemów i komponentów systemu do indywidualnych potrzeb może ułatwić wykrywanie zamienników, a tym samym ograniczyć uszkodzenia.

Zabezpieczenia powiązane: SA-3.

Referencje: [ISO 20243].

SR-10 KONTROLA SYSTEMÓW / KOMPONENTÓW

Zabezpieczenie podstawowe: Kontrolowanie [*Wybór (jeden lub więcej): losowo;* z [Realizacja: *częstotliwość zdefiniowana przez organizację*] następujących systemów lub komponentów systemu po wystąpieniu [*Realizacja: zdefiniowane przez organizację przesłanki przeprowadzenia inspekcji*]] w celu wykrycia ingerencji w: [*Realizacja: systemy lub części składowe systemu określone przez organizację*].

Omówienie: Inspekcja systemów lub komponentów systemów pod kątem odporności na manipulacje i wykrywania dotyczy fizycznych i logicznych manipulacji i jest stosowana do systemów i komponentów systemów usuniętych z obszarów kontrolowanych przez organizację. Wskaźniki wymagające przeprowadzenia inspekcji obejmują zmiany w opakowaniu, specyfikacjach, lokalizacji fabryki lub podmiotu, w którym część została zakupiona, a także po powrocie osób z delegacji do miejsc wysokiego ryzyka.

Zabezpieczenia powiązane: AT-3, PM-30, SI-4, SI-7, SR-3, SR-4, SR-5, SR-9, SR-11.

Referencje: [ISO 20243].

SR-11 AUTENTYCZNOŚĆ KOMPONENTU

Zabezpieczenie podstawowe:

a. Opracowanie i wdrożenie polityki i procedur walki z fałszerstwami, które obejmują środki wykrywania i zapobiegania wprowadzaniu podrabianych komponentów do systemu; oraz

b. Zgłaszanie podrobionych elementów systemu do [Wybór (jeden lub więcej): źródło podrobionego elementu; [Realizacja: zdefiniowane przez organizację zewnętrzne organizacje zajmujące się sporządzaniem raportów]; [Realizacja: zdefiniowany przez organizację personel lub role]].

Omówienie: Źródła podrabianych komponentów to producenci, deweloperzy, sprzedawcy i wykonawcy. Polityka i procedury zapobiegające podrabianiu wspierają odporność na manipulacje i zapewniają odpowiedni poziom ochrony przed wprowadzeniem złośliwego kodu.

Zabezpieczenia powiązane: PE-3, SA-4, SI-7, SR-9, SR-10.

Zabezpieczenia rozszerzone:

(1) AUTENTYCZNOŚĆ KOMPONENTU | SZKOLENIE Z ZAKRESU ZAPOBIEGANIA FAŁSZERSTWOM

Szkolenie [***Realizacja: personel lub role zdefiniowane przez organizację***] **w zakresie wykrywania podrobionych elementów systemu (w tym sprzętu, oprogramowania i oprogramowania układowego).**

Omówienie: Brak.

Zabezpieczenia powiązane: AT-3.

(2) AUTENTYCZNOŚĆ KOMPONENTU | ZABEZPIECZENIE KONFIGURACJI SERWISOWANYCH I NAPRAWIANYCH KOMPONENTÓW

Utrzymywanie kontroli konfiguracji następujących komponentów systemu oczekujących na serwis lub naprawę oraz komponentów serwisowanych lub

naprawianych oczekujących na powrót do eksploatacji: [Realizacja: komponenty systemu zdefiniowane przez organizację].

Omówienie: Brak.

Zabezpieczenia powiązane: CM-3, MA-2, MA-4, SA-10.

(3) AUTENTYCZNOŚĆ KOMPONENTU | SKANOWANIE ANTYFAŁSZERSKIE

Skanowanie w poszukiwaniu fałszywych komponentów systemu [***Realizacja: częstotliwość zdefiniowana przez organizację***]**.**

Omówienie: Rodzaj komponentu określa rodzaj skanowania, które ma być przeprowadzone (np. skanowanie aplikacji internetowej, jeśli komponent jest aplikacją internetową).

Zabezpieczenia powiązane: RA-5.

Referencje: [ISO 20243].

SR-12 USUWANIE KOMPONENTÓW

Zabezpieczenie podstawowe: Usuwanie [*Realizacja: dane zdefiniowane przez organizację, dokumentacja, narzędzia lub komponenty systemu*] przy użyciu następujących technik i metod: [*Realizacja: techniki i metody określone przez organizację*].

Omówienie: Dane, dokumentacja, narzędzia lub komponenty systemu mogą być utylizowane w dowolnym momencie cyklu życia systemu (nie tylko w fazie utylizacji lub wycofania z użytkowania). Na przykład, utylizacja może mieć miejsce podczas badań i rozwoju, projektowania, tworzenia prototypów lub obsługi/konserwacji i obejmuje metody takie jak czyszczenie dysku, usuwanie kluczy kryptograficznych, częściowe ponowne użycie komponentów. Możliwości kompromitacji podczas utylizacji mają wpływ na dane fizyczne i logiczne, w tym na dokumentację systemową w postaci papierowej lub cyfrowej; dokumentację wysyłkową i dostawczą; pamięci z kodem oprogramowania; lub kompletne routery lub serwery zawierające trwałe nośniki zawierające informacje wrażliwe lub autorskie. Dodatkowo, prawidłowa utylizacja komponentów systemu przeciwdziała przedostawaniu się ich do obrotu w szarej strefie.

Zabezpieczenia powiązane: MP-6.

Referencje: Brak.

REFERENCJE

	NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA
NSC 199	*Standardy kategoryzacji bezpieczeństwa* – na podstawie FIPS 199
NSC 200	*Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych* – na podstawie FIPS 200
NSC 800-18	*Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych* – na podstawie NIST SP 800- 18
NSC 800-30	*Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne* – na podstawie NIST SP 800-30
NSC 800-34	*Poradnik planowania awaryjnego* – na podstawie NIST SP 800-34
NSC 800-37	*Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu* – na podstawie NIST SP 800-37
NSC 800-53A	*Ocena środków bezpieczeństwa i ochrony prywatności systemów informatycznych oraz organizacji. Tworzenie skutecznych planów oceny* – na podstawie NIST SP 800-53A
NSC 800-53B	*Zabezpieczenia bazowe systemów informatycznych oraz organizacji* – na podstawie NIST SP 800-53B
NSC 800-60	*Wytyczne w zakresie określania kategorii bezpieczeństwa informacji I kategorii bezpieczeństwa systemu informatycznego* – na podstawie NIST SP 800-60
NSC 800-61	*Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego* – na podstawie NIST SP 800-61

LAWS, POLICIES, DIRECTIVES, REGULATIONS, STANDARDS, AND GUIDELINES[112]

LAWS AND EXECUTIVE ORDERS	
[ATOM54]	Atomic Energy Act (P.L. 83-703), August 1954. https://www.govinfo.gov/content/pkg/STATUTE-68/pdf/STATUTE-68-Pg919.pdf
[CMPPA]	Computer Matching and Privacy Protection Act of 1988 (P.L. 100-503), October 1988. https://www.govinfo.gov/content/pkg/STATUTE-102/pdf/STATUTE-102-Pg2507.pdf
[EGOV]	E-Government Act [includes FISMA] (P.L. 107-347), December 2002. https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf
[EVIDACT]	Foundations for Evidence-Based Policymaking Act of 2018 (P.L. 115-435), January 2019. https://www.congress.gov/115/plaws/publ435/PLAW-115publ435.pdf
[FASC18]	Secure Technology Act [includes Federal Acquisition Supply Chain Security Act] (P.L. 115-390), December 2018. https://www.congress.gov/bill/115th-congress/senate-bill/3085
[FISMA]	Federal Information Security Modernization Act (P.L. 113-283), December 2014. https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[FOIA96]	Freedom of Information Act (FOIA), 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996. https://www.govinfo.gov/content/pkg/PLAW-104publ231/pdf/PLAW-104publ231.pdf

[112] W niniejszym dodatku cytowane są te publikacje zewnętrzne, które bezpośrednio wspierają projekty FISMA i ochrony prywatności w NIST. Dodatkowe standardy, wytyczne i raporty NIST są również cytowane w całej publikacji, w tym w części referencyjnej odpowiednich mechanizmów zabezpieczeń w rozdziale trzecim. W celu uzyskania dostępu do tych publikacji podano bezpośrednie linki do strony internetowej NIST.

[PRIVACT]	Privacy Act (P.L. 93-579), December 1974. https://www.govinfo.gov/content/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf
[USA PATRIOT]	USA Patriot Act (P.L. 107-56), October 2001. https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf
[USC 552]	United States Code, 2006 Edition, Supplement 4, Title 5 - *Government Organization and Employees*, January 2011. https://www.govinfo.gov/content/pkg/USCODE-2010-title5/pdf/USCODE-2010-title5-partI-chap5-subchapII-sec552a.pdf
[USC 2901]	United States Code, 2008 Edition, Title 44 - *Public Printing and Documents*, Chapters 29, 31, and 33, January 2012. https://www.govinfo.gov/content/pkg/USCODE-2011-title44/pdf/USCODE-2011-title44-chap29-sec2901.pdf
[USC 3502]	"Definitions," Title 44 U.S. Code, Sec. 3502. 2011 ed. https://www.govinfo.gov/app/details/USCODE-2011-title44/USCODE-2011-title44-chap35-subchapI-sec3502
[USC 11101]	"Definitions," Title 40 U.S. Code, Sec. 11101. 2018 ed. https://www.govinfo.gov/app/details/USCODE-2018-title40/USCODE-2018-title40-subtitleIII-chap111-sec11101
[EO 13526]	Executive Order 13526, Classified National Security Information, December 2009. https://www.archives.gov/isoo/policy-documents/cnsi-eo.html
[EO 13556]	Executive Order 13556, Controlled Unclassified Information, November 2010. https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information
[EO 13587]	Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 2011. https://obamawhitehouse.archives.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net

[EO 13636]	Executive Order 13636, Improving Critical Infrastructure Cybersecurity, February 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
[EO 13800]	Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 2017. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure
[EO 13873]	Executive Order 13873, Executive Order on Securing the Information and Communications Technology and Services Supply Chain, May 2019. https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain
	REGULATIONS, DIRECTIVES, PLANS, AND POLICIES
[HSPD 7]	Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 2003. https://www.dhs.gov/homeland-security-presidential-directive-7
[HSPD 12]	Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 2004. https://www.dhs.gov/homeland-security-presidential-directive-12
[NITP12]	Presidential Memorandum for the Heads of Executive Departments and Agencies, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, November 2012. https://obamawhitehouse.archives.gov/the-press-office/2012/11/21/presidential-memorandum-national-insider-threat-policy-and-minimum-stand
[5 CFR 731]	Code of Federal Regulations, Title 5, Administrative Personnel, Section 731.106, Designation of Public Trust Positions and Investigative Requirements (5 C.F.R. 731.106). https://www.govinfo.gov/content/pkg/CFR-2012-title5-vol2/pdf/CFR-2012-title5-vol2-sec731-106.pdf

[32 CFR 2002]	Code of Federal Regulations, Title 32, Controlled Unclassified Information (32 C.F.R. 2002). https://www.federalregister.gov/documents/2016/09/14/2016-21665/controlled-unclassified-information
[41 CFR 201]	"Federal Acquisition Supply Chain Security Act; Rule," 85 Federal Register 54263 (September 1, 2020), pp 54263-54271. https://www.federalregister.gov/d/2020-18939 [or as published in Title 41 Code of Federal Regulations, Sec. 201 (forthcoming)]
[ODNI NITP]	Office of the Director National Intelligence, National Insider Threat Policy https://www.dni.gov/files/NCSC/documents/nittf/National_Insider_Threat_Policy.pdf
[OMB A-108]	Office of Management and Budget Memorandum Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act, December 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A108/omb_circular_a-108.pdf
[OMB A-130]	Office of Management and Budget Memorandum Circular A-130, Managing Information as a Strategic Resource, July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf
[OMB M-03-22]	Office of Management and Budget Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 2003. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2003/m03_22.pdf
[OMB M-08-05]	Office of Management and Budget Memorandum M-08-05, Implementation of Trusted Internet Connections (TIC), November 2007. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf
[OMB M-17-06]	Office of Management and Budget Memorandum M-17-06, Policies for Federal Agency Public Websites and Digital Services, November 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-06.pdf

[OMB M-17-12]	Office of Management and Budget Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, January 2017. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf
[OMB M-17-25]	Office of Management and Budget Memorandum M-17-25, Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 2017. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/M-17-25.pdf
[OMB M-19-03]	Office of Management and Budget Memorandum M-19-03, Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program, December 2018. https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf
[OMB M-19-15]	Office of Management and Budget Memorandum M-19-15, Improving Implementation of the Information Quality Act, April 2019. https://www.whitehouse.gov/wp-content/uploads/2019/04/M-19-15.pdf
[OMB M-19-23]	Office of Management and Budget Memorandum M-19-23, Phase 1 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Learning Agendas, Personnel, and Planning Guidance, July 2019. https://www.whitehouse.gov/wp-content/uploads/2019/07/M-19-23.pdf
[CNSSD 505]	Committee on National Security Systems Directive No. 505, Supply Chain Risk Management (SCRM), August 2017. https://www.cnss.gov/CNSS/issuances/Directives.cfm
[CNSNIST SP 22]	Committee on National Security Systems Policy No. 22, Cybersecurity Risk Management Policy, August 2016. https://www.cnss.gov/CNSS/issuances/Policies.cfm

[CNSSI 1253]	Committee on National Security Systems Instruction No. 1253, Security Categorization and Control Selection for National Security Systems, March 2014. https://www.cnss.gov/CNSS/issuances/Instructions.cfm
[CNSSI 4009]	Committee on National Security Systems Instruction No. 4009, Committee on National Security Systems (CNSS) Glossary, April 2015. https://www.cnss.gov/CNSS/issuances/Instructions.cfm
[DODI 8510.01]	Department of Defense Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), March 2014. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf?ver=2019-02-26-101520-300
[DHS NIPP]	Department of Homeland Security, National Infrastructure Protection Plan (NIPP), 2009. https://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf
STANDARDS, GUIDELINES, AND REPORTS	
[ISO 15026-1]	International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 15026-1:2019, *Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary*, March 2019. https://www.iso.org/standard/73567.html
[ISO 15408-1]	International Organization for Standardization/International Electrotechnical Commission 15408-1:2009, Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model, April 2017. https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf
[ISO 15408-2]	International Organization for Standardization/International Electrotechnical Commission 15408-2:2008, Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements, April 2017. https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf

[ISO 15408-3]	International Organization for Standardization/International Electrotechnical Commission 15408-3:2008, Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements, April 2017. https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf
[ISO 15288]	International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 15288:2015, Systems and software engineering — Systems life cycle processes, May 2015. https://www.iso.org/standard/63711.h1ml
[ISO 20243]	International Organization for Standardization/International Electrotechnical Commission 20243-1:2018, Information technology — Open Trusted Technology ProviderTM Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products — Part 1: Requirements and recommendations, February 2018. https://www.iso.org/standard/74399.html
[ISO 25237]	International Organization for Standardization/International Electrotechnical Commission 25237:2017, Health informatics — Pseudonymization, January 2017. https://www.iso.org/standard/63553.html
[ISO 27036]	International Organization for Standardization/International Electrotechnical Commission 27036-1:2014, Information technology — Security techniques — Information security for supplier relationships, Part 1: Overview and concepts, April 2014. https://www.iso.org/standard/59648.html
[ISO 29100]	International Organization for Standardization/International Electrotechnical Commission 29100:2011, Information technology — Security techniques — Privacy framework, December 2011. https://www.iso.org/standard/45123.html
[ISO 29147]	International Organization for Standardization/International Electrotechnical Commission 29147:2018, Information technology — Security techniques — Vulnerability disclosure, October 2018. https://www.iso.org/standard/72311.html

[ISO 29148]	International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 29148:2018, Systems and software engineering—Life cycle processes—Requirements engineering, November 2018. https://www.iso.org/standard/72089.html
[FIPS 140-3]	National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 140-3. https://doi.org/10.6028/NIST.FIPS.140-3
[FIPS 180-4]	National Institute of Standards and Technology (2015) Secure Hash Standard (SHS). (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 180-4. https://doi.org/10.6028/NIST.FIPS.180-4
[FIPS 186-4]	National Institute of Standards and Technology (2013) Digital Signature Standard (DSS). (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 186-4. https://doi.org/10.6028/NIST.FIPS.186-4
[FIPS 197]	National Institute of Standards and Technology (2001) Advanced Encryption Standard (AES). (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 197. https://doi.org/10.6028/NIST.FIPS.197
[FIPS 199]	National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199
[FIPS 200]	National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 200. https://doi.org/10.6028/NIST.FIPS.200

[FIPS 201-2]	National Institute of Standards and Technology (2013) Personal Identity Verification (PIV) of Federal Employees and Contractors. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 201-2. https://doi.org/10.6028/NIST.FIPS.201-2
[FIPS 202]	National Institute of Standards and Technology (2015) SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 202. https://doi.org/10.6028/NIST.FIPS.202
[NIST SP 800-12]	Nieles M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-12, Rev. 1. https://doi.org/10.6028/NIST.SP.800-12r1
[NIST SP 800-18]	Swanson MA, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-18, Rev. 1. https://doi.org/10.6028/NIST.SP.800-18r1
[NIST SP 800-28]	Jansen W, Winograd T, Scarfone KA (2008) Guidelines on Active Content and Mobile Code. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-28, Version 2. https://doi.org/10.6028/NIST.SP.800-28ver2
[NIST SP 800-30]	Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1
[NIST SP 800-32]	Kuhn R, Hu VC, Polk T, Chang S-J (2001) Introduction to Public Key Technology and the Federal PKI Infrastructure. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-32. https://doi.org/10.6028/NIST.SP.800-32

[NIST SP 800-34]	Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D (2010) Contingency Planning Guide for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-34, Rev. 1, Includes updates as of November 11, 2010. https://doi.org/10.6028/NIST.SP.800-34r1
[NIST SP 800-35]	Grance T, Hash J, Stevens M, O'Neal K, Bartol N (2003) Guide to Information Technology Security Services. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-35. https://doi.org/10.6028/NIST.SP.800-35
[NIST SP 800-37]	Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2
[NIST SP 800-39]	Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39
[NIST SP 800-40]	Souppaya MP, Scarfone KA (2013) Guide to Enterprise Patch Management Technologies. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-40, Rev. 3. https://doi.org/10.6028/NIST.SP.800-40r3
[NIST SP 800-41]	Scarfone KA, Hoffman P (2009) Guidelines on Firewalls and Firewall Policy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-41, Rev. 1. https://doi.org/10.6028/NIST.SP.800-41r1
[NIST SP 800-45]	Tracy MC, Jansen W, Scarfone KA, Butterfield J (2007) Guidelines on Electronic Mail Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-45, Version 2. https://doi.org/10.6028/NIST.SP.800-45ver2

[NIST SP 800-46]	Souppaya MP, Scarfone KA (2016) Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-46, Rev. 2. https://doi.org/10.6028/NIST.SP.800-46r2
[NIST SP 800-47]	Grance T, Hash J, Peck S, Smith J, Korow-Diks K (2002) Security Guide for Interconnecting Information Technology Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-47. https://doi.org/10.6028/NIST.SP.800-47
[NIST SP 800-50]	Wilson M, Hash J (2003) Building an Information Technology Security Awareness and Training Program. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-50. https://doi.org/10.6028/NIST.SP.800-50
[NIST SP 800-52]	McKay KA, Cooper DA (2019) Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-52, Rev. 2. https://doi.org/10.6028/NIST.SP.800-52r2
[NIST SP 800-53A]	Joint Task Force Transformation Initiative (2014) Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 4, Includes updates as of December 18, 2014. https://doi.org/10.6028/NIST.SP.800-53Ar4
[NIST SP 800-53B]	Joint Task Force (2020) Control Baselines and Tailoring Guidance for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53B. https://doi.org/10.6028/NIST.SP.800-53B
[NIST SP 800-55]	Chew E, Swanson MA, Stine KM, Bartol N, Brown A, Robinson W (2008) Performance Measurement Guide for Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-55, Rev. 1. https://doi.org/10.6028/NIST.SP.800-55r1

[NIST SP 800-56A]	Barker EB, Chen L, Roginsky A, Vassilev A, Davis R (2018) Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56A, Rev. 3. https://doi.org/10.6028/NIST.SP.800-56Ar3
[NIST SP 800-56B]	Barker EB, Chen L, Roginsky A, Vassilev A, Davis R, Simon S (2019) Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56B, Rev. 2. https://doi.org/10.6028/NIST.SP.800-56Br2
[NIST SP 800-56C]	Barker EB, Chen L, Davis R (2020) Recommendation for Key-Derivation Methods in Key-Establishment Schemes. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56C, Rev. 2. https://doi.org/10.6028/NIST.SP.800-56Cr2
[NIST SP 800-57-1]	Barker EB (2020) Recommendation for Key Management: Part 1 – General. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 1, Rev. 5. https://doi.org/10.6028/NIST.SP.800-57pt1r5
[NIST SP 800-57-2]	Barker EB, Barker WC (2019) Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-57pt2r1
[NIST SP 800-57-3]	Barker EB, Dang QH (2015) Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 3, Rev. 1. https://doi.org/10.6028/NIST.SP.800-57pt3r1

[NIST SP 800-60-1]	Stine KM, Kissel RL, Barker WC, Fahlsing J, Gulick J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 1, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v1r1
[NIST SP 800-60-2]	Stine KM, Kissel RL, Barker WC, Lee A, Fahlsing J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v2r1
[NIST SP 800-61]	Cichonski PR, Millar T, Grance T, Scarfone KA (2012) Computer Security Incident Handling Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-61, Rev. 2. https://doi.org/10.6028/NIST.SP.800-61r2
[NIST SP 800-63-3]	Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3, Includes updates as of March 2, 2020. https://doi.org/10.6028/NIST.SP.800-63-3
[NIST SP 800-63A]	Grassi PA, Fenton JL, Lefkovitz NB, Danker JM, Choong Y-Y, Greene KK, Theofanos MF (2017) Digital Identity Guidelines: Enrollment and Identity Proofing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63A, Includes updates as of March 2, 2020. https://doi.org/10.6028/NIST.SP.800-63a
[NIST SP 800-63B]	Grassi PA, Fenton JL, Newton EM, Perlner RA, Regenscheid AR, Burr WE, Richer, JP, Lefkovitz NB, Danker JM, Choong Y-Y, Greene KK, Theofanos MF (2017) Digital Identity Guidelines: Authentication and Lifecycle Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63B, Includes updates as of March 2, 2020. https://doi.org/10.6028/NIST.SP.800-63b

[NIST SP 800-70]	Quinn SD, Souppaya MP, Cook MR, Scarfone KA (2018) National Checklist Program for IT Products: Guidelines for Checklist Users and Developers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-70, Rev. 4. https://doi.org/10.6028/NIST.SP.800-70r4
[NIST SP 800-73-4]	Cooper DA, Ferraiolo H, Mehta KL, Francomacaro S, Chandramouli R, Mohler J (2015) Interfaces for Personal Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-73-4, Includes updates as of February 8, 2016. https://doi.org/10.6028/NIST.SP.800-73-4
[NIST SP 800-76-2]	Grother PJ, Salamon WJ, Chandramouli R (2013) Biometric Specifications for Personal Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-76-2. https://doi.org/10.6028/NIST.SP.800-76-2
[NIST SP 800-77]	Barker EB, Dang QH, Frankel SE, Scarfone KA, Wouters P (2020) Guide to IPsec VPNs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-77, Rev. 1. https://doi.org/10.6028/NIST.SP.800-77r1
[NIST SP 800-78-4]	Polk T, Dodson DF, Burr WE, Ferraiolo H, Cooper DA (2015) Cryptographic Algorithms and Key Sizes for Personal Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-78-4. https://doi.org/10.6028/NIST.SP.800-78-4
[NIST SP 800-79-2]	Ferraiolo H, Chandramouli R, Ghadiali N, Mohler J, Shorter S (2015) Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-79-2. https://doi.org/10.6028/NIST.SP.800-79-2
[NIST SP 800-81-2]	Chandramouli R, Rose SW (2013) Secure Domain Name System (DNS) Deployment Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-81-2. https://doi.org/10.6028/NIST.SP.800-81-2

[NIST SP 800-82]	Stouffer KA, Lightman S, Pillitteri VY, Abrams M, Hahn A (2015) Guide to Industrial Control Systems (ICS) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-82, Rev. 2. https://doi.org/10.6028/NIST.SP.800-82r2
[NIST SP 800-83]	Souppaya MP, Scarfone KA (2013) Guide to Malware Incident Prevention and Handling for Desktops and Laptops. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-83, Rev. 1. https://doi.org/10.6028/NIST.SP.800-83r1
[NIST SP 800-84]	Grance T, Nolan T, Burke K, Dudley R, White G, Good T (2006) Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-84. https://doi.org/10.6028/NIST.SP.800-84
[NIST SP 800-86]	Kent K, Chevalier S, Grance T, Dang H (2006) Guide to Integrating Forensic Techniques into Incident Response. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-86. https://doi.org/10.6028/NIST.SP.800-86
[NIST SP 800-88]	Kissel RL, Regenscheid AR, Scholl MA, Stine KM (2014) Guidelines for Media Sanitization. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-88, Rev. 1. https://doi.org/10.6028/NIST.SP.800-88r1
[NIST SP 800-92]	Kent K, Souppaya MP (2006) Guide to Computer Security Log Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-92. https://doi.org/10.6028/NIST.SP.800-92
[NIST SP 800-94]	Scarfone KA, Mell PM (2007) Guide to Intrusion Detection and Prevention Systems (IDPS). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-94. https://doi.org/10.6028/NIST.SP.800-94

[NIST SP 800-95]	Singhal A, Winograd T, Scarfone KA (2007) Guide to Secure Web Services. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-95. https://doi.org/10.6028/NIST.SP.800-95
[NIST SP 800-97]	Frankel SE, Eydt B, Owens L, Scarfone KA (2007) Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-97. https://doi.org/10.6028/NIST.SP.800-97
[NIST SP 800-100]	Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007. https://doi.org/10.6028/NIST.SP.800-100
[NIST SP 800-101]	Ayers RP, Brothers S, Jansen W (2014) Guidelines on Mobile Device Forensics. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-101, Rev. 1. https://doi.org/10.6028/NIST.SP.800-101r1
[NIST SP 800-111]	Scarfone KA, Souppaya MP, Sexton M (2007) Guide to Storage Encryption Technologies for End User Devices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-111. https://doi.org/10.6028/NIST.SP.800-111
[NIST SP 800-113]	Frankel SE, Hoffman P, Orebaugh AD, Park R (2008) Guide to SSL VPNs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-113. https://doi.org/10.6028/NIST.SP.800-113
[NIST SP 800-114]	Souppaya MP, Scarfone KA (2016) User's Guide to Telework and Bring Your Own Device (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-114, Rev. 1. https://doi.org/10.6028/NIST.SP.800-114r1

[NIST SP 800-115]	Scarfone KA, Souppaya MP, Cody A, Orebaugh AD (2008) Technical Guide to Information Security Testing and Assessment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-115. https://doi.org/10.6028/NIST.SP.800-115
[NIST SP 800-116]	Ferraiolo H, Mehta KL, Ghadiali N, Mohler J, Johnson V, Brady S (2018) A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-116, Rev. 1. https://doi.org/10.6028/NIST.SP.800-116r1
[NIST SP 800-121]	Padgette J, Bahr J, Holtmann M, Batra M, Chen L, Smithbey R, Scarfone KA (2017) Guide to Bluetooth Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-121, Rev. 2. https://doi.org/10.6028/NIST.SP.800-121r2
[NIST SP 800-124]	Souppaya MP, Scarfone KA (2013) Guidelines for Managing the Security of Mobile Devices in the Enterprise. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-124, Rev. 1. https://doi.org/10.6028/NIST.SP.800-124r1
[NIST SP 800-125B]	Chandramouli R (2016) Secure Virtual Network Configuration for Virtual Machine (VM) Protection. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-125B. https://doi.org/10.6028/NIST.SP.800-125B
[NIST SP 800-126]	Waltermire DA, Quinn SD, Booth H, III, Scarfone KA, Prisaca D (2018) The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-126, Rev. 3. https://doi.org/10.6028/NIST.SP.800-126r3

[NIST SP 800-128]	Johnson LA, Dempsey KL, Ross RS, Gupta S, Bailey D (2011) Guide for Security-Focused Configuration Management of Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-128, Includes updates as of October 10, 2019. https://doi.org/10.6028/NIST.SP.800-128
[NIST SP 800-130]	Barker EB, Smid ME, Branstad DK, Chokhani S (2013) A Framework for Designing Cryptographic Key Management Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-130. https://doi.org/10.6028/NIST.SP.800-130
[NIST SP 800-137]	Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh AD, Scholl MA, Stine KM (2011) Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-137. https://doi.org/10.6028/NIST.SP.800-137
[NIST SP 800-137A]	Dempsey KL, Pillitteri VY, Baer C, Niemeyer R, Rudman R, Urban S (2020) Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-137A. https://doi.org/10.6028/NIST.SP.800-137A
[NIST SP 800-147]	Cooper DA, Polk T, Regenscheid AR, Souppaya MP (2011) BIOS Protection Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-147. https://doi.org/10.6028/NIST.SP.800-147
[NIST SP 800-150]	Johnson CS, Waltermire DA, Badger ML, Skorupka C, Snyder J (2016) Guide to Cyber Threat Information Sharing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-150. https://doi.org/10.6028/NIST.SP.800-150

[NIST SP 800-152]	Barker EB, Branstad DK, Smid ME (2015) A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-152. https://doi.org/10.6028/NIST.SP.800-152
[NIST SP 800-154]	Souppaya MP, Scarfone KA (2016) Guide to Data-Centric System Threat Modeling. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Special Publication (SP) 800-154. https://csrc.nist.gov/publications/detail/sp/800-154/draft
[NIST SP 800-156]	Ferraiolo H, Chandramouli R, Mehta KL, Mohler J, Skordinski S, Brady S (2016) Representation of PIV Chain-of-Trust for Import and Export. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-156. https://doi.org/10.6028/NIST.SP.800-156
[NIST SP 800-160-1]	Ross RS, Oren JC, McEvilley M (2016) Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Includes updates as of March 21, 2018. https://doi.org/10.6028/NIST.SP.800-160v1
[NIST SP 800-160-2]	Ross RS, Pillitteri VY, Graubart R, Bodeau D, McQuaid R (2019) Developing Cyber Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 2. https://doi.org/10.6028/NIST.SP.800-160v2
[NIST SP 800-161]	Boyens JM, Paulsen C, Moorthy R, Bartol N (2015) Supply Chain Risk Management Practices for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161. https://doi.org/10.6028/NIST.SP.800-161

[NIST SP 800-162]	Hu VC, Ferraiolo DF, Kuhn R, Schnitzer A, Sandlin K, Miller R, Scarfone KA (2014) Guide to Attribute Based Access Control (ABAC) Definition and Considerations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-162, Includes updates as of August 2, 2019. https://doi.org/10.6028/NIST.SP.800-162
[NIST SP 800-166]	Cooper DA, Ferraiolo H, Chandramouli R, Ghadiali N, Mohler J, Brady S (2016) Derived PIV Application and Data Model Test Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-166. https://doi.org/10.6028/NIST.SP.800-166
[NIST SP 800-167]	Sedgewick A, Souppaya MP, Scarfone KA (2015) Guide to Application Whitelisting. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-167. https://doi.org/10.6028/NIST.SP.800-167
[NIST SP 800-171]	Ross RS, Pillitteri VY, Dempsey KL, Riddle M, Guissanie G (2020) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171, Rev. 2. https://doi.org/10.6028/NIST.SP.800-171r2
[NIST SP 800-172]	Ross RS, Pillitteri VY, Graubart RD, Guissanie G, Wagner R, Bodeau D (2020) Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171 (Final Public Draft). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-172. https://doi.org/10.6028/NIST.SP.800-172-draft
[NIST SP 800-177]	Rose SW, Nightingale S, Garfinkel SL, Chandramouli R (2019) Trustworthy Email. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-177, Rev. 1. https://doi.org/10.6028/NIST.SP.800-177r1

[NIST SP 800-178]	Ferraiolo DF, Hu VC, Kuhn R, Chandramouli R (2016) A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications: Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-178. https://doi.org/10.6028/NIST.SP.800-178
[NIST SP 800-181]	Petersen R, Santos D, Smith MC, Wetzel KA, Witte G (2020) Workforce Framework for Cybersecurity (NICE Framework). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181, Rev. 1. https://doi.org/10.6028/NIST.SP.800-181r1
[NIST SP 800-184]	Bartock M, Scarfone KA, Smith MC, Witte GA, Cichonski JA, Souppaya MP (2016) Guide for Cybersecurity Event Recovery. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-184. https://doi.org/10.6028/NIST.SP.800-184
[NIST SP 800-188]	Garfinkel S (2016) De-Identifying Government Datasets. (National Institute of Standards and Technology, Gaithersburg, MD), Second Draft NIST Special Publication (SP) 800-188. https://csrc.nist.gov/publications/detail/sp/800-188/draft
[NIST SP 800-189]	Sriram K, Montgomery D (2019) Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-189. https://doi.org/10.6028/NIST.SP.800-189
[NIST SP 800-192]	Yaga DJ, Kuhn R, Hu VC (2017) Verification and Test Methods for Access Control Policies/Models. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-192. https://doi.org/10.6028/NIST.SP.800-192
[IR 7539]	Cooper DA, MacGregor WI (2008) Symmetric Key Injection onto Smart Cards. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7539. https://doi.org/10.6028/NIST.IR.7539

[IR 7559]	Singhal A, Gunestas M, Wijesekera D (2010) Forensics Web Services (FWS). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7559. https://doi.org/10.6028/NIST.IR.7559
[IR 7622]	Boyens JM, Paulsen C, Bartol N, Shankles S, Moorthy R (2012) Notional Supply Chain Risk Management Practices for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7622. https://doi.org/10.6028/NIST.IR.7622
[IR 7676]	Cooper DA (2010) Maintaining and Using Key History on Personal Identity Verification (PIV) Cards. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7676. https://doi.org/10.6028/NIST.IR.7676
[IR 7788]	Singhal A, Ou X (2011) Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7788. https://doi.org/10.6028/NIST.IR.7788
[IR 7817]	Ferraiolo H (2012) A Credential Reliability and Revocation Model for Federated Identities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7817. https://doi.org/10.6028/NIST.IR.7817
[IR 7849]	Chandramouli R (2014) A Methodology for Developing Authentication Assurance Level Taxonomy for Smart Card-based Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7849. https://doi.org/10.6028/NIST.IR.7849
[IR 7870]	Cooper DA (2012) NIST Test Personal Identity Verification (PIV) Cards. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7870. https://doi.org/10.6028/NIST.IR.7870

[IR 7874]	Hu VC, Scarfone KA (2012) Guidelines for Access Control System Evaluation Metrics. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7874. https://doi.org/10.6028/NIST.IR.7874
[IR 7956]	Chandramouli R, Iorga M, Chokhani S (2013) Cryptographic Key Management Issues & Challenges in Cloud Services. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7956. https://doi.org/10.6028/NIST.IR.7956
[IR 7966]	Ylonen T, Turner P, Scarfone KA, Souppaya MP (2015) Security of Interactive and Automated Access Management Using Secure Shell (SSH). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7966. https://doi.org/10.6028/NIST.IR.7966
[IR 8011-1]	Dempsey KL, Eavy P, Moore G (2017) Automation Support for Security Control Assessments: Volume 1: Overview. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 1. https://doi.org/10.6028/NIST.IR.8011-1
[IR 8011-2]	Dempsey KL, Eavy P, Moore G (2017) Automation Support for Security Control Assessments: Volume 2: Hardware Asset Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 2. https://doi.org/10.6028/NIST.IR.8011-2
[IR 8011-3]	Dempsey KL, Eavy P, Goren N, Moore G (2018) Automation Support for Security Control Assessments: Volume 3: Software Asset Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 3. https://doi.org/10.6028/NIST.IR.8011-3
[IR 8011-4]	Dempsey KL, Takamura E, Eavy P, Moore G (2020) Automation Support for Security Control Assessments: Volume 4: Software Vulnerability Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 4. https://doi.org/10.6028/NIST.IR.8011-4

[IR 8023] Dempsey KL, Paulsen C (2015) Risk Management for Replication Devices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8023.

https://doi.org/10.6028/NIST.IR.8023

[IR 8040] Greene KK, Kelsey JM, Franklin JM (2016) Measuring the Usability and Security of Permuted Passwords on Mobile Platforms. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8040.

https://doi.org/10.6028/NIST.IR.8040

[IR 8062] Brooks S, Garcia M, Lefkovitz N, Lightman S, Nadeau E (2017) An Introduction to Privacy Engineering and Risk Management in Federal Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8062.

https://doi.org/10.6028/NIST.IR.8062

[IR 8112] Grassi P, Lefkovitz N, Nadeau E, Galluzzo R, Dinh, A (2018) Attribute Metadata: A Proposed Schema for Evaluating Federated Attributes. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8112.

https://doi.org/10.6028/NIST.IR.8112

[IR 8179] Paulsen C, Boyens JM, Bartol N, Winkler K (2018) Criticality Analysis Process Model: Prioritizing Systems and Components. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8179.

https://doi.org/10.6028/NIST.IR.8179

[IR 8272] Paulsen C, Winkler K, Boyens JM, Ng J, Gimbi J (2020) Impact Analysis Tool for Interdependent Cyber Supply Chain Risks. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8272.

https://doi.org/10.6028/NIST.IR.8272

MISCELLANEOUS PUBLICATIONS AND WEBSITES

[USCERT IR] Department of Homeland Security, *US-CERT Federal Incident Notification Guidelines*, April 2017.

https://us-cert.cisa.gov/incident-notification-guidelines

[DHS TIC]	Department of Homeland Security, *Trusted Internet Connections (TIC)*. https://www.dhs.gov/trusted-internet-connections
[DSB 2017]	Department of Defense, Defense Science Board, *Task Force on Cyber Deterrence*, February 2017. https://dsb.cto.mil/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf
[DOD STIG]	Defense Information Systems Agency, *Security Technical Implementation Guides (STIG)*. https://public.cyber.mil/stigs
[DODTERMS]	Department of Defense, *Dictionary of Military and Associated Terms*. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf
[FED PKI]	General Services Administration, *Federal Public Key Infrastructure*. https://www.idmanagement.gov/topics/fpki
[FISMA IMP]	Federal Information Security Modernization Act (FISMA) Implementation Project. https://nist.gov/RMF
[IETF 4949]	Internet Engineering Task Force (IETF), Request for Comments: 4949, *Internet Security Glossary, Version 2*, August 2007. https://tools.ietf.org/html/rfc4949
[IETF 5905]	Internet Engineering Task Force (IETF), Request for Comments: 5905, Network Time Protocol Version 4: Protocol and Algorithms Specification, June 2010. https://tools.ietf.org/pdf/rfc5905.pdf
[LAMPSON73]	B. W. Lampson, A Note on the Confinement Problem, Communications of the ACM 16, 10, pp. 613-615, October 1973.
[NARA CUI]	National Archives and Records Administration, Controlled Unclassified Information (CUI) Registry. https://www.archives.gov/cui
[NIAP CCEVS]	National Information Assurance Partnership, Common Criteria Evaluation and Validation Scheme. https://www.niap-ccevs.org

[NIST CAVP]	National Institute of Standards and Technology (2020) Cryptographic Algorithm Validation Program. Available at https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program
[NIST CMVP]	National Institute of Standards and Technology (2020) Cryptographic Module Validation Program. Available at https://csrc.nist.gov/projects/cryptographic-module-validation-program
[NIST CSF]	National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018
[NIST PF]	National Institute of Standards and Technology (2020) Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.01162020
[NCPR]	National Institute of Standards and Technology (2020) National Checklist Program Repository. Available at https://nvd.nist.gov/ncp/repository
[NVD 800-53]	National Institute of Standards and Technology (2020) National Vulnerability Database: NIST Special Publication 800-53 [database of controls]. Available at https://nvd.nist.gov/800-53
[NEUM04]	Principled Assuredly Trustworthy Composable Architectures, P. Neumann, CDRL A001 Final Report, SRI International, December 2004. http://www.csl.sri.com/users/neumann/chats4.pdf
[NSA CSFC]	National Security Agency, Commercial Solutions for Classified Program (CSfC). https://www.nsa.gov/resources/everyone/csfc
[NSA MEDIA]	National Security Agency, Media Destruction Guidance. https://www.nsa.gov/resources/everyone/media-destruction

[ODNI CTF]	Office of the Director of National Intelligence (ODNI) Cyber Threat Framework. https://www.dni.gov/index.php/cyber-threat-framework
[POPEK74]	G. Popek, The Principle of Kernel Design, in 1974 NCC, AFIPS Cong. Proc., Vol. 43, pp. 977-978.
[SALTZER75]	J. Saltzer and M. Schroeder, The Protection of Information in Computer Systems, in Proceedings of the IEEE 63(9), September 1975, pp. 1278-1308.
[SP 800-53 RES]	NIST Special Publication 800-53, Revision 5 Resource Center. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
[USGCB]	National Institute of Standards and Technology (2020) United States Government Configuration Baseline. Available at https://csrc.nist.gov/projects/united-states-government-configuration-baseline

ZAŁĄCZNIK A SŁOWNIK

PATRZ: NSC 7298, SŁOWNIK KLUCZOWYCH POJĘĆ Z ZAKRESU CYBERBEZPIECZEŃSTWA

ZAŁĄCZNIK B AKRONIMY

PATRZ: NSC 7298, SŁOWNIK KLUCZOWYCH POJĘĆ Z ZAKRESU CYBERBEZPIECZEŃSTWA

ZAŁĄCZNIK C ZESTAWIENIA ZABEZPIECZEŃ

WDRAŻANIE, WYCOFYWANIE I POŚWIADCZANIE WIARYGODNOŚCI

Tabele C-1 do C-20 zawierają podsumowanie zabezpieczeń podstawowych i ochrony prywatności oraz zabezpieczeń rozszerzonych przedstawionych w rozdziale trzecim. Każda z tabel dotyczy innej kategorii zabezpieczeń.

- Zabezpieczenie podstawowe lub zabezpieczenie rozszerzone, które zostało wycofane z katalogu zabezpieczeń lub przeniesione do innej kategorii zabezpieczeń, jest oznaczone symbolem "W", z objaśnieniem dokonanym czcionką kursywa w jasnoszarym kolorze.
- Zabezpieczenie podstawowe lub zabezpieczenie rozszerzone, które jest standardowo realizowane przez system informatyczny za pomocą środków technicznych, jest oznaczone literą "S" w kolumnie *Wdrożone przez.*
- Zabezpieczenie podstawowe lub zabezpieczenie rozszerzone, które jest zazwyczaj wdrażane przez organizację (tj. przez osobę w sposób nietechniczny), jest oznaczane literą "O" w kolumnie *Wdrożone przez*.[113]
- Zabezpieczenie podstawowe lub zabezpieczenie rozszerzone, które może być wdrożone przez organizację, system lub kombinację tych dwóch podmiotów, jest oznaczone symbolem "O/S" w kolumnie *Wdrożone przez*.
- Zabezpieczenie podstawowe lub zabezpieczenie rozszerzone oznaczone literą "V" w kolumnie *Wiarygodność* oznacza, że zabezpieczenie podstawowe lub

113 Wskazanie w tabelach C-1 do C-20, że dane zabezpieczenie podstawowe lub zabezpieczenie rozszerzone jest realizowane przez *system* lub *organizację*, jest hipotetyczne. Organizacje mają możliwość elastycznego wdrażania wybranych przez siebie zabezpieczeń podstawowych i zabezpieczeń rozszerzonych w sposób najbardziej efektywny kosztowo i skuteczny, przy jednoczesnym zachowaniu zgodności zgodności z założeniami zabezpieczenia podstawowego lub zabezpieczenia rozszerzonego. W zależności od sytuacji, zabezpieczenie podstawowe lub zabezpieczenie rozszerzone może być wdrożone przez system, organizację lub kombinację tych dwóch podmiotów.

zabezpieczenie rozszerzone przyczynia się do powstania podstaw zaufania, że założenie dotyczące bezpieczeństwa lub ochrony prywatności zostało lub zostanie osiągnięte.[114]

Zabezpieczenia podstawowe lub zabezpieczenia rozszerzone przedstawione w tabelach C-1 do C-20 są połączone hiperłączem z tekstem opisującym dane zabezpieczenie w rozdziale trzecim.

Kategorie zabezpieczeń zawierają zabezpieczenia podstawowe i zabezpieczenia rozszerzone. Zabezpieczenia rozszerzone są bezpośrednio związane z zabezpieczeniem podstawowym. Zabezpieczenia rozszerzone albo dodają funkcjonalność lub specyficzność do zabezpieczenia podstawowego, albo zwiększają siłę zabezpieczenia podstawowego. W obu przypadkach, zabezpieczenia rozszerzone są stosowane w systemach i środowiskach działania, które wymagają większej ochrony niż ta zapewniona przez zabezpieczenie podstawowe. Ta zwiększona ochrona jest wymagana ze względu na potencjalne niekorzystne wpływy organizacyjne / indywidualne, lub gdy organizacje wymagają uzupełnienia funkcji zabezpieczenia podstawowego lub wiarygodności w oparciu o organizacyjną ocenę ryzyka. Wykorzystanie zabezpieczeń rozszerzonych **zawsze** wymaga zastosowania zabezpieczenia podstawowego.

Kategorie są ułożone w porządku alfabetycznym, podczas gdy zabezpieczenia podstawowe i zabezpieczenia rozszerzone w każdej kategorii są ułożone w porządku numerycznym. Kolejność alfabetyczna lub numeryczna kategorii, zabezpieczeń podstawowych lub zabezpieczeń rozszerzonych **nie oznacza** żadnego rodzaju priorytetyzacji, poziomu ważności ani kolejności, w jakiej zabezpieczenia podstawowe lub zabezpieczenia rozszerzone mają być wdrażane.

114 Wiarygodność jest krytycznym aspektem w określaniu zaufania systemów. Wiarygodność jest miarą zaufania, że funkcje bezpieczeństwa i ochrony prywatności, cechy, praktyki, polityki, procedury, mechanizmy i architektura systemów organizacyjnych właściwie odzwierciedlają i egzekwują ustalone polityki w zakresie bezpieczeństwa i ochrony prywatności.

TABELA C-1 KATEGORIA AC - KONTROLA DOSTĘPU

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
AC-1	**POLITYKA I PROCEDURY**	O	V
AC-2	**ZARZĄDZANIE KONTAMI**	O	
AC-2(1)	AUTOMATYCZNE ZARZĄDZANIE KONTEM SYSTEMU	O	
AC-2(2)	AUTOMATYCZNE ZARZĄDZANIE KONTEM CZASOWYM | AWARYJNYM	S	
AC-2(3)	WYŁĄCZANIE KONT	S	
AC-2(4)	AUTOMATYCZNE DZIAŁANIA AUDYTOWE	S	
AC-2(5)	WYLOGOWANIE PRZEZ UŻYTKOWNIKA PO OKREŚLONYM OKRESIE NIEAKTYWNOŚCI	O/S	
AC-2(6)	DYNAMICZNE ZARZĄDZANIE UPRAWNIENIAMI	S	
AC-2(7)	UPRZYWILEJOWANE KONTA UŻYTKOWNIKÓW	O	
AC-2(8)	DYNAMICZNE ZARZĄDZANIE KONTEM	S	
AC-2(9)	OGRANICZENIA W KORZYSTANIU Z KONT WSPÓLNYCH I GRUPOWYCH	O	
AC-2(10)	*ZMIANA POŚWIADCZANIA UPRAWNIEŃ KONTA WSPÓLNEGO I GRUPOWEGO*	*W: włączone do AC-2k.*	
AC-2(11)	WARUNKI UŻYTKOWANIA	S	
AC-2(12)	MONITOROWANIE KONTA POD WZGLĘDEM NIETYPOWYCH ZASTOSOWAŃ	O/S	
AC-2(13)	WYŁĄCZANIE KONT DOSTĘPOWYCH UŻYTKOWNIKOM WYSOKIEGO RYZYKA	O	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
AC-3	**EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU**	S	
AC-3(1)	*OGRANICZONY DOSTĘP DO FUNKCJI UPRZYWILEJOWANYCH*	*W: włączone do AC-6.*	
AC-3(2)	PODWÓJNA AUTORYZACJA	S	
AC-3(3)	OBOWIĄZKOWA KONTROLA DOSTĘPU	S	
AC-3(4)	UZNANIOWA KONTROLA DOSTĘPU	S	
AC-3(5)	INFORMACJE DOTYCZĄCE BEZPIECZEŃSTWA	S	
AC-3(6)	*OCHRONA INFORMACJI UŻYTKOWNIKA I SYSTEMU*	*W: włączone do MP-4 i SC-28.*	
AC-3(7)	KONTROLA DOSTĘPU OPARTA NA ROLI	O/S	
AC-3(8)	COFNIĘCIE ZEZWOLEŃ NA DOSTĘP	O/S	
AC-3(9)	KONTROLOWANE UDOSTĘPNIENIE INFORMACJI	O/S	
AC-3(10)	NADZOROWANE OBEJŚCIE MECHANIZMÓW KONTROLI DOSTĘPU	O	
AC-3(11)	OGRANICZENIE DOSTĘPU DO OKREŚLONYCH RODZAJÓW INFORMACJI	S	
AC-3(12)	ZAPEWNIENIE I EGZEKWOWANIE DOSTĘPU DO APLIKACJI	S	
AC-3(13)	KONTROLA DOSTĘPU NA PODSTAWIE ATRYBUTÓW	S	
AC-3(14)	DOSTĘP INDYWIDUALNY	S	
AC-3(15)	UZNANIOWA I OBOWIĄZKOWA KONTROLA DOSTĘPU	S	
AC-4	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI**	S	
AC-4(1)	BEZPIECZEŃSTWO OBIEKTÓW I ATRYBUTY PRYWATNOŚCI	S	

NUMER ZABEZPIECZENIA	**NAZWA ZABEZPIECZENIA PODSTAWOWEGO** NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
AC-4(2)	PRZETWARZANIE DOMEN	S	
AC-4(3)	DYNAMICZNA KONTROLA PRZEPŁYWU INFORMACJI	S	
AC-4(4)	KONTROLA PRZEPŁYWU ZASZYFROWANYCH INFORMACJI	S	
AC-4(5)	WBUDOWANE RODZAJE DANYCH	S	
AC-4(6)	METADANE	S	
AC-4(7)	MECHANIZMY PRZEPŁYWU JEDNOKIERUNKOWEGO	S	
AC-4(8)	FILTRY POLITYKI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI	S	
AC-4(9)	OCENA PRZEZ UPRAWNIONĄ OSOBĘ	O/S	
AC-4(10)	WŁĄCZANIE I WYŁĄCZANIE FILTRÓW BEZPIECZEŃSTWA LUB POLITYKI PRYWATNOŚCI	S	
AC-4(11)	KONFIGURACJA FILTRÓW BEZPIECZEŃSTWA LUB POLITYKI PRYWATNOŚCI	S	
AC-4(12)	IDENTYFIKATORY TYPÓW DANYCH	S	
AC-4(13)	DEKOMPOZYCJA INFORMACJI NA ODPOWIEDNIE PODSKŁADNIKI	S	
AC-4(14)	POLITYKA STOSOWANIA FILTRÓW BEZPIECZEŃSTWA LUB OCHRONY PRYWATNOŚCI	S	
AC-4(15)	WYKRYWANIE INFORMACJI NIEAKCEPTOWANYCH	S	
AC-4(16)	*PRZEKAZYWANIE INFORMACJI POMIĘDZY SYSTEMAMI*	*W: włączone do AC-4.*	
AC-4(17)	UWIERZYTELNIANIE DOMEN	S	
AC-4(18)	*POWIĄZANIE ATRYBUTÓW BEZPIECZEŃSTWA*	*W: włączone do AC-16.*	
AC-4(19)	UWIERZYTELNIANIE METADANYCH	S	

NUMER ZABEZPIECZENIA	**NAZWA ZABEZPIECZENIA PODSTAWOWEGO** NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
AC-4(20)	ZATWIERDZONE ROZWIĄZANIA BEZPIECZEŃSTWA	O	
AC-4(21)	FIZYCZNA LUB LOGICZNA SEPARACJA PRZEPŁYWÓW INFORMACJI	O/S	
AC-4(22)	TYLKO DOSTĘP	S	
AC-4(23)	MODYFIKACJA INFORMACJI, KTÓRYCH NIE MOŻNA UDOSTĘPNIAĆ	O/S	
AC-4(24)	WEWNĘTRZNY ZNORMALIZOWANY FORMAT	S	
AC-4(25)	SANITYZACJA DANYCH	S	
AC-4(26)	AUDYT DZIAŁAŃ FILTRUJĄCYCH	O/S	
AC-4(27)	REDUNDANTNE / NIEZALEŻNE MECHANIZMY FILTRACJI	S	
AC-4(28)	KASKADOWY FILTR TREŚCI	S	
AC-4(29)	SILNIKI ARANŻACJI FILTROWANIA	O/S	
AC-4(30)	MECHANIZMY FILTRUJĄCE WYKORZYSTUJĄCE PROCESY WIELOKROTNE	S	
AC-4(31)	ZAPOBIEGANIE PRZENOSZENIU NIEWŁAŚCIWYCH TREŚCI	S	
AC-4(32)	WYMAGANIA DOTYCZĄCE PROCESU PRZEKAZYWANIA INFORMACJI	S	
AC-5	**ROZDZIAŁ OBOWIĄZKÓW**	O	
AC-6	**ZASADA WIEDZY KONIECZNEJ**	O	
AC-6(1)	UPOWAŻNIONY DOSTĘPU DO FUNKCJI BEZPIECZEŃSTWA	O	
AC-6(2)	NIEUPRZYWILEJOWANY DOSTĘP DLA FUNKCJI NIEZWIĄZANYCH Z BEZPIECZEŃSTWEM	O	
AC-6(3)	DOSTĘP SIECIOWY DO UPRZYWILEJOWANYCH POLECEŃ	O	

NUMER ZABEZPIECZENIA	**NAZWA ZABEZPIECZENIA PODSTAWOWEGO** NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
AC-6(4)	ODDZIELNE DOMENY PRZETWARZANIA	O/S	
AC-6(5)	UPRZYWILEJOWANE KONTA	O	
AC-6(6)	UPRZYWILEJOWANY DOSTĘP PRZEZ UŻYTKOWNIKÓW NIEORGANIZACYJNYCH	O	
AC-6(7)	PRZEGLĄD UPRAWNIEŃ UŻYTKOWNIKA	O	
AC-6(8)	POZIOMY UPRAWNIEŃ DO WYKONYWANIA KODU	S	
AC-6(9)	KONTROLA WYKORZYSTANIA UPRZYWILEJOWANYCH FUNKCJI	S	
AC-6(10)	ODMOWA WYKONYWANIA PRZEZ NIEUPRZYWILEJOWANYCH UŻYTKOWNIKÓW UPRZYWILEJOWANYCH FUNKCJI	S	
AC-7	**NIEUDANE PRÓBY LOGOWANIA**	S	
AC-7(1)	*AUTOMATYCZNE ZAMKNIĘCIE KONTA*	*W: włączone do AC-7.*	
AC-7(2)	USUWANIE INFORMACJI Z URZĄDZEŃ PRZENOŚNYCH	S	
AC-7(3)	OGRANICZENIE PRÓB LOGOWANIA BIOMETRYCZNEGO	O	
AC-7(4)	UŻYCIE ALTERNATYWNEGO CZYNNIKA UWIERZYTELNIANIA	O/S	
AC-8	**POWIADOMIENIE O ZASADACH UŻYCIA SYSTEMU**	O/S	
AC-9	**POWIADOMIENIE O POPRZEDNIM ZALOGOWANIU**	S	
AC-9(1)	NIEUDANE LOGOWANIE	S	
AC-9(2)	UDANE I NIEUDANE LOGOWANIE	S	
AC-9(3)	POWIADAMIANIE O ZMIANACH W KONCIE	S	
AC-9(4)	DODATKOWE INFORMACJE DOTYCZĄCE LOGOWANIA	S	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
AC-10	**KONTROLA ILOŚCI RÓWNOCZESNYCH SESJI**	S	
AC-11	**BLOKADA URZĄDZENIA**	S	
AC-11(1)	WYGASZACZ EKRANU	S	
AC-12	**ZAKOŃCZENIE SESJI**	S	
AC-12(1)	WYLOGOWANIE INICJOWANE PRZEZ UŻYTKOWNIKA	O/S	
AC-12(2)	KOMUNIKAT O ZAKOŃCZENIU SESJI (WYLOGOWANIU)	S	
AC-12(3)	KOMUNIKAT OSTRZEGAWCZY O PRZEKROCZENIU LIMITU CZASU	S	
AC-13	*NADZÓR I PRZEGLĄD KONTROLI DOSTĘPU*	*W: włączone do AC-2 i AU-6.*	
AC-14	**DZIAŁANIA DOZWOLONE BEZ IDENTYFIKACJI LUB UWIERZYTELNIENIA**	O	
AC-14(1)	*NIEZBĘDNE ZASTOSOWANIA*	*W: włączone do AC-14.*	
AC-15	*ZNAKOWANIE AUTOMATYCZNE*	*W: włączone do MP-3.*	
AC-16	**ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI**	O	
AC-16(1)	DYNAMICZNE KOJARZENIE ATRYBUTÓW	S	
AC-16(2)	ZMIANY WARTOŚCI ATRYBUTÓW PRZEZ UPOWAŻNIONE OSOBY	S	
AC-16(3)	UTRZYMANIE KOJARZENIA ATRYBUTÓW PRZEZ SYSTEM INFORMATYCZNY	S	
AC-16(4)	KOJARZENIE ATRYBUTÓW PRZEZ AUTORYZOWANY PERSONEL	S	
AC-16(5)	ATRYBUTY BEZPIECZEŃSTWA PREZENTOWANE NA WYŚWIETLACZACH URZĄDZEŃ WYJŚCIOWYCH	S	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
AC-16(6)	ZARZĄDZANIE POWIĄZANYMI ATRYBUTAMI	O	
AC-16(7)	INTERPRETACJA WSPÓLNYCH ATRYBUTÓW	O	
AC-16(8)	TECHNIKI I TECHNOLOGIE WIĄZANIA	S	
AC-16(9)	PONOWNY PRZYDZIAŁ ATRYBUTÓW - MECHANIZMY ZMIANY KLASYFIKACJI	O	
AC-16(10)	KONFIGURACJA ATRYBUTÓW PRZEZ UPOWAŻNIONE OSOBY	O	
AC-17	**DOSTĘP ZDALNY**	O	
AC-17(1)	AUTOMATYCZNE MONITOROWANIE I KONTROLA	O/S	
AC-17(2)	OCHRONA POUFNOŚCI I INTEGRALNOŚCI Z WYKORZYSTANIEM SZYFROWANIA	S	
AC-17(3)	ZARZĄDZANE PUNKTY KONTROLI DOSTĘPU	S	
AC-17(4)	POLECENIA UPRZYWILEJOWANE I DOSTĘP	O	
AC-17(5)	*MONITOROWANIE NIEAUTORYZOWANYCH POŁĄCZEŃ*	*W: włączone do SI-4.*	
AC-17(6)	OCHRONA MECHANIZMÓW DOSTĘPU ZDALNEGO	O	
AC-17(7)	*DODATKOWA OCHRONA DOSTĘPU DO FUNKCJI BEZPIECZEŃSTWA*	*W: włączone do AC-3(10).*	
AC-17(8)	*WYŁĄCZANIE NIEZABEZPIECZONYCH PROTOKOŁÓW SIECIOWYCH*	*W: włączone do CM-7.*	
AC-17(9)	ODŁĄCZENIE LUB WYŁĄCZENIE DOSTĘP	O	
AC-17(10)	UWIERZYTELNIANIE ZDALNYCH POLECEŃ	S	
AC-18	**DOSTĘP BEZPRZEWODOWY**	O	
AC-18(1)	UWIERZYTELNIANIE ORAZ SZYFROWANIE	S	

NUMER ZABEZPIECZENIA	**NAZWA ZABEZPIECZENIA PODSTAWOWEGO** NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
AC-18(2)	*MONITOROWANIE POŁĄCZEŃ NIEAUTORYZOWANYCH*	*W: włączone do SI-4.*	
AC-18(3)	DEZAKTYWACJA SIECI BEZPRZEWODOWEJ	O/S	
AC-18(4)	OGRANICZENIE DOKONYWANIE KONFIGURACJI PRZEZ UŻYTKOWNIKÓW	O	
AC-18(5)	POZIOMY MOCY ANTEN / TRANSMISJI	O	
AC-19	**KONTROLA DOSTĘPU DO URZĄDZEŃ PRZENOŚNYCH**	0	
AC-19(1)	*KORZYSTANIE Z ZAPISYWALNYCH I PRZENOŚNYCH URZĄDZEŃ MAGAZYNUJĄCYCH*	*W: włączone do MP-7.*	
AC-19(2)	*KORZYSTANIE Z OSOBISTYCH PRZENOŚNYCH URZĄDZEŃ MAGAZYNUJĄCYCH*	*W: włączone do MP-7.*	
AC-19(3)	*KORZYSTANIE Z OGÓLNODOSTĘPNYCH PRZENOŚNYCH URZĄDZEŃ MAGAZYNUJĄCYCH*	*W: włączone do MP-7.*	
AC-19(4)	OGRANICZENIA DOTYCZĄCE INFORMACJI NIEJAWNYCH	O	
AC-19(5)	SZYFROWANIE ZAWARTOŚCI CAŁEGO URZĄDZENIA / WYBRANYCH ZASOBÓW URZĄDZENIA	O	
AC-20	**WYKORZYSTANIE SYSTEMÓW ZEWNĘTRZNYCH**	O	
AC-20(1)	OGRANICZENIA AUTORYZOWANEGO DOSTĘPU	O	
AC-20(2)	PRZENOŚNE URZĄDZENIA MAGAZYNUJĄCE - OGRANICZONE ZASTOSOWANIE	O	
AC-20(3)	SYSTEMY NIE NALEŻĄCE ORGANIZACJI - OGRANICZONE ZASTOSOWANIE	O	
AC-20(4)	SIECIOWE URZĄDZENIA MAGAZYNUJĄCE - ZAKAZ UŻYWANIA	O	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
AC-20(5)	PRZENOŚNE URZĄDZENIA MAGAZYNUJĄCE - ZAKAZ UŻYWANIA	O	
AC-21	**UDOSTĘPNIANIE INFORMACJI**	O	
AC-21(1)	AUTOMATYCZNE WSPARCIE DECYZJI	S	
AC-21(2)	WYSZUKIWANIE I ODZYSKIWANIE INFORMACJI	S	
AC-22	**TREŚCI PUBLICZNIE DOSTĘPNE**	O	
AC-23	**OCHRONA PRZED PRZESZUKIWANIEM DANYCH**	O	
AC-24	**PRZYZNAWANIE PRAW DOSTĘPU**	O	
AC-24(1)	PRZESYŁANIE INFORMACJI O AUTORYZACJI DOSTĘPU	S	
AC-24(2)	BRAK TOŻSAMOŚCI UŻYTKOWNIKA LUB PROCESU	S	
AC-25	**MONITOR REFERENCYJNY**	S	V

TABELA C-2 KATEGORIA AT - UŚWIADAMIANIE I SZKOLENIA

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
AT-1	**POLITYKA I PROCEDURY**	O	V
AT-2	**SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA**	O	V
AT-2(1)	ĆWICZENIA PRAKTYCZNE	O	V
AT-2(2)	ZAGROŻENIE WEWNĘTRZNE	O	V
AT-2(3)	INŻYNIERIA SPOŁECZNA I POZYSKIWANIE DANYCH	O	V
AT-2(4)	PODEJRZANA TRANSMISJA I ANOMALIE ZACHOWANIA SYSTEMU	O	V
AT-2(5)	ZAAWANSOWANE TRWAŁE ZAGROŻENIA (TYPU APT)	O	V
AT-2(6)	ŚRODOWISKA CYBERZAGROŻEŃ	O	V
AT-3	**SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH**	O	V
AT-3(1)	ZABEZPIECZENIA ŚRODOWISKOWE	O	V
AT-3(2)	ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO	O	V
AT-3(3)	ĆWICZENIA PRAKTYCZNE	O	V
AT-3(4)	*PODEJRZANE TRANSMISJE I ANOMALIE ZACHOWANIA SYSTEMU*	*W: włączone do AT-2(4).*	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
AT-3(5)	PRZETWARZANIE DANYCH OSOBOWYCH	O	V
AT-4	**DOKUMENTACJA SZKOLENIOWA**	O	V
AT-5	*UTRZYMYWANIE KONTAKTÓW Z ZESPOŁAMI I STOWARZYSZENIAMI SPECJALIZUJĄCYMI SIĘ W CYBERBEZPIECZEŃSTWIE*	*W: włączone do PM-15.*	
AT-6	**INFORMACJE ZWROTNE O SZKOLENIACH**		

TABELA C-3 KATEGORIA AU - AUDYT I ROZLICZALNOŚĆ

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
AU-1	**POLITYKA I PROCEDURY**	O	V
AU-2	**AUDYT ZDARZEŃ**	O	
AU-2(1)	*KOMPILACJA ZAPISÓW AUDYTU Z WIELU ŹRÓDEŁ*	*W: włączone do AU-12.*	
AU-2(2)	*WYBÓR ZDARZEŃ AUDYTOWYCH WEDŁUG KOMPONENTÓW*	*W: włączone do AU-12.*	
AU-2(3)	*OPINIE I AKTUALIZACJE*	*W: włączone do AU-2.*	
AU-2(4)	*UPRZYWILEJOWANE FUNKCJE*	*W: włączone do AC-6(9).*	
AU-3	**ZAWARTOŚĆ REJESTRÓW AUDYTU**	S	
AU-3(1)	DODATKOWE INFORMACJE KONTROLNE	S	
AU-3(2)	CENTRALNE ZARZĄDZANIE TREŚCIĄ PLANOWANEGO REJESTRU AUDYTU	W: włączone do PL-9.	
AU-3(3)	OGRANICZENIE INFORMACJI UMOŻLIWIAJĄCYCH IDENTYFIKACJĘ OSÓB	O	
AU-4	**POJEMNOŚĆ PAMIĘCI ZAPISÓW AUDYTU**	O/S	
AU-4(1)	TRANSFER REKORDÓW DO ALTERNATYWNYCH URZĄDZEŃ MAGAZYNUJĄCYCH	O/S	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
AU-5	**REAKCJA NA BŁĘDY PROCESÓW AUDYTU**	S	
AU-5(1)	OSTRZEŻENIA DOTYCZĄCE LIMITU PAMIĘCI PRZECHOWYWANIA REKORDÓW AUDYTU	S	
AU-5(2)	ALERTY CZASU RZECZYWISTEGO	S	
AU-5(3)	KONFIGUROWALNE PROGI NATĘŻENIA RUCHU	S	
AU-5(4)	WYŁĄCZENIE W PRZYPADKU AWARII	S	
AU-5(5)	ZDOLNOŚĆ ALTERNATYWNEGO PROWADZENIA REJESTRU AUDYTÓW	O	
AU-6	**PRZEGLĄD ZAPISÓW AUDYTU, ANALIZA I RAPORTOWANIE**	O	V
AU-6(1)	ZAUTOMATYZOWANA INTEGRACJA PROCESÓW	O	V
AU-6(2)	*AUTOMATYCZNE ALARMY BEZPIECZEŃSTWA*	*W: włączone do SI-4.*	
AU-6(3)	KORELACJA ZBIORÓW AUDYTU	O	V
AU-6(4)	CENTRALNE PRZEGLĄDANIE I ANALIZY	S	V
AU-6(5)	ZINTEGROWANA ANALIZA ZAPISÓW Z AUDYTU	O	V
AU-6(6)	KORELACJA AUDYTU Z MONITOROWANIEM FIZYCZNYM	O	V

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
AU-6(7)	DOPUSZCZALNE DZIAŁANIA	O	V
AU-6(8)	PEŁNA ANALIZA TEKSTU UPRZYWILEJOWANYCH POLECEŃ	O	V
AU-6(9)	KORELACJA Z INFORMACJAMI UZYSKANYMI ZE ŹRÓDEŁ NIETECHNICZNYCH	O	V
AU-6(10)	*KORYGOWANIE POZIOMU AUDYTU*	*W: włączone do AU-6.*	
AU-7	**REDUKCJA TREŚCI ZAPISÓW Z AUDYTU I GENEROWANIE RAPORTÓW**	S	V
AU-7(1)	AUTOMATYZACJA PROCESU	S	V
AU-7(2)	*AUTOMATYCZNE SORTOWANIE I WYSZUKIWANIE*	*W: włączone do AU-7(1).*	
AU-8	**ZNACZNIKI CZASU**	S	
AU-8(1)	*SYNCHRONIZACJA Z AUTORYZOWANYM ŹRÓDŁEM CZASU ODNIESIENIA*	*W: włączone do SC-45(1).*	
AU-8(2)	*WTÓRNE ŹRÓDŁO CZASU ODNIESIENIA*	*W: włączone do SC-45(2).*	
AU-9	**OCHRONA INFORMACJI AUDYTOWYCH**	S	
AU-9(1)	NOŚNIKI JEDNOKROTNEGO ZAPISU	S	
AU-9(2)	BACKUP AUDYTU W ODSEPAROWANYM FIZYCZNIE SYSTEMIE / KOMPONENCIE	S	

NUMER ZABEZPIECZENIA	**NAZWA ZABEZPIECZENIA PODSTAWOWEGO** NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
AU-9(3)	OCHRONA KRYPTOGRAFICZNA	S	
AU-9(4)	DOSTĘP DO PODZBIORU UPRZYWILEJOWANYCH UŻYTKOWNIKÓW	O	
AU-9(5)	PODWÓJNA AUTORYZACJA	O/S	
AU-9(6)	DOSTĘP TYLKO DO ODCZYTU	O/S	
AU-9(7)	PRZECHOWYWANIE INFORMACJI NA KOMPONENTACH Z RÓŻNYMI SYSTEMAMI OPERACYJNYMI	O	
AU-10	**NIEZAPRZECZALNOŚĆ**	S	V
AU-10(1)	POŁĄCZENIE TOŻSAMOŚCI	S	V
AU-10(2)	POWIĄZANIE INFORMACJI Z TOŻSAMOŚCIĄ TWÓRCY	S	V
AU-10(3)	ŁAŃCUCH NADZORU	O/S	V
AU-10(4)	POTWIERDZANIE TOŻSAMOŚCI PRZEGLĄDAJĄCEGO INFORMACJE	S	V
AU-10(5)	*PODPISY CYFROWE*	*W: włączone do SI-7.*	
AU-11	**RETENCJA ZAPISÓW AUDYTU**	O	
AU-11(1)	DŁUGOTERMINOWA ZDOLNOŚĆ DO ODZYSKU	O	V
AU-12	**TWORZENIE ZAPISÓW AUDYTU**	S	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
AU-12(1)	*OGÓLNOSYSTEMOWE / SKORELOWANE W CZASIE* ŚCIEŻKI AUDYTU	S	
AU-12(2)	UJEDNOLICONE FORMATY	S	
AU-12(3)	ZMIANY DOKONYWANE PRZEZ UPRAWNIONE OSOBY	S	
AU-12(4)	AUDYT PARAMETRÓW ZAPYTAŃ O DANE OSOBOWE	S	
AU-13	**MONITOROWANIE UJAWNIANIA INFORMACJI**	O	V
AU-13(1)	WYKORZYSTANIE ZAUTOMATYZOWANYCH NARZĘDZI	O/S	V
AU-13(2)	PRZEGLĄD MONITOROWANYCH STRON	O	V
AU-13(3)	NIEAUTORYZOWANE POWIELANIE INFORMACJI	O/S	V
AU-14	**AUDYT SESJI**	S	V
AU-14(1)	URUCHAMIANIE SYSTEMU	S	V
AU-14(2)	PRZECHWYTY / NAGRYWANIE I ZAWARTOŚĆ DZIENNIKÓW LOGOWANIA	*W: włączone do AU-14.*	
AU-14(3)	ZDALNE WYŚWIETLANIE I ODSŁUCHIWANIE	S	V
AU-15	*ZDOLNOŚĆ DO ALTERNATYWNEGO AUDYTU*	*W: włączone do AU-5(5).*	
AU-16	**AUDYT MIĘDZYORGANIZACYJNY**	O	

NUMER ZABEZPIECZENIA	**NAZWA ZABEZPIECZENIA PODSTAWOWEGO** NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
AU-16(1)	OCHRONA TOŻSAMOŚCI	O	
AU-16(2)	UDOSTĘPNIANIE INFORMACJI AUDYTOWYCH	O	
AU-16(3)	ODDZIELANIE DANYCH OSOBOWYCH	O	

TABELA C-4 KATEGORIA CA - OCENA, AUTORYZACJA I MONITOROWANIE

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
CA-1	**POLITYKA I PROCEDURY**	O	V
CA-2	**OCENA ZABEZPIECZEŃ**	O	V
CA-2(1)	NIEZALEŻNI AUDYTORZY	O	V
CA-2(2)	OCENY SPECJALISTYCZNE	O	V
CA-2(3)	KORZYSTANIE Z WYNIKÓW UZYSKANYCH OD ORGANIZACJI ZEWNĘTRZNYCH	O	V
CA-3	**WYMIANA INFORMACJI**	O	V
CA-3(1)	*POŁĄCZENIA JAWNYCH BEZPIECZNYCH SYSTEMÓW KRAJOWYCH*	*W: włączone do SC-7(25).*	
CA-3(2)	*POŁĄCZENIA NIEJAWNYCH SYSTEMÓW KRAJOWYCH*	*W: włączone do SC-7(26).*	
CA-3(3)	*POŁĄCZENIA JAWNYCH BEZPIECZNYCH SYSTEMÓW TRANSGRANICZNYCH*	*W: włączone do SC-7(27).*	
CA-3(4)	*POŁĄCZENIA Z SIECIAMI PUBLICZNYMI*	*W: włączone do SC-7(28).*	
CA-3(5)	*OGRANICZENIA DOTYCZĄCE POŁĄCZEŃ SYSTEMÓW ZEWNĘTRZNYCH*	*W: włączone do SC-7(5).*	
CA-3(6)	AUTORYZACJA PRZESYŁU	O/S	V

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
CA-3(7)	POBIERANIE INFORMACJI	O/S	V
CA-4	*CERTYFIKACJA BEZPIECZEŃSTWA*	*W: włączone do CA-2.*	
CA-5	**PLAN I ETAPY DZIAŁANIA**	O	V
CA-5(1)	AUTOMATYZACJA WSPIERAJĄCA AKTUALNOŚĆ / SZCZEGÓŁOWOŚĆ PLANÓW	O	V
CA-6	**AUTORYZACJA**	O	V
CA-6(1)	AUTORYZACJA WSPÓLNA - WEWNĄTRZORGANIZACYJNA	O	V
CA-6(2)	AUTORYZACJA WSPÓLNA - MIĘDZYORGANIZACYJNA	O	V
CA-7	**CIĄGŁE MONITOROWANIE**	O	V
CA-7(1)	NIEZALEŻNA OCENA	O	V
CA-7(2)	*RODZAJE OCEN*	*W: włączone do CA-2.*	
CA-7(3)	ANALIZY TRENDÓW	O	V
CA-7(4)	MONITOROWANIE RYZYKA	O/S	V
CA-7(5)	ANALIZA SPÓJNOŚCI	O	V
CA-7(6)	AUTOMATYZACJA WSPARCIA MONITOROWANIA	O/S	V
CA-8	**BADANIE PENETRACYJNE**	O	V

NUMER ZABEZPIECZENIA	**NAZWA ZABEZPIECZENIA PODSTAWOWEGO** NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
CA-8(1)	NIEZALEŻNY TESTER LUB ZESPÓŁ PENETRACYJNY	O	V
CA-8(2)	ĆWICZENIA ZESPOŁU ATAKUJĄCEGO TYPU „RED TEAM”	O	V
CA-8(3)	LOKALNE TESTY PENETRACYJNE	O	V
CA-9	**POŁĄCZENIA WEWNĘTRZSYSTEMOWE**	O	V
CA-9(1)	KONTROLE ZGODNOŚCI	O/S	V

TABELA C-5 KATEGORIA CM - ZARZĄDZANIE KONFIGURACJĄ

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
CM-1	**POLITYKA I PROCEDURY**	O	V
CM-2	**KONFIGURACJA BAZOWA**	O	V
CM-2(1)	*PRZEGLĄDY I AKTUALIZACJE*	*W: włączone do CM-2.*	
CM-2(2)	AUTOMATYZACJA WSPIERAJĄCA AKTUALNOŚĆ / SZCZEGÓŁOWOŚĆ	O	V
CM-2(3)	RETENCJA ZACHOWANYCH KONFIGURACJI	O	V
CM-2(4)	*NIEAUTORYZOWANE OPROGRAMOWANIE*	*W: włączone do CM-7.*	
CM-2(5)	*AUTORYZOWANE OPROGRAMOWANIE*	*W: włączone do CM-7.*	
CM-2(6)	ŚRODOWISKA PROGRAMISTYCZNE I TESTOWE	O	V
CM-2(7)	KONFIGUROWANIE SYSTEMÓW I KOMPONENTÓW W OBSZARACH WYSOKIEGO RYZYKA	O	V
CM-3	**ZABEZPIECZANIE ZMIAN KONFIGURACJI**	O	V
CM-3(1)	AUTOMATYCZNA DOKUMENTACJA / POWIADAMIANIE / ZAKAZ WPROWADZANIA ZMIAN	O	V
CM-3(2)	TESTY, WALIDACJA I ZMIANY DOKUMENTÓW	O	V
CM-3(3)	AUTOMATYCZNE WPROWADZANIE ZMIAN	O	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
CM-3(4)	FUNKCYJNI DS. BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI	O	
CM-3(5)	AUTOMATYCZNA REAKCJA BEZPIECZEŃSTWA	S	
CM-3(6)	ZARZĄDZANIE KRYPTOGRAFICZNE	O	
CM-3(7)	PRZEGLĄD ZMIAN W SYSTEMIE	O	
CM-3(8)	ZAPOBIEGANIE LUB OGRANICZANIE ZMIAN KONFIGURACJI	S	
CM-4	**ANALIZY WPŁYWU**	O	V
CM-4(1)	ODDZIELNE ŚRODOWISKA BADAWCZE	O	V
CM-4(2)	WERYFIKACJA ZABEZPIECZEŃ	O	V
CM-5	**OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN**	O	
CM-5(1)	AUTOMATYCZNE EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU I ZAPISY Z AUDYTU	S	
CM-5(2)	*PRZEGLĄD ZMIAN W SYSTEMIE*	*W: włączone do CM-3(7).*	
CM-5(3)	*PODPISANE KOMPONENTY*	*W: włączone do CM-14.*	
CM-5(4)	PODWÓJNA AUTORYZACJA	O/S	
CM-5(5)	OGRANICZANIE PRZYWILEJÓW W ZAKRESIE WYTWARZANIA I EKSPLOATACJI	O	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
CM-5(6)	OGRANICZANIE PRZYWILEJÓW W BIBLIOTEKACH OPROGRAMOWANIA	O/S	
CM-5(7)	*AUTOMATYCZNE WDRAŻANIE ŚRODKÓW BEZPIECZEŃSTWA*	*W: włączone do SI-7.*	
CM-6	**USTAWIENIA KONFIGURACYJNE**	O/S	
CM-6(1)	AUTOMATYCZNE ZARZĄDZANIE, STOSOWANIE I WERYFIKACJA	O	
CM-6(2)	ODPOWIEDŹ NA NIEAUTORYZOWANE ZMIANY	O	
CM-6(3)	*WYKRYWANIE NIEAUTORYZOWANYCH ZMIAN*	*W: włączone do SI-7.*	
CM-6(4)	*PREZENTACJA ZGODNOŚCI*	*W: włączone do CM-4.*	
CM-7	**ZASADA MINIMALNEJ FUNKCJONALNOŚCI**	O/S	
CM-7(1)	PRZEGLĄDY OKRESOWE	O/S	
CM-7(2)	ZAPOBIEGANIE WYKONYWANIU PROGRAMU	S	
CM-7(3)	STOSOWANIE REJESTRACJI	O	
CM-7(4)	NIEAUTORYZOWANE OPROGRAMOWANIE („CZARNA LISTA”)	O/S	
CM-7(5)	AUTORYZOWANE OPROGRAMOWANIE („BIAŁA LISTA”)	O/S	
CM-7(6)	ZAMKNIĘTE ŚRODOWISKA Z OGRANICZONYMI UPRAWNIENIAMI	O	V
CM-7(7)	WYKONYWANIE KODU W CHRONIONYCH ŚRODOWISKACH	O/S	V

NUMER ZABEZPIECZENIA	**NAZWA ZABEZPIECZENIA PODSTAWOWEGO** NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
CM-7(8)	KOD BINARNY LUB KOD WYKONYWALNY (MOBILNY)	O/S	V
CM-7(9)	ZAKAZ UŻYWANIA NIEAUTORYZOWANEGO SPRZĘTU	O/S	V
CM-8	**INWENTARYZACJA KOMPONENTÓW SYSTEMU**	O	V
CM-8(1)	AKTUALIZACJE INSTALACJI I USUWANIA KOMPONENTÓW	O	V
CM-8(2)	AUTOMATYCZNA KONSERWACJA (UTRZYMYWANIE)	O	V
CM-8(3)	AUTOMATYCZNE WYKRYWANIE KOMPONENTÓW NIEAUTORYZOWANYCH	O	V
CM-8(4)	INFORMACJA DOTYCZĄCE ODPOWIEDZIALNOŚCI I ROZLICZALNOŚCI	O	V
CM-8(5)	*BRAK DUPLIKACJI KOMPONENTÓW*	*W: włączone do CM-8.*	
CM-8(6)	OCENA KONFIGURACJI I ZATWIERDZONE ODSTĘPSTWA	O	V
CM-8(7)	SCENTRALIZOWANE REPOZYTORIUM	O	V
CM-8(8)	AUTOMATYCZNE ŚLEDZENIE LOKALIZACJI	O	V
CM-8(9)	PRZYPISANIE KOMPONENTÓW DO SYSTEMÓW	O	V
CM-9	**PLAN ZARZĄDZANIA KONFIGURACJĄ**	O	
CM-9(1)	PRZYPISANIE ODPOWIEDZIALNOŚCI	O	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
CM-10	**OGRANICZENIA W UŻYCIU OPROGRAMOWANIA**	O	
CM-10(1)	OPROGRAMOWANIE OTWARTE (OPEN-SOURCE)	O	
CM-11	**OPROGRAMOWANIE ZAINSTALOWANE PRZEZ UŻYTKOWNIKA**	O	
CM-11(1)	*OSTRZEGANIE O NIEAUTORYZOWANYCH INSTALACJACH*	*W: włączone do CM8(3)*	
CM-11(2)	ZABRONIONA INSTALACJA BEZ POSIADANIA STOSOWNYCH UPRAWNIEŃ	S	
CM-11(3)	AUTOMATYCZNE EGZEKWOWANIE I MONITOROWANIE	S	V
CM-12	**POŁOŻENIE (LOKACJA) INFORMACJI**	O	V
CM-12(1)	AUTOMATYCZNE NARZĘDZIA DO OBSŁUGI LOKACJI INFORMACJI	O	V
CM-13	**MAPOWANIE DZIAŁAŃ NA DANYCH**	O	
CM-14	**PODPISYWANIE KOMPONENTÓW**	O/S	V

TABELA C-6 KATEGORIA CP - PLANOWANIE AWARYJNE / CIĄGŁOŚĆ DZIAŁANIA

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
CP-1	**POLITYKA I PROCEDURY**	O	V
CP-2	**PLAN CIĄGŁOŚCI DZIAŁANIA**	O	
CP-2(1)	KOORDYNACJA Z POWIĄZANYMI PLANAMI	O	
CP-2(2)	PLANOWANIE ZDOLNOŚCI FUNKCJONOWANIA	O	
CP-2(3)	WZNAWIANIE PODSTAWOWYCH DZIAŁAŃ I FUNKCJI BIZNESOWYCH	O	
CP-2(4)	*PRZYWRÓCENIE DZIAŁANIA WSZYSTKICH FUNKCJI BIZNESOWYCH*	*W: włączone do CP-2(3).*	
CP-2(5)	KONTYNUACJA NIEZBĘDNYCH DZIAŁAŃ / FUNKCJI BIZNESOWYCH	O	
CP-2(6)	PROCESY ALTERNATYWNE / ZAPASOWE MIEJSCA PRZETWARZANIA	O	
CP-2(7)	KOORDYNACJA Z USŁUGODAWCAMI ZEWNĘTRZNYMI	O	
CP-2(8)	IDENTYFIKACJA ZASOBÓW KRYTYCZNYCH	O	
CP-3	**SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA**	O	V
CP-3(1)	WYDARZENIA SYMULOWANE	O	V
CP-3(2)	ZAUTOMATYZOWANE ŚRODOWISKA SZKOLENIOWE	O	V
CP-4	**TESTOWANIE PLANU AWARYJNEGO**	O	V
CP-4(1)	KOORDYNACJA Z POWIĄZANYMI PLANAMI	O	V
CP-4(2)	ZAPASOWE MIEJSCE PRZETWARZANIA	O	V
CP-4(3)	AUTOMATYCZNE TESTOWANIE	O	V

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
CP-4(4)	PEŁNE ODZYSKIWANIE I ODTWARZANIE	O	V
CP-4(5)	PRÓBNE AWARIE	O/S	V
CP-5	*AKTUALIZACJA PLANU AWARYJNEGO*	*W: włączone do CP-2.*	
CP-6	**ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII**	O	
CP-6(1)	SEPARACJA OD MIEJSCA GŁÓWNEGO	O	
CP-6(2)	CZAS ODZYSKIWANIA I PUNKT ODTWORZENIA DANYCH	O	
CP-6(3)	DOSTĘPNOŚĆ	O	
CP-7	**ZAPASOWE MIEJSCE PRZETWARZANIA**	O	
CP-7(1)	ODSEPAROWANIE OD LOKALIZACJI PODSTAWOWEJ	O	
CP-7(2)	DOSTĘPNOŚĆ	O	
CP-7(3)	PRIORYTET USŁUG	O	
CP-7(4)	GOTOWOŚĆ DO UŻYCIA	O	
CP-7(5)	*ZASTĘPCZE ŚRODKI BEZPIECZEŃSTWA*	*W: włączone do CP-7.*	
CP-7(6)	BRAK MOŻLIWOŚCI POWROTU DO LOKALIZACJI PODSTAWOWEJ	O	
CP-8	**USŁUGI TELEKOMUNIKACYJNE**	O	
CP-8(1)	PRIORYTETY ŚWIADCZENIA USŁUG	O	
CP-8(2)	POJEDYNCZE PUNKTY AWARII	O	
CP-8(3)	ROZDZIELENIE DOSTAWCÓW PODSTAWOWYCH I ALTERNATYWNYCH	O	
CP-8(4)	PLAN AWARYJNY DOSTAWCY	O	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
CP-8(5)	ALTERNATYWNE TESTOWANIE USŁUG TELEKOMUNIKACYJNYCH	O	
CP-9	**KOPIA ZAPASOWA**	O	
CP-9(1)	BADANIE NIEZAWODNOŚCI NOŚNIKÓW / INTEGRALNOŚCI INFORMACJI	O	
CP-9(2)	TESTY ODTWORZENIOWE Z WYKORZYSTANIEM PRÓBEK DANYCH	O	
CP-9(3)	SEPARACJA PRZECHOWYWANIA INFORMACJI KRYTYCZNYCH	O	
CP-9(4)	*OCHRONA PRZED NIEAUTORYZOWANĄ MODYFIKACJĄ*	*W: włączone do CP-9.*	
CP-9(5)	PRZEKAZANIE KOPII DO ALTERNATYWNEJ LOKALIZACJI	O	
CP-9(6)	REDUNDANCJA (NADMIAROWOŚĆ) SYSTEMU	O	
CP-9(7)	PODWÓJNA AUTORYZACJA	O	
CP-9(8)	OCHRONA KRYPTOGRAFICZNA	O	
CP-10	**ODZYSKIWANIE I ODTWARZANIE SYSTEMU**	O	
CP-10(1)	*TESTOWANIE PLANU AWARYJNEGO*	*W: włączone do CP-4.*	
CP-10(2)	ODTWARZANIE TRANSAKCJI	O	
CP-10(3)	*KOMPENSACYJNE ŚRODKI BEZPIECZEŃSTWA*	*W: omawiane w procesie dostosowywania zabezpieczeń*	
CP-10(4)	PRZYWRACANIE W OKREŚLONYM PRZEDZIALE CZASOWYM	O	
CP-10(5)	*PRACE AWARYJNE*	*W: włączone do SI-13.*	
CP-10(6)	OCHRONA KOMPONENETÓW	O	
CP-11	**ALTERNATYWNE PROTOKOŁY KOMUNIKACJI**	O	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
CP-12	**TRYB BEZPIECZNY**	S	V
CP-13	**ALTERNATYWNE MECHANIZMY BEZPIECZEŃSTWA**	O/S	

TABELA C-7 KATEGORIA IA - IDENTYFIKACJA I UWIERZYTELNIANIE

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
IA-1	**POLITYKA I PROCEDURY**	O	V
IA-2	**IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI)**	O/S	
IA-2(1)	UWIERZYTELNIANIE WIELOSKŁADNIKOWE DOSTĘPU DO KONT UPRZYWILEJOWANYCH	S	
IA-2(2)	UWIERZYTELNIANIE WIELOSKŁADNIKOWE DOSTĘPU DO KONT NIEUPRZYWILEJOWANYCH	S	
IA-2(3)	*DOSTĘP LOKALNY DO KONT UPRZYWILEJOWANYCH*	*W: włączone do IA-2(1)(2).*	
IA-2(4)	*DOSTĘP LOKALNY DO KONT NIEUPRZYWILEJOWANYCH*	*W: włączone do IA-2(1)(2).*	
IA-2(5)	UWIERZYTELNIANIE INDYWIDUALNE PRZED UWIERZYTELNIANIEM GRUPOWYM	O/S	
IA-2(6)	DOSTĘP DO KONT – ODSEPAROWANE URZĄDZENIE	S	
IA-2(7)	*DOSTĘP SIECIOWY DO KONT NIEUPRZYWILEJOWANYCH – ODSEPAROWANE URZĄDZENIE*	*W: włączone do IA-2(6).*	
IA-2(8)	DOSTĘP DO KONT – ODPORNOŚĆ NA POWTARZANIE	S	
IA-2(9)	DOSTĘP SIECIOWY DO KONT NIEUPRZYWILEJOWANYCH – ODPORNOŚĆ NA POWTARZANIE	*W: włączone do IA-2(8).*	
IA-2(10)	LOGOWANIE POJEDYNCZE (SINGLE SIGN-ON)	S	
IA-2(11)	*ZDALNY DOSTĘP - ODSEPAROWANE URZĄDZENIE*	*W: włączone do IA-2(6).*	
IA-2(12)	AUTORYZACJA DANYCH DOSTĘPOWYCH	S	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
IA-2(13)	UWIERZYTELNIANIE "POZA PASMEM" (Z WYKORZYSTANIEM DWÓCH ODDZIELNYCH ŚCIEŻEK)	S	
IA-3	**IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA**	S	
IA-3(1)	DWUKIERUNKOWE UWIERZYTELNIANIE KRYPTOGRAFICZNE	S	
IA-3(2)	*DWUKIERUNKOWE SIECIOWE UWIERZYTELNIANIE KRYPTOGRAFICZNE*	*W: włączone do IA-3(1).*	
IA-3(3)	ALOKACJA ADRESU DYNAMICZNEGO	O	
IA-3(4)	ATESTACJA URZĄDZENIA	O	
IA-4	**ZARZĄDZANIE IDENTYFIKATOREM**	O	
IA-4(1)	ZAKAZ UŻYWANIA IDENTYFIKATORÓW KONT JAKO IDENTYFIKATORÓW PUBLICZNYCH	O	
IA-4(2)	*AUTORYZACJA PRZEŁOŻONEGO*	*W: włączone do IA-12(1).*	
IA-4(3)	*WIELE FORM CERTYFIKACJI*	*W: włączone do IA-12(2)*	
IA-4(4)	IDENTYFIKACJA STATUSU UŻYTKOWNIKA	O	
IA-4(5)	ZARZĄDZANIE DYNAMICZNE	S	
IA-4(6)	ZARZĄDZANIE MIĘDZYORGANIZACYJNE	O	
IA-4(7)	*REJESTRACJA OSOBISTA*	*W: włączone do IA-12(4)*	
IA-4(8)	PAROWANIE IDENTYFIKATORÓW PODCZAS PSEUDONIMIZACJI	O	
IA-4(9)	UTRZYMANIE I OCHRONA ATRYBUTÓW	O/S	
IA-5	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA**	O/S	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
IA-5(1)	UWIERZYTELNIANIE OPARTE O HASŁA	O/S	
IA-5(2)	UWIERZYTELNIANIE OPARTE O INFRASTRUKTURĘ KLUCZA PUBLICZNEGO	S	
IA-5(3)	*REJESTRACJA OSOBISTA LUB PRZEZ ZAUFANĄ TRZECIĄ STRONĘ*	*W: włączone do IA-12(4).*	
IA-5(4)	*AUTOMATYCZNE WSPARCIE OKREŚLANIA SIŁY HASŁA*	*W: włączone do IA-5(1).*	
IA-5(5)	ZMIANA METODY UWIERZYTELNIANIA PRZED DOSTAWĄ	O	
IA-5(6)	OCHRONA METOD UWIERZYTELNIANIA	O	
IA-5(7)	BRAK WBUDOWANYCH NIEZASZYFROWANYCH STATYCZNYCH ELEMENTÓW UWIERZYTELNIANIA	O	
IA-5(8)	JEDNO KONTO W WIELU SYSTEMACH INFORMACYJNYCH	O	
IA-5(9)	ZARZĄDZANIE DANYMI UWIERZYTELNIAJĄCYMI MIĘDZY ORGANIZACJAMI	O	
IA-5(10)	DYNAMICZNE KOJARZENIE DANYCH UWIERZYTELNIAJĄCYCH	S	
IA-5(11)	*UWIERZYTELNIANIE PRZY UŻYCIU TOKENA*	*W: włączone do IA-2(1) i IA-2(2).*	
IA-5(12)	WYDAJNOŚĆ UWIERZYTELNIANIA BIOMETRYCZNEGO	S	
IA-5(13)	PRZEDAWNIENIE BUFOROWANYCH ELEMENTÓW UWIERZYTELNIANIA	S	
IA-5(14)	ZARZĄDZANIE ZAWARTOŚCIĄ ZAUFANYCH MAGAZYNÓW INFRASTRUKTURY KLUCZA PUBLICZNEGO	O	
IA-5(15)	ZATWIERDZANIE PRODUKÓW I USŁUG WEDŁUG Z GÓRY USTALONYCH REGUŁ	O	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
IA-5(16)	WYDAWANIE POŚWIADCZEŃ UWIERZYTELNIAJĄCYCH OSOBIŚCIE LUB PRZEZ ZAUFANĄ TRZECIĄ STRONĘ	O	
IA-5(17)	WYKRYWANIE ATAKÓW PREZENTACYJNYCH PODCZAS UWIERZYTELNIANIA BIOMETRYCZNEGO	S	
IA-5(18)	MENEDŻER HASEŁ	S	
IA-6	**OCHRONA PROCESU UWIERZYTELNIANIA**	S	
IA-7	**MODUŁ KRYPTOGRAFICZNY UWIERZYTELNIANIE**	S	
IA-8	**IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI)**	S	
IA-8(1)	AKCEPTACJA POŚWIADCZEŃ TOŻSAMOŚCI WYDANYCH PRZEZ INNE ORGANIZACJE	S	
IA-8(2)	AKCEPTACJA POŚWIADCZEŃ STRON TRZECICH	S	
IA-8(3)	*WYKORZYSTANIE CERTYFIKOWANYCH PRODUKTÓW*	*W: włączone do IA-8(2).*	
IA-8(4)	WYKORZYSTANIE PROFILI WYDAWANYCH PRZEZ STOSOWNE INSTYTUCJE	S	
IA-8(5)	AKCEPTACJA POŚWIADCZEŃ OSOBISTEJ WERYFIKACJI TOŻSAMOŚCI	S	
IA-8(6)	NIEPOŁĄCZALNOŚĆ (DEZASOCJACYJNOŚĆ)	O	
IA-9	**IDENTYFIKACJA I UWIERZYTELNIANIE USŁUG**	O/S	
IA-9(1)	*WYMIANA INFORMACJI*	*W: włączone do IA-9.*	
IA-9(2)	*PRZEKAZYWANIE DECYZJI O POZYTYWNEJ IDENTYFIKACJI I UWIERZYTELNIENIU*	*W: włączone do IA-9.*	
IA-10	**UWIERZYTELNIANIE ADAPTACYJNE**	O	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
IA-11	**PONOWNE UWIERZYTELNIENIE**	O/S	
IA-12	**POTWIERDZENIE TOŻSAMOŚCI**	O	
IA-12(1)	AUTORYZACJA PRZEŁOŻONEGO	O	
IA-12(2)	DOWODZENIE TOŻSAMOŚCI	O	
IA-12(3)	POTWIERDZANIE I WERYFIKACJA DOWODÓW TOŻSAMOŚCI	O	
IA-12(4)	OSOBISTE ZATWIERDZENIE I WERYFIKACJA	O	
IA-12(5)	POTWIERDZENIE ADRESU	O	
IA-12(6)	AKCEPTACJA ZEWNĘTRZNYCH TOŻSAMOŚCI	O	

TABELA C-8 KATEGORIA IR - REAGOWANIE NA INCYDENTY

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
IR-1	**POLITYKA I PROCEDURY**	O	V
IR-2	**SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY**	O	V
IR-2(1)	WYDARZENIA SYMULOWANE	O	V
IR-2(2)	ZAUTOMATYZOWANE ŚRODOWISKA SZKOLENIOWE	O	V
IR-2(3)	NARUSZENIE	O	V
IR-3	**TESTOWANIE REAGOWANIA NA INCYDENTY**	O	V
IR-3(1)	AUTOMATYCZNE TESTOWANIE	O	V
IR-3(2)	KOORDYNACJA Z POWIĄZANYMI PLANAMI	O	V
IR-3(3)	CIĄGŁE DOSKONALENIE	O	V
IR-4	**OBSŁUGA INCYDENTÓW**	O	
IR-4(1)	AUTOMATYCZNE PROCESY OBSŁUGI ZDARZEŃ	O	
IR-4(2)	DYNAMICZNA REKONFIGURACJA	O	
IR-4(3)	CIĄGŁOŚĆ OPERACJI	O	
IR-4(4)	KORELACJA INFORMACJI	O	
IR-4(5)	AUTOMATYCZNE WYŁĄCZANIE SYSTEMU	O/S	
IR-4(6)	ZAGROŻENIA WEWNĘTRZNE	O	
IR-4(7)	ZAGROŻENIA WEWNĘTRZNE - KOORDYNACJA WEWNĄTRZ ORGANIZACJI	O	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
IR-4(8)	KOORDYNACJA Z ORGANIZACJAMI ZEWNĘTRZNYMI	O	
IR-4(9)	ZDOLNOŚĆ DO REAGOWANIA DYNAMICZNEGO	O	
IR-4(10)	KOORDYNACJA ŁAŃCUCHA DOSTAW	O	
IR-4(11)	ZINTEGROWANY ZESPÓŁ REAGOWANIA NA INCYDENTY	O	
IR-4(12)	ANALIZA KRYMINALISTYCZNA ZŁOŚLIWEGO KODU	O	
IR-4(13)	ANALIZA ZACHOWANIA	O	
IR-4(14)	OPERACYJNE CENTRUM BEZPIECZEŃSTWA (SOC)	O/S	
IR-4(15)	RELACJE PUBLICZNE I NAPRAWA REPUTACJI	O	
IR-5	**MONITOROWANIE INCYDENTÓW**	O	V
IR-5(1)	AUTOMATYCZNE ŚLEDZENIE, ZBIERANIE DANYCH I ANALIZA	O	V
IR-6	**ZGŁASZANIE INCYDENTÓW**	O	
IR-6(1)	ZGŁASZANIE AUTOMATYCZNE	O	
IR-6(2)	PODATNOŚĆ NA INCYDENTY	O	
IR-6(3)	KOORDYNACJA ŁAŃCUCHA DOSTAW	O	
IR-7	**WSPARCIE REAGOWANIA NA INCYDENTY**	O	
IR-7(1)	AUTOMATYCZNE WSPARCIE DOSTĘPNOŚCI INFORMACJI / OBSŁUGI	O	
IR-7(2)	KOORDYNACJA Z DOSTAWCAMI ZEWNĘTRZNYMI	O	
IR-8	**PLAN REAGOWANIA NA INCYDENTY**	O	
IR-8(1)	NARUSZENIA	O	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
IR-9	**REAKCJA NA WYCIEK / UJAWNIENIE INFORMACJI**	O	
IR-9(1)	*ODPOWIEDZIALNY PERSONEL*	*W: włączone do IR-9.*	
IR-9(2)	SZKOLENIE	O	
IR-9(3)	DZIAŁANIA PO UJAWNIENIU	O	
IR-9(4)	WYSTAWIENIE NA DZIAŁANIA OSÓB NIEAUTORYZOWANYCH	O	
IR-10	*ZINTEGROWANY ZESPÓŁ DS. ANALIZY BEZPIECZEŃSTWA INFORMACJI*	*W: włączone do IR-4(11).*	

TABELA C-9 KATEGORIA MA – UTRZYMANIE I WSPARCIE

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
MA-1	**POLITYKA I PROCEDURY**	O	V
MA-2	**NADZÓR NAD UTRZYMANIEM**	O	
MA-2(1)	*ZAWARTOŚĆ REKORDU*	*W: włączone do MA-2.*	
MA-2(2)	AUTOMATYCZNE DZIAŁANIA KONSERWACYJNE	O	
MA-3	**NARZĘDZIA UTRZYMANIOWE**	O	
MA-3(1)	SPRAWDZANIE NARZĘDZI	O	
MA-3(2)	SPRAWDZANIE NOŚNIKÓW DANYCH	O	
MA-3(3)	ZAPOBIEGANIE NIEAUTORYZOWANEMU USUWANIU	O	
MA-3(4)	OGRANICZANIE UŻYWANIA NARZĘDZI	O/S	
MA-3(5)	WYKORZYSTYWANIE PODWYŻSZONYCH UPRAWNIEŃ	O/S	
MA-3(6)	AKTUALIZACJE I POPRAWKI OPROGRAMOWANIA	O/S	
MA-4	**UTRZYMANIE ZDALNE**	O	
MA-4(1)	AUDYT I PRZEGLĄD	O	
MA-4(2)	*DOKUMENTY ZDALNEGO UTRZYMANIE*	*W: włączone do MA-1 i MA-4.*	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
MA-4(3)	PORÓWNYWALNE POZIOMY BEZPIECZEŃSTWA / SANITYZACJA	O	
MA-4(4)	UWIERZYTELNIANIE / SEPARACJA SESJI UTRZYMANIOWYCH	O	
MA-4(5)	ZGODY I POWIADOMIENIA	O	
MA-4(6)	OCHRONA KRYPTOGRAFICZNA	O/S	
MA-4(7)	ZDALNA WERYFIKACJA ZAKOŃCZENIA SESJI	S	
MA-5	**PERSONEL UTZRYMANIOWY**	O	
MA-5(1)	OSOBY NIEPOSIADAJĄCE STOSOWNYCH PRAW DOSTĘPU	O	
MA-5(2)	POŚWIADCZENIA BEZPIECZEŃSTWA / SYSTEMY NIEJAWNE	O	
MA-5(3)	OBYWATELSTWO / SYSTEMY NIEJAWNE	O	
MA-5(4)	CUDZOZIEMCY	O	
MA-5(5)	OBSŁUGA NIEZWIĄZANA Z UTRZYMANIEM SYSTEMU	O	
MA-6	**TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI**	O	
MA-6(1)	KONSERWACJA ZAPOBIEGAWCZA	O	
MA-6(2)	KONSERWACJA PLANOWA	O	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
MA-6(3)	AUTOMATYCZNE WSPARCIE W ZAKRESIE KONSERWACJI PROGNOZOWANEJ	O	
MA-7	**KONSERWACJA W TERENIE**	O	

TABELA C-10 KATEGORIA MP - OCHRONA NOŚNIKÓW DANYCH

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
MP-1	**POLITYKA I PROCEDURY**	O	V
MP-2	**DOSTĘP DO NOŚNIKÓW DANYCH**	O	
MP-2(1)	*OGRANICZONY DOSTĘP AUTOMATYCZNY*	*W: włączone do MP-4(2).*	
MP-2(2)	*OCHRONA KRYPTOGRAFICZNA*	*W: włączone do SC-28(1).*	
MP-3	**OZNAKOWANIE NOŚNIKÓW DANYCH**	O	
MP-4	**PRZECHOWYWANIE NOŚNIKÓW DANYCH**	O	
MP-4(1)	*OCHRONA KRYPTOGRAFICZNA*	*W: włączone do SC-28(1).*	
MP-4(2)	OGRANICZONY DOSTĘP AUTOMATYCZNY	O	
MP-5	**TRANSPORT NOŚNIKÓW DANYCH**	O	
MP-5(1)	*OCHRONA POZA STREFAMI KONTROLNYMI*	*W: włączone do MP-5.*	
MP-5(2)	*DOKUMENTOWANIE DZIAŁAŃ*	*W: włączone do MP-5.*	
MP-5(3)	KONWOJENCI	O	
MP-5(4)	*OCHRONA KRYPTOGRAFICZNA*	*W: włączone do SC-28(1).*	
MP-6	**SANITYZACJA NOŚNIKÓW DANYCH**	O	
MP-6(1)	PRZEGLĄD / ZATWIERDZANIE / ŚLEDZENIE / DOKUMENTOWANIE / WERYFIKACJA	O	
MP-6(2)	TESTOWANIE SPRZĘTU	O	
MP-6(3)	TECHNIKI NIEDESTRUKCYJNE	O	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
MP-6(4)	*KONTROLOWANE INFORMACJE JAWNE*	*W: włączone do MP-6.*	
MP-6(5)	*INFORMACJE NIEJAWNE*	*W: włączone do MP-6.*	
MP-6(6)	*NISZCZENIE NOŚNIKÓW DANYCH*	*W: włączone do MP-6.*	
MP-6(7)	PODWÓJNE UPOWAŻNIENIE	O	
MP-6(8)	ZDALNE KASOWANIE / WYMAZYWANIE INFORMACJI	O	
MP-7	**UŻYWANIE NOŚNIKÓW DANYCH**	O	
MP-7(1)	*ZABRONIONE WYKORZYSTANIE NIEZIDENTYFIKOWANEJ WŁASNOŚCI*	*W: włączone do MP-7.*	
MP-7(2)	ZABRONIONE WYKORZYSTANIE MEDIÓW ODPORNYCH NA SANITYZACJĘ	O	
MP-8	**DEKLASYFIKACJA NOŚNIKÓW DANYCH**	O	
MP-8(1)	DOKUMENTACJA PROCESU	O	
MP-8(2)	TESTOWANIE SPRZĘTU	O	
MP-8(3)	KONTROLOWANE INFORMACJE JAWNE	O	
MP-8(4)	INFORMACJE NIEJAWNE	O	

TABELA C-11 KATEGORIA PE – OCHRONA FIZYCZNA I ŚRODOWISKOWA

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
PE-1	**POLITYKA I PROCEDURY**	O	V
PE-2	**ZEZWOLENIA NA DOSTĘP FIZYCZNY**	O	
PE-2(1)	DOSTĘP ZGODNIE Z POSIADANĄ POZYCJĄ / ROLĄ	O	
PE-2(2)	PODWÓJNA IDENTYFIKACJA	O	
PE-2(3)	OGRANICZANIE DOSTĘPU BEZ ASYSTY	O	
PE-3	**KONTROLA DOSTĘPU FIZYCZNEGO**	O	
PE-3(1)	DOSTĘP DO SYSTEMU	O	
PE-3(2)	OBIEKT / OBSZAR SYSTEMU	O	
PE-3(3)	CIĄGŁOŚĆ OCHRONY FIZYCZNEJ	O	
PE-3(4)	ZAMYKANE OBUDOWY	O	
PE-3(5)	OCHRONA PRZED MANIPULACJĄ	O	
PE-3(6)	*TESTY PENETRACYJNE OBIEKTU*	*W: włączone do CA-8.*	
PE-3(7)	BARIERY FIZYCZNE	O	
PE-3(8)	ŚLUZY W KONTROLI DOSTĘPU	O	
PE-4	**KONTROLA DOSTĘPU DO MEDIUM TRANSMISYJNEGO**	O	
PE-5	**KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA**	O	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
PE-5(1)	*DOSTĘP UPOWAŻNIONYCH OSÓB DO URZĄDZEŃ*	*W: włączone do PE-5.*	
PE-5(2)	DOSTĘP DO DANYCH NA PODSTAWIE INDYWIDUALNEJ TOŻSAMOŚCI	S	
PE-5(3)	*OZNACZANIE URZĄDZEŃ WEJŚCIA - WYJŚCIA*	*W: włączone do PE-22.*	
PE-6	**MONITOROWANIE DOSTĘPU FIZYCZNEGO**	O	V
PE-6(1)	ALARMY WŁAMANIOWE I URZĄDZENIA NADZORUJĄCE	O	V
PE-6(2)	AUTOMATYCZNE ROZPOZNAWANIE WŁAMANIA / INFORMOWANIE	O	V
PE-6(3)	MONITORING WIZYJNY	O	V
PE-6(4)	MONITOROWANIE DOSTĘPU FIZYCZNEGO DO SYSTEMÓW	O	V
PE-7	***KONTROLA GOŚCI***	***W: włączone do PE-2 i PE-3.***	
PE-8	**REJESTRY DOSTĘPU GOŚCI**	O	V
PE-8(1)	AUTOMATYCZNA REJESTRACJA / PRZEGLĄD	O	
PE-8(2)	*ZAPISY DOTYCZĄCE DOSTĘPU FIZYCZNEGO*	*W: włączone do PE-2.*	
PE-8(3)	OGRANICZANIE ELEMENTÓW DANYCH OSOBOWYCH UMOŻLIWIAJĄCYCH IDENTYFIKACJĘ	O	
PE-9	**WYPOSAŻENIE ENERGETYCZNE I OKABLOWANIE**	O	
PE-9(1)	REDUNDANCJA OKABLOWANIA	O	
PE-9(2)	AUTOMATYCZNA KONTROLA JAKOŚCI NAPIĘCIA	O	
PE-10	**WYŁĄCZENIE AWARYJNE**	O	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
PE-10(1)	*PRZYPADKOWA I NIEAUTORYZOWANA AKTYWACJA*	*W: włączone do PE-10.*	
PE-11	**ZASILANIE AWARYJNE**	O	
PE-11(1)	ALTERNATYWNE ZASILANIE - MINIMALNA ZDOLNOŚĆ OPERACYJNA	O	
PE-11(2)	ALTERNATYWNE SAMOOBSŁUGOWE ŹRÓDŁO ZASILANIA	O	
PE-12	**OŚWIETLENIE AWARYJNE**	O	
PE-12(1)	ZASADNICZE DZIAŁANIA / FUNKCJE BIZNESOWE	O	
PE-13	**OCHRONA PRZECIWPOŻAROWA**	O	
PE-13(1)	SYSTEMY DETEKCJI - AUTOMATYCZNA AKTYWACJA I POWIADAMIANIE	O	
PE-13(2)	SYSTEMY GASZĄCE - AUTOMATYCZNA AKTYWACJA I POWIADOMIENIE	O	
PE-13(3)	*AUTOMATYCZNE GASZENIE POŻARU*	*W: włączone do PE-13(2).*	
PE-13(4)	INSPEKCJE	O	
PE-14	**ZABEZPIECZENIA ŚRODOWISKOWE**	O	
PE-14(1)	STEROWANIE AUTOMATYCZNE	O	
PE-14(2)	MONITOROWANIE ZA POMOCĄ ALARMÓW I POWIADOMIEŃ	O	
PE-15	**OCHRONA PRZED ZALANIEM**	O	
PE-15(1)	AUTOMATYCZNE WYKRYWANIE	O	
PE-16	**DOSTAWA I USUWANIE**	O	
PE-17	**ZAPASOWE MIEJSCE PRACY**	O	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
PE-18	**LOKALIZACJA KOMPONENTÓW SYSTEMU**	O	
PE-18(1)	*LOKALIZACJA OBIEKTU*	*W: włączone do PE-23.*	
PE-19	**ULOT INFORMACJI / ELEKTROMAGNETYCZNA EMISJA UJAWNIAJĄCA**	O	
PE-19(1)	KRAJOWE POLITYKI I PROCEDURY DOTYCZĄCE EMISJI UJAWNIAJĄCEJ	O	
PE-20	**MONITOROWANIE I ŚLEDZENIE ZASOBÓW**	O	
PE-21	**OCHRONA PRZED IMPULSEM ELEKTROMAGNETYCZNYM**	O	
PE-22	**ZNAKOWANIE KOMPONENTÓW**	O	
PE-23	**LOKALIZACJA OBIEKTU**	O	

TABELA C-12 KATEGORIA PL – PLANOWANIE

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
PL-1	**POLITYKA I PROCEDURY**	O	V
PL-2	**PLANY BEZPIECZEŃSTWA SYSTEMU I OCHRONY PRYWATNOŚCI**	O	V
PL-2(1)	*KONCEPCJA DZIAŁANIA*	*W: włączone do PL-7.*	
PL-2(2)	*ARCHITEKTURA FUNKCJONALNA*	*W: włączone do PL-8.*	
PL-2(3)	*PLANOWANIE / KOORDYNACJA Z INNYMI PODMIOTAMI ORGANIZACYJNYMI*	*W: włączone do PL-2.*	
PL-3	*AKTUALIZACJA PLANU BEZPIECZEŃSTWA SYSTEMU*	*W: włączone do PL-2.*	
PL-4	**ZASADY POSTĘPOWANIA**	O	V
PL-4(1)	MEDIA SPOŁECZNOŚCIOWE I OGRANICZENIA KORZYSTANIA ZE STRON / APLIKACJI ZEWNĘTRZNYCH	O	V
PL-5	*OCENA WPŁYWU NA PRYWATNOŚĆ*	*W: włączone do RA-8.*	
PL-6	*PLANOWANIE DZIAŁALNOŚCI ZWIĄZANEJ Z BEZPIECZEŃSTWEM*	*W: włączone do PL-2.*	
PL-7	**KONCEPCJA BEZPIECZEŃSTWA DZIAŁAŃ OPERACYJNYCH**	O	
PL-8	**ARCHITEKTURA BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI**	O	V
PL-8(1)	ZABEZPIECZENIE WIELOSTOPNIOWE (OCHRONA WARSTWOWA)	O	V
PL-8(2)	DYWERSYFIKACJA DOSTAWCY	O	V

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
PL-9	**ZARZĄDZANIE CENTRALNE**	O	V
PL-10	**WYBÓR ZABEZPIECZEŃ BAZOWYCH**	O	
PL-11	**DOSTOSOWYWANIE ZABEZPIECZEŃ BAZOWYCH**	O	

TABELA C-13 KATEGORIA PM – PROGRAMY ZARZĄDZANIA

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
PM-1	**PLAN PROGRAMU BEZPIECZEŃSTWA INFORMACJI**	O	
PM-2	**ROLE KIEROWNICZE PROGRAMU BEZPIECZEŃSTWA INFORMACJI**	O	
PM-3	**ZASOBY W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI I OCHRONY PRYWATNOŚCI**	O	
PM-4	**PLAN DZIAŁANIA I ETAPY WPROWADZANIA ZABEZPIECZEŃ**	O	
PM-5	**INWENTARYZACJA SYSTEMU**	O	
PM-5(1)	REJESTR DANYCH OSOBOWYCH	O	
PM-6	**MIARY WYDAJNOŚCI**	O	V
PM-7	**STRUKTURA ORGANIZACYJNA**	O	
PM-7(1)	ODCIĄŻENIA	O	
PM-8	**PLAN INFRASTRUKTURY KRYTYCZNEJ**	O	
PM-9	**STRATEGIA ZARZĄDZANIA RYZYKIEM**	O	V
PM-10	**PROCES AUTORYZACJI**	O	V
PM-11	**DEFINICJA MISJI I PROCESU BIZNESOWEGO**	O	
PM-12	**ZAGROŻENIA WEWNĘTRZNE**	O	V
PM-13	**PESONEL BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI**	O	
PM-14	**TESTOWANIE, SZKOLENIA I MONITOROWANIE**	O	V

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
PM-15	**GRUPY I STOWARZYSZENIA ZAJMUJĄCE SIĘ BEZPIECZEŃSTWEM I OCHRONĄ PRYWATNOŚCI**	O	
PM-16	**OSTRZEGANIE O ZAGROŻENIACH**	O	V
PM-16(1)	ZAUTOMATYZOWANE ŚRODKI WYMIANY INFORMACJI O ZAGROŻENIACH	O	V
PM-17	**OCHRONA NADZOROWANYCH INFORMACJI JAWNYCH PRZETWARZANYCH W SYSTEMACH ZEWNĘTRZNYCH**	O	V
PM-18	**PLAN PROGRAMU OCHRONY PRYWATNOŚCI**	O	
PM-19	**ROLE KIEROWNICZE PROGRAMU OCHRONY PRYWATNOŚCI**	O	
PM-20	**ROZPOWSZECHNIANIE INFORMACJI O PROGRAMIE OCHRONY PRYWATNOŚCI**	O	
PM-20(1)	POLITYKA PRYWATNOŚCI PREZENTOWANE NA STRONACH INTERNETOWYCH, W APLIKACJACH I USŁUGACH CYFROWYCH	O	V
PM-21	**REJESTROWANIE UJAWNIEŃ**	O	
PM-22	**ZARZĄDZANIE JAKOŚCIĄ DANYCH OSOBOWYCH**	O	V
PM-23	**ORGAN ZARZĄDZANIA DANYMI**	O	V
PM-24	**RADA DS. INTEGRALNOŚCI DANYCH**	O	V
PM-25	**MINIMALIZACJA DANYCH OSOBOWYCH WYKORZYSTYWANYCH W TESTACH, SZKOLENIACH I BADANIACH**	O	
PM-26	**ZARZĄDZANIE SKARGAMI**	O	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
PM-27	**SPRAWOZDAWCZOŚĆ W ZAKRESIE OCHRONY PRYWATNOŚCI**	O	
PM-28	**OPRACOWYWANIE RAM RYZYKA**	O	V
PM-29	**ROLE KIEROWNICZE PROGRAMU ZARZĄDZANIA RYZYKIEM**	O	
PM-30	**STRATEGIA ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW**	O	V
PM-30(1)	DOSTAWCY ELEMENTÓW KRYTYCZNYCH LUB ISTOTNYCH Z PUNKTU WIDZENIA MISJI	O	V
PM-31	**STRATEGIA CIĄGŁEGO MONITORINGU**	O	
PM-32	**PRZEZNACZENIE**	O	V

TABELA C-14 KATEGORIA PS – BEZPIECZEŃSTWO OSOBOWE

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
PS-1	**POLITYKA I PROCEDURY**	O	V
PS-2	**OKREŚLANIE RYZYKA DLA STANOWISKA PRACY**	O	
PS-3	**DOBÓR PERSONELU**	O	
PS-3(1)	INFORMACJE NIEJAWNE	O	
PS-3(2)	POSTĘPOWANIA SPRAWDZAJĄCE	O	
PS-3(3)	INFORMACJE WYMAGAJĄCE SZCZEGÓLNEJ OCHRONY	O	
PS-3(4)	WYMAGANIA DOTYCZĄCE OBYWATELSTWA	O	
PS-4	**ZAKOŃCZENIE ZATRUDNIENIA**	O	
PS-4(1)	ZOBOWIĄZANIA PO ZAKOŃCZENIU ZATRUDNIENIA	O	
PS-4(2)	AUTOMATYCZNE POWIADAMIANIE	O	
PS-5	**OBSADZENIE LUB PRZENIESIENIE STANOWISKA**	O	
PS-6	**UMOWY DOSTĘPU / WSPÓŁPRACY**	O	V
PS-6(1)	*INFORMACJE WYMAGAJĄCE SZCZEGÓLNEJ OCHRONY*	*W: włączone do PS-3.*	
PS-6(2)	INFORMACJE NIEJAWNE WYMAGAJĄCE OCHRONY SPECJALNEJ	O	V
PS-6(3)	WYMOGI PO ZAKOŃCZENIU ZATRUDNIENIA	O	V
PS-7	**BEZPIECZEŃSTWO OSOBOWE STRON TRZECICH**	O	V
PS-8	**SANKCJE PERSONALNE**	O	
PS-9	**OPISY STANOWISK PRACY**	O	

TABELA C-15 KATEGORIA PT- PRZEJRZYSTOŚĆ PRZETWARZANIA DANYCH OSOBOWYCH

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
PT-1	**POLITYKA I PROCEDURY**	O	V
PT-2	**UPRAWNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH**	O	V
PT-2(1)	OZNACZANIE DANYCH	S	V
PT-2(2)	AUTOMATYZACJA	O	V
PT-3	**CELE PRZETWARZANIA DANYCH OSOBOWYCH**	O	
PT-3(1)	OZNACZANIE DANYCH	S	V
PT-3(2)	AUTOMATYZACJA	O	V
PT-4	**ZGODY**	O	
PT-4(1)	ZGODA NA PODSTAWIE ART. 6 UST. 1 RODO	O	
PT-4(2)	ZGODA TYPU „JUST-IN TIME”	O	
PT-4(3)	WYCOFANIE ZGODY	O	
PT-5	**INFORMACJA O OCHRONIE PRYWATNOŚCI**	O	
PT-5(1)	INFORMACJA NA ŻĄDANIE	O	
PT-5(2)	OŚWIADCZENIE O OCHRONIE PRYWATNOŚCI	O	
PT-6	**SYSTEM ZAWIADOMIEŃ O REJESTRACH**	O	
PT-6(1)	RUTYNOWE ZASTOSOWANIE	O	
PT-6(2)	ZASADY WYŁĄCZENIA	O	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
PT-7	**SZCZEGÓŁOWE KATEGORIE DANYCH OSOBOWYCH**	O	
PT-7(1)	IDENTYFIKATOR OSOBY - NP. NR PESEL	O	
PT-7(2)	PRZETWARZANIE WRAŻLIWYCH DANYCH OSOBOWYCH	O	
PT-8	**WYMAGANIA DOTYCZĄCE ZGODNOŚCI PRZY PRZETWARZANIU KOMPUTEROWOWYM**	O	

TABELA C-16 KATEGORIA RA - OCENA RYZYKA

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
RA-1	**POLITYKA I PROCEDURY**	O	V
RA-2	**KATEGORYZACJA BEZPIECZEŃSTWA**	O	
RA-2(1)	PRIORYTETYZACJA POZIOMÓW WPŁYWU	O	
RA-3	**SZACOWANIE RYZYKA**	O	V
RA-3(1)	SZACOWANIE RYZYKA ŁAŃCUCHA DOSTAW	O	V
RA-3(2)	WYMIANA INFORMACJI O ZAGROŻENIACH	O	V
RA-3(3)	ŚWIADOMOŚĆ DYNAMIKI ZAGROŻEŃ	O	V
RA-3(4)	PROGNOZOWANIA CYBERANALITYKA	O	V
RA-4	*AKTUALIZACJA SZACOWANIA RYZYKA*	*W: włączone do RA-3.*	
RA-5	**MONITOROWANIE I SKANOWANIE PODATNOŚCI**	O	V
RA-5(1)	*AKTUALIZACJA NARZĘDZI*	*W: włączone do RA-5.*	
RA-5(2)	NADZOROWANIE WYKRYTYCH PODATNOŚCI	O	V
RA-5(3)	ZAKRES PODATNOŚCI	O	V
RA-5(4)	WYKRYWANIE SKANOWANIA	O	V
RA-5(5)	DOSTĘP UPRZYWILEJOWANY	O	V
RA-5(6)	AUTOMATYCZNE ANALIZY TRENDÓW	O	V
RA-5(7)	*AUTOMATYCZNE WYKRYWANIE I POWIADAMIANIE O NIEAUTORYZOWANYCH KOMPONENTACH*	*W: włączone do CM-8.*	
RA-5(8)	PRZEGLĄD HISTORYCZNYCH LOGÓW AUDYTU	O	V

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
RA-5(9)	*TESTY PENETRACYJNE I ANALIZY*	*W: włączone do CA-8.*	
RA-5(10)	*KORELACJA SKANOWANYCH DANYCH*	O	V
RA-5(11)	PROGRAM UPUBLICZNIANIA PODATNOŚCI	O	V
RA-6	**TECHNICZNE ZABEZPIECZENIE PRZED PODGLĄDEM I PODSŁUCHEM**	O	V
RA-7	**REAKCJA NA RYZYKO**	O	V
RA-8	**OCENY WPŁYWU NA PRYWATNOŚĆ**	O	V
RA-9	**ANALIZA KRYTYCZNOŚCI**	O	
RA-10	**WYSZUKIWANIE ZAGROŻEŃ**	O/S	V

TABELA C-17 KATEGORIA SA - NABYWANIE SYSTEMU I USŁUGI

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SA-1	**POLITYKA I PROCEDURY**	O	V
SA-2	**PRZYDZIAŁ ZASOBÓW**	O	V
SA-3	**CYKL ŻYCIA SYSTEMU**	O	V
SA-3(1)	ZARZĄDZANIE ŚRODOWISKIEM PRZEDPRODUKCYJNYM	O	V
SA-3(2)	WYKORZYSTYWANIE DANYCH BIEŻĄCYCH LUB OPERACYJNYCH	O	V
SA-3(3)	ODŚWIEŻANIE TECHNOLOGII	O	V
SA-4	**PROCES NABYCIA**	O	V
SA-4(1)	WŁAŚCIWOŚCI FUNKCJONALNE ZABEZPIECZEŃ	O	V
SA-4(2)	PROJEKTOWANIE / IMPLEMENTACJA ZABEZPIECZEŃ	O	V
SA-4(3)	METODY, TECHNIKI I PRAKTYKI ROZWOJU	O	V
SA-4(4)	*PRZYPISANIE KOMPONENTÓW DO SYSTEMÓW*	*W: włączone do CM-8(9).*	
SA-4(5)	KONFIGURACJA SYSTEMU, KOMPONENTÓW I USŁUG	O	V
SA-4(6)	KORZYSTANIE Z PRODUKTÓW ZAPEWNIAJĄCYCH BEZPIECZEŃSTWO INFORMACJI	O	V
SA-4(7)	ZATWIERDZONE PROFILE OCHRONY	O	V
SA-4(8)	PLAN CIĄGŁEGO MONITOROWANIA ZABEZPIECZEŃ	O	V
SA-4(9)	FUNKCJE, PORTY, PROTOKOŁY / USŁUGI	O	V
SA-4(10)	WYKORZYSTANIE ZATWIERDZONYCH PRODUKTÓW	O	V
SA-4(11)	SYSTEM DOKUMENTOWANIA	O	V

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SA-4(12)	WŁASNOŚĆ DANYCH	O	V
SA-5	**DOKUMENTACJA SYSTEMU**	O	V
SA-5(1)	*WŁAŚCIWOŚCI FUNKCJONALNE ZABEZPIECZEŃ*	*W: włączone do SA-4(1).*	
SA-5(2)	*BEZPIECZEŃSTWO INTERFEJSÓW SYSTEMU ZEWNĘTRZNEGO*	*W: włączone do SA-4(2).*	
SA-5(3)	*PROJEKTOWANIE WYSOKOPOZIOMOWE*	*W: włączone do SA-4(2).*	
SA-5(4)	*PROJEKTOWANIE NISKOPOZIOMOWE*	*W: włączone do SA-4(2).*	
SA-5(5)	*KOD ŹRÓDŁOWY*	*W: włączone do SA-4(2).*	
SA-6	***OGRANICZENIA W UŻYCIU OPROGRAMOWANIA***	***W: włączone do CM-10 i SI-7.***	
SA-7	***OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA***	***W: włączone do CM-11 i SI-7.***	
SA-8	**ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI**	O	V
SA-8(1)	PRZEJRZYSTE ABSTRAKCJE	O/S	V
SA-8(2)	MINIMALIZACJA MECHANIZMÓW WSPÓLNYCH	O/S	V
SA-8(3)	MODUŁOWOŚĆ I WARSTWOWOŚĆ	O/S	V
SA-8(4)	UPORZĄDKOWANIE ZALEŻNOŚCI POMIĘDZY SEGMENTAMI SYSTEMU	O/S	V
SA-8(5)	DOSTĘP Z EFEKTYWNĄ MEDIACJĄ	O/S	V
SA-8(6)	MINIMALIZACJA WSPÓŁUŻYTKOWANIA	O/S	V
SA-8(7)	ZMNIEJSZONA ZŁOŻONOŚĆ	O/S	V
SA-8(8)	BEZPIECZNA EWOLUCJA	O/S	V

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SA-8(9)	ZAUFANE KOMPONENTY	O/S	V
SA-8(10)	ZAUFANIE HIERARCHICZNE	O/S	V
SA-8(11)	ODWROTNY PRÓG MODYFIKACJI	O/S	V
SA-8(12)	OCHRONA HIERARCHICZNA	O/S	V
SA-8(13)	MINIMALIZACJA ELEMENTÓW BEZPIECZEŃSTWA	O/S	V
SA-8(14)	ZASADA NAJMNIEJSZEGO UPRZYWILEJOWANIA	O/S	V
SA-8(15)	PREDYKAT ZEZWOLEŃ	O/S	V
SA-8(16)	SAMOISTNA WIARYGODNOŚĆ	O/S	V
SA-8(17)	BEZPIECZNY SKŁAD ROZPROSZONY	O/S	V
SA-8(18)	ZAUFANE KANAŁY KOMUNIKACJI	O/S	V
SA-8(19)	CIĄGŁA OCHRONA	O/S	V
SA-8(20)	BEZPIECZNE ZARZĄDZANIE METADANYMI	O/S	V
SA-8(21)	SAMOANALIZY	O/S	V
SA-8(22)	ROZLICZALNOŚĆ I IDENTYFIKOWALNOŚĆ	O/S	V
SA-8(23)	ZABEZPIECZENIA DOMYŚLNE	O/S	V
SA-8(24)	BEZPIECZNA AWARIA I ODZYSKIWANIE DANYCH	O/S	V
SA-8(25)	BEZPIECZEŃSTWO EKONOMICZNE	O/S	V
SA-8(26)	PEWNOŚĆ DZIAŁANIA	O/S	V
SA-8(27)	BEZPIECZEŃSTWO UWZGLĘDNIAJĄCE CZYNNIK LUDZKI	O/S	V

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SA-8(28)	AKCEPTOWALNY POZIOM BEZPIECZEŃSTWA	O/S	V
SA-8(29)	POWTARZALNE I UDOKUMENTOWANE PROCEDURY	O/S	V
SA-8(30)	RYGOR PROCEDURALNY	O/S	V
SA-8(31)	BEZPIECZNA MODYFIKACJA SYSTEMU	O/S	V
SA-8(32)	MIEZBĘDNA DOKUMENTACJA	O/S	V
SA-8(33)	ZASADA MINIMALIZACJA	O/S	V
SA-9	**USŁUGI SYSTEMU ZEWNĘTRZNEGO**	O	V
SA-9(1)	OCENY RYZYKA / ZATWIERDZENIA ORGANIZACYJNE	O	V
SA-9(2)	IDENTYFIKACJA FUNKCJI, PORTÓW, PROTOKOŁÓW I USŁUG	O	V
SA-9(3)	TWORZENIE / UTRZYMANIE RELACJI ZAUFANIA Z DOSTAWCAMI	O	V
SA-9(4)	ZGODNOŚĆ INTERESÓW KONSUMENTÓW I DOSTAWCÓW	O	V
SA-9(5)	OBSZAR PROCESOWANIA, PRZECHOWYWANIA I OBSŁUGI TECHNICZNEJ	O	V
SA-9(6)	NADZOROWANIE ZARZĄDZANIA KLUCZAMI KRYPTOGRAFICZNYMI PRZEZ ORGANIZACJĘ	O	V
SA-9(7)	ORGANIZACYJNIE KONTROLOWANE ZABEZPIECZENIA INTEGRALNOŚCI	O	V
SA-9(8)	MIEJSCE PRZETWARZANIA I PRZECHOWYWANIA - JURYSDYKCJA KRAJOWA	O	V
SA-10	**ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA**	O	V

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SA-10(1)	WERYFIKACJA INTEGRALNOŚCI PROGRAMÓW I OPROGRAMOWANIA UKŁADOWEGO	O	V
SA-10(2)	ALTERNATYWNE PROCESY ZARZĄDZANIA KONFIGURACJĄ	O	V
SA-10(3)	WERYFIKACJA INTEGRALNOŚCI SPRZĘTU	O	V
SA-10(4)	ZAUFANA GENERACJA	O	V
SA-10(5)	INTEGRALNOŚĆ MAPOWANIA KONTROLI WERSJI	O	V
SA-10(6)	ZAUFANA DYSTRYBUCJA	O	V
SA-10(7)	PERSONEL BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI	O	V
SA-11	**TESTOWANIE I OCENA PRZEZ DEWELOPERA**	O	V
SA-11(1)	ANALIZA KODU STATYCZNEGO	O	V
SA-11(2)	MODELOWANIE ZAGROŻEŃ I ANALIZA PODATNOŚCI NA ZAGROŻENIA	O	V
SA-11(3)	NIEZALEŻNA WERYFIKACJA PLANÓW OCENY / EWIDENCJA	O	V
SA-11(4)	MANUALNY PRZEGLĄD KODU	O	V
SA-11(5)	TESTOWANIE PENETRACYJNE	O	V
SA-11(6)	PRZEGLĄD PŁASZCZYZNY ATAKU	O	V
SA-11(7)	WERYFIKACJA ZAKRESU TESTU / OCENA	O	V
SA-11(8)	DYNAMICZNA ANALIZA KODU	O	V
SA-11(9)	INTERAKTYWNE TESTOWANIE BEZPIECZEŃSTWA APLIKACJI	O	V
SA-12	***BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW***	***W: włączone do Kategorii SR.***	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SA-12(1)	*STRATEGIE ZAKUPÓW, NARZĘDZIA I METODY*	*W: włączone do SR-5.*	
SA-12(2)	*DYWERSYFIKACJA DOSTAWCÓW*	*W: włączone do SR-6.*	
SA-12(3)	*ZAUFANA WYSYŁKA I MAGAZYNOWANIE*	*W: włączone do SR-3.*	
SA-12(4)	*RÓŻNORODNOŚĆ DOSTAWCÓW*	*W: włączone do SR-3(1).*	
SA-12(5)	*OGRANICZENIE SZKODY*	*W: włączone do SR-3(2).*	
SA-12(6)	*MINIMALIZACJA CZASU ZAMÓWIENIA*	*W: włączone do SR-5(1).*	
SA-12(7)	*OCENY PRZED WYBOREM / ODBIOREM / AKTUALIZACJĄ*	*W: włączone do SR-5(2).*	
SA-12(8)	*POZYSKIWANIE INFORMACJI Z WSZYSTKICH DOSTĘPNYCH ŹRÓDEŁ*	*W: włączone do RA-3(2).*	
SA-12(9)	*BEZPIECZEŃSTWO OPERACYJNE*	*W: włączone do SR-7.*	
SA-12(10)	*OCENA ORYGINALNOŚCI I NIEZMIENNOŚCI*	*W: włączone do SR-4(3).*	
SA-12(11)	*TESTOWANIE PENETRACYJNE / ANALIZA ELEMENTÓW, PROCESÓW I WYKONAWCÓW*	*W: włączone do SR-6(1).*	
SA-12(12)	*UMOWY MIĘDZYORGANIZACYJNE*	*W: włączone do SR-8.*	
SA-12(13)	*KOMPONENTY KRYTYCZNE SYSTEMU INFORMATYCZNEGO*	*W: włączone do MA-6 i RA-9.*	
SA-12(14)	*IDENTYFIKACJA I ŚLEDZENIE*	*W: włączone do SR-4(1) i SR 4(2).*	
SA-12(15)	*MECHANIZMY ADRESOWANIA SŁABYCH STRON LUB WAD*	*W: włączone do SR-3.*	
SA-13	***WIARYGODNOŚĆ***	***W: włączone do SA-8.***	
SA-14	***ANALIZA KRYTYCZNOŚCI***	***W: włączone do RA-9.***	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SA-14(1)	*KRYTYCZNE KOMPONENTY POZBAWIONE ALTERNATYWNEGO ŹRÓDŁA ZAOPATRZENIA*	*W: włączone do SA-20.*	
SA-15	**PROCES ROZWOJU, STANDARDY I NARZĘDZIA**	O	V
SA-15(1)	METRYKI JAKOŚCI	O	V
SA-15(2)	NARZĘDZIA DO MONITOROWANIA BEZPIECZEŃSTWA I PRYWATNOŚCI	O	V
SA-15(3)	ANALIZA KRYTYCZNOŚCI	O	V
SA-15(4)	*MODELOWANIE ZAGROŻEŃ / ANALIZA PODATNOŚCI*	*W: włączone do SA-11(2).*	
SA-15(5)	OGRANICZANIE PŁASZCZYZNY ATAKU	O	V
SA-15(6)	CIĄGŁE DOSKONALENIE	O	V
SA-15(7)	ZAUTOMATYZOWANA ANALIZA PODATNOŚCI	O	V
SA-15(8)	PONOWNIE UŻYCIE INFORMACJI O ZAGROŻENIACH I PODATNOŚCI	O	V
SA-15(9)	*KREATYWNE WYKORZYSTANIE DANYCH*	*W: włączone do SA-3(2).*	
SA-15(10)	PLAN ODPOWIEDZI NA INCYDENT	O	V
SA-15(11)	ARCHIWIZACJA SYSTEMU LUB KOMPONENTU	O	V
SA-15(12)	MINIMALIZACJA INFORMACJI UMOŻLIWIAJĄCYCH IDENTYFIKACJĘ OSOBY	O	V
SA-16	**SZKOLENIA PROWADZONE PRZEZ DEWELOPERA**	O	V
SA-17	**ARCHITEKTURA ORAZ PROJEKT BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI DEWELOPERA**	O	V

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SA-17(1)	FORMALNY MODEL POLITYKI	O	V
SA-17(2)	BAZOWE ELEMENTY BEZPIECZEŃSTWA	O	V
SA-17(3)	FORMALNA SPECYFIKACJA	O	V
SA-17(4)	NIEFORMALNE SPECYFIKACJE	O	V
SA-17(5)	PROJEKT PROSTY KONCEPCYJNIE	O	V
SA-17(6)	STRUKTURA DO TESTOWANIA	O	V
SA-17(7)	STRUKTURA DLA NAJNIŻSZYCH UPRAWNIEŃ	O	V
SA-17(8)	ARANŻACJA (ORKIESTRACJA)	O	V
SA-17(9)	ROZPROSZENIE PROJEKTOWANIA	O	V
SA-18	***ODPORNOŚĆ NA SABOTAŻ I WYKRYWANIE MANIPULACJI***	***W: włączone do SR-9.***	
SA-18(1)	*WIELOFAZOWOŚĆ CYKLU ŻYCIA SYSTEMU*	*W: włączone do SR-9(1).*	
SA-18(2)	*KONTROLA SYSTEMÓW INFORMATYCZNYCH, KOMPONENTÓW LUB URZĄDZEŃ*	*W: włączone do SR-10.*	
SA-19	***AUTENTYCZNOŚĆ KOMPONENTÓW***	***W: włączone do SR-11.***	
SA-19(1)	*SZKOLENIE / ROZPOZNAWANIE AUTENTYCZNOŚCI*	*W: włączone do SR-11(1).*	
SA-19(2)	*KONTROLA KONFIGURACJI NA POTRZEBY SERWISOWANIA / NAPRAWY KOMPONENTÓW*	*W: włączone do SR-11(2).*	
SA-19(3)	*UTYLIZACJA KOMPONENTÓW*	*W: włączone do SR-12.*	
SA-19(4)	*SKANOWANIE AUTENTYCZNOŚCI*	*W: włączone do SR-10(3).*	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SA-20	**NIESTANDARDOWA (NA ZAMÓWIENIE) ROZBUDOWA KOMPONENTÓW KRYTYCZNYCH**	O	V
SA-21	**DOBÓR DEWELOPERÓW**	O	V
SA-21(1)	*OCENA PRZEGLĄDU*	*W: włączone do SA-21.*	
SA-22	**KOMPONENTY SYSTEMU BEZ WSPARCIA**	O	V
SA-22(1)	**ALTERNATYWNE ŹRÓDŁA STAŁEGO WSPARCIA**	*W: włączone do SA-22.*	
SA-23	**SPECJALIZACJA**	O	V

TABELA C-18 KATEGORIA SC – OCHRONA SYSTEMÓW I SIECI TELEKOMUNIKACYJNYCH

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SC-1	**POLITYKA I PROCEDURY**	O	V
SC-2	**ROZDZIELENIE FUNKCJONALNOŚCI SYSTEMU I UŻYTKOWNIKA**	S	V
SC-2(1)	INTERFEJSY DLA UŻYTKOWNIKÓW NIEUPRZYWILEJOWANYCH	S	V
SC-2(2)	NIEPOŁĄCZALNOŚĆ (DEZASOCJACJA)	S	V
SC-3	**IZOLACJA FUNKCJI BEZPIECZEŃSTWA**	S	V
SC-3(1)	SEPARACJA SPRZĘTOWA	S	V
SC-3(2)	FUNKCJE KONTROLI DOSTĘPU I PRZEPŁYWU	S	V
SC-3(3)	MINIMALIZACJA FUNKCJONALNOŚCI NIE ZWIĄZANYCH Z BEZPIECZEŃSTWEM	O/S	V
SC-3(4)	MODUŁ SPRZĘŻENIA I SPÓJNOŚCI	O/S	V
SC-3(5)	STRUKTURY WARSTWOWE	O/S	V
SC-4	**INFORMACJE NA WSPÓŁDZIELONYCH ZASOBACH SYSTEMOWYCH**	S	
SC-4(1)	*POZIOMY BEZPIECZEŃSTWA*	*W: włączone do SC-4.*	
SC-4(2)	PRZETWARZANIE WIELOPOZIOMOWE LUB OKRESOWE	S	
SC-5	**OCHRONA PRZED BLOKADĄ USŁUG (DoS)**	S	
SC-5(1)	OGRANICZENIE MOŻLIWOŚCI ATAKOWANIA INNYCH SYSTEMÓW	S	
SC-5(2)	PRZEPUSTOWOŚĆ, SZEROKOŚĆ PASMA I NADMIAROWOŚĆ	S	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SC-5(3)	WYKRYWANIE I MONITOROWANIE	S	
SC-6	**DOSTĘPNOŚĆ ZASOBÓW**	S	V
SC-7	**OCHRONA POŁĄCZEŃ BRZEGOWYCH**	S	
SC-7(1)	*FIZYCZNIE ODDZIELONE PODSIECI*	*W: WŁĄCZONE DO SC-7.*	
SC-7(2)	*DOSTĘP PUBLICZNY*	*W: WŁĄCZONE DO SC-7.*	
SC-7(3)	PUNKTY DOSTĘPOWE	S	
SC-7(4)	ZEWNĘTRZNE USŁUGI TELEKOMUNIKACYJNE	O	
SC-7(5)	ODRZUĆ DOMYŚLNIE / POZWÓL NA WYJĄTEK	S	
SC-7(6)	*ODPOWIEDŹ NA ROZPOZNANE AWARIE*	*W: WŁĄCZONE DO SC-7(18).*	
SC-7(7)	DZIELONE TUNELOWANIE URZĄDZEŃ ZDALNYCH	S	
SC-7(8)	RUCH TELEKOMUNIKACYJNY DO AUTORYZOWANYCH SERWERÓW PROXY	S	
SC-7(9)	OGRANICZENIE ZAGROŻEŃ WYJŚCIOWEGO RUCHU TELEKOMUNIKACYJNEGO	S	
SC-7(10)	ZAPOBIEGANIE EKSFILTRACJI	S	
SC-7(11)	OGRANICZENIE PRZYCHODZĄCEGO RUCHU KOMUNIKACYJNEGO	S	
SC-7(12)	SYSTEM OCHRONY KOMPUTERA GŁÓWNEGO TYPU HOST	S	
SC-7(13)	IZOLACJA NARZĘDZI BEZPIECZEŃSTWA / MECHANIZMÓW / KOMPONENTÓW WSPARCIA	S	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SC-7(14)	OCHRONA PRZED NIEAUTORYZOWANYMI POŁĄCZENIAMI FIZYCZNYMI	S	
SC-7(15)	SIECIOWY DOSTĘP UPRZYWILEJOWANY	S	
SC-7(16)	ZAPOBIEGANIE WYKRYWANIU KOMPONENTÓW SYSTEMU	S	
SC-7(17)	AUTOMATYCZNE EGZEKWOWANIE FORMATÓW PROTOKOŁU	S	
SC-7(18)	BŁĄD BEZPIECZEŃSTWA	S	V
SC-7(19)	BLOKOWANIE KOMUNIKACJI Z HOSTAMI SPOZA ORGANIZACJI	S	
SC-7(20)	DYNAMICZNA IZOLACJA I SEGREGACJA	S	
SC-7(21)	IZOLACJA ELEMENTÓW SYSTEMU	O/S	V
SC-7(22)	ODDZIELNE PODSIECI DO PODŁĄCZENIA DO RÓŻNYCH DOMEN BEZPIECZEŃSTWA	S	V
SC-7(23)	WYŁĄCZENIE INFORMACJI ZWROTNEJ NADAWCY W PRZYPADKU AWARII PROTOKOŁU UWIERZYTELNIAJĄCEGO	S	
SC-7(24)	DANE OSOBOWE	O/S	
SC-7(25)	BEZPIECZNE POŁĄCZENIA KRAJOWYCH SYSTEMÓW JAWNYCH	O	
SC-7(26)	BEZPIECZNE POŁĄCZENIA KRAJOWYCH SYSTEMÓW NIEJAWNYCH	O	
SC-7(27)	BEZPIECZNE POŁĄCZENIA TRANSGRANICZNYCH SYSTEMÓW JAWNYCH	O	
SC-7(28)	POŁĄCZENIA Z SIECIAMI PUBLICZNYMI	O	
SC-7(29)	SEPARACJA PODSIECI W CELU ODIZOLOWANIA FUNKCJI	S	
SC-8	**POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI**	S	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SC-8(1)	OCHRONA KRYPTOGRAFICZNA	S	
SC-8(2)	OBSŁUGA „PRZED" I „PO" TRANSMISJI	S	
SC-8(3)	OCHRONA KRYPTOGRAFICZNA ZEWNĘTRZNYCH KOMUNIKATÓW	S	
SC-8(4)	UKRYWANIE LUB RANDOMIZOWANIE KOMUNIKACJI	S	
SC-8(5)	CHRONIONY SYSTEM DYSTRYBUCJI	S	
SC-9	*POUFNOŚĆ TRANSMISJI*	*W: włączone do SC-8.*	
SC-10	**ZAKOŃCZENIE POŁĄCZENIA SIECIOWEGO**	S	
SC-11	**ZAUFANA ŚCIEŻKA KOMUNIKACYJNA**	S	V
SC-11(1)	NIEPODWAŻALNA ŚCIEŻKA KOMUNIKACYJNA	S	V
SC-12	**GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI**	O/S	
SC-12(1)	DOSTĘPNOŚĆ	O/S	
SC-12(2)	KLUCZE SYMETRYCZNE	O/S	
SC-12(3)	KLUCZE ASYMETRYCZNE	O/S	
SC-12(4)	*CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO*	*W: włączone do SC-12(3).*	
SC-12(5)	*CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO / TOKENY SPRZĘTOWE*	*W: włączone do SC-12(3).*	
SC-12(6)	FIZYCZNE ZABEZPIECZENIE KLUCZY KRYPTOGRAFICZNYCH	O/S	
SC-13	**OCHRONA KRYPTOGRAFICZNA**	S	
SC-13(1)	*KRYPTOGRAFIA KOMERCYJNA*	*W: włączone do SC-13.*	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SC-13(2)	*KRYPTOGRAFIA ZATWIERDZONA PRZEZ KRAJOWĄ WŁADZĘ BEZPIECZEŃSTWA*	*W: włączone do SC-13.*	
SC-13(3)	*OSOBY NIEPOSIADAJĄCE FORMALNYCH ZEZWOLEŃ NA DOSTĘP*	*W: włączone do SC-13.*	
SC-13(4)	*PODPISY CYFROWE*	*W: włączone do SC-13.*	
SC-14	***OCHRONA DOSTĘPU PUBLICZNEGO***	*W: włączone do AC-2, AC-3, AC-5, SI-3, SI-4, SI-5, SI-7, SI-10.*	
SC-15	**WSPÓŁPRACUJĄCE URZĄDZENIA I APLIKACJE**	S	
SC-15(1)	ODŁĄCZENIE FIZYCZNE LUB LOGICZNE	S	
SC-15(2)	*BLOKOWANIE RUCHU WEJŚCIOWEGO / WYJŚCIOWEGO*	*W: włączone do SC-7.*	
SC-15(3)	DEZAKTYWACJA / USUWANIE W CHRONIONYCH OBSZARACH PRACY	O	
SC-15(4)	WYRAŹNIE WYKAZANIE AKTUALNYCH UŻYTKOWNIKÓW	S	
SC-16	**TRANSMISJA ATRYBUTÓW BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI**	S	
SC-16(1)	WERYFIKACJA INTEGRALNOŚCI	S	
SC-16(2)	MECHANIZMY ANTYSPOOFINGOWE	S	
SC-16(3)	POWIĄZANIE KRYPTOGRAFICZNE	S	
SC-17	**CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO**	O/S	
SC-18	**KOD MOBILNY**	O	
SC-18(1)	IDENTYFIKACJA NIEDOPUSZCZALNEGO KODU / PODEJMOWANIE DZIAŁAŃ NAPRAWCZYCH	S	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SC-18(2)	NABYCIE / OPRACOWYWANIE / UŻYTKOWANIE	O	
SC-18(3)	ZAPOBIEGANIE POBIERANIU I WYKONYWANIU	S	
SC-18(4)	ZAPOBIEGANIE AUTOMATYCZNEMU WYKONANIU	S	
SC-18(5)	POZWALANIE NA WYKONANIE TYLKO W OGRANICZONYCH ŚRODOWISKACH	S	
SC-19	*PROTOKÓŁ TRANSMISJI PAKIETOWEJ (VOIP)*	***W: specyficzne dla danej technologii; uwzględnione w innych zabezpieczeniach protokołów.***	
SC-20	**BEZPIECZEŃSTWO NAZW DOMEN / ADRESÓW IP (AUTENTYCZNOŚĆ POCHODZENIA)**	S	
SC-20(1)	*STREFA PODRZĘDNA (PODPRZESTRZEŃ)*	*W: włączone do SC-20.*	
SC-20(2)	INTEGRALNOŚĆ DANYCH	S	
SC-21	**BEZPIECZEŃSTWO NAZW DOMEN / USŁUGA USTALANIA ADRESU IP**	S	
SC-21(1)	*INTEGRALNOŚĆ*	*W: włączone do SC-21.*	
SC-22	**ARCHITEKTURA NAZW DOMEN / ADRESÓW IP / ZAMAWIANIE USŁUGI DNS**	S	
SC-23	**AUTENTYCZNOŚĆ SESJI**	S	
SC-23(1)	UNIEWAŻNIENIE IDENTYFIKATORÓW SESJI PO WYLOGOWANIU	S	
SC-23(2)	*WYLOGOWANIE INICJOWANE PRZEZ UŻYTKOWNIKA / WYŚWIETLANIE WIADOMOŚCI*	W: włączone do AC-12(1).	
SC-23(3)	UNIKATOWE IDENTYFIKATORY SESJI GENEROWANE PRZEZ SYSTEM	S	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SC-23(4)	*LOSOWE UNIKALNE IDENTYFIKATORY SESJI*	W: włączone do SC-23(3).	
SC-23(5)	AUTORYZOWANE URZĘDY CERTYFIKACYJNE	S	
SC-24	**PRZEJŚCIE DO OKREŚLONEGO STANU SYSTEMU PO BŁĘDZIE**	S	V
SC-25	**THIN NODES / TERMINALOWE STACJE ROBOCZE**	S	
SC-26	**WABIKI**	S	
SC-26(1)	*WYKRYWANIE KODU ZŁOŚLIWEGO*	*W: włączone do SC-35.*	
SC-27	**WIELOPLATFORMOWOŚĆ APLIKACJI**	S	
SC-28	**OCHRONA DANYCH W SKŁADOWANIU / KOPIE KONFIGURACJI SYSTEMU**	S	
SC-28(1)	OCHRONA KRYPTOGRAFICZNA	S	
SC-28(2)	PRZECHOWYWANIE W TRYBIE OFF-LINE	O	
SC-28(3)	KLUCZE KRYPTOGRAFICZNE	O/S	
SC-29	**HETEROGENICZNOŚĆ SYSTEMU**	O	V
SC-29(1)	TECHNIKI WIRTUALIZACJI	O	V
SC-30	**MASKOWANIE I DEZINFORMACJA**	O	V
SC-30(1)	*TECHNIKI WIRTUALIZACJI*	*W: włączone do SC-29(1).*	
SC-30(2)	LOSOWOŚĆ	O	V
SC-30(3)	*ZMIANA LOKALIZACJI PRZETWARZANIA / PRZECHOWYWANIA*	O	V
SC-30(4)	INFORMACJE DEZINFORMUJĄCE	O	V

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SC-30(5)	UKRYWANIE KOMPONENTÓW SYSTEMU	O	V
SC-31	**ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI**	O	V
SC-31(1)	TESTOWANIE KANAŁÓW UKRYTYCH POD KĄTEM MOŻLIWOŚCI ICH WYKORZYSTANIA	O	V
SC-31(2)	MAKSYMALNA PRZEPUSTOWOŚĆ ŁĄCZA	O	V
SC-31(3)	POMIAR PRZEPUSTOWOŚCI W ŚRODOWISKU OPERACYJNYM	O	V
SC-32	**DZIELENIE SYSTEMU NA PARTYCJE**	O/S	V
SC-32(1)	FIZYCZNE WYDZIELONE DOMENY DLA FUNKCJI UPRZYWILEJOWANYCH	O/S	V
SC-33	***INTEGRALNOŚĆ TRANSMISJI***	*W: włączone do SC-8.*	
SC-34	**NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE**	S	V
SC-34(1)	NIEZAPISYWALNE PAMIĘCI	O	V
SC-34(2)	OCHRONA INTEGRALNOŚCI / NOŚNIKI TYLKO DO ODCZYTU	O	V
SC-34(3)	*OCHRONA SPRZĘTOWA*	*W: włączone do SC-51.*	
SC-35	**ZEWNĘTRZNA IDENTYFIKACJA ZŁOŚLIWEGO KODU**	S	
SC-36	**PRZETWARZANIE I PRZECHOWYWANIE ROZPROSZONE**	O	V
SC-36(1)	TECHNIKI PRZEGLĄDANIA CYKLICZNEGO	O	V
SC-36(2)	SYNCHRONIZACJA	O	V
SC-37	**KANAŁY POZAPASMOWE**	O	V

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SC-37(1)	GWARANTOWANA DOSTAWA / TRANSMISJA	O	V
SC-38	**BEZPIECZEŃSTWO OPERACJI**	O	V
SC-39	**IZOLACJA PROCESÓW**	S	V
SC-39(1)	SEPARACJA SPRZĘTOWA	S	V
SC-39(2)	ODDZIELNA DOMENA WYKONAWCZA DLA KAŻDEGO WĄTKU	S	V
SC-40	**OCHRONA ŁĄCZA BEZPRZEWODOWEGO**	S	
SC-40(1)	INTERFERENCJA ELEKTROMAGNETYCZNA	S	
SC-40(2)	REDUKCJA POTENCJALNEJ DETEKCJI	S	
SC-40(3)	NAŚLADOWCZE LUB MANIPULACYJNE OSZUSTWO TELEKOMUNIKACYJNE	S	
SC-40(4)	IDENTYFIKACJA PARAMETRÓW SYGNAŁU	S	
SC-41	**DOSTĘP DO PORTÓW I URZĄDZEŃ WEJŚCIA / WYJŚCIA**	O/S	
SC-42	**CZUJNIKI**	S	
SC-42(1)	RAPORTOWANIE DO UPOWAŻNIONYCH OSÓB LUB RÓL	O	
SC-42(2)	*AUTORYZOWANE UŻYCIE*	O	
SC-42(3)	*ZABRONIONE WYKORZYSTANIE URZĄDZEŃ*	*W: włączone do SC-42.*	
SC-42(4)	POWIADOMIENIE O ZBIERANIU DANYCH	O	
SC-42(5)	MINIMALIZACJA GROMADZENIA DANYCH	O	
SC-43	**OGRANICZENIA UŻYCIA**	O/S	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SC-44	**KOMORY DETONACYJNE**	S	
SC-45	**SYNCHRONIZACJA CZASU SYSTEMOWEGO**	S	
SC-45(1)	SYNCHRONIZACJA Z AUTORYZOWANYM ŹRÓDŁEM CZASU ODNIESIENIA	S	
SC-45(2)	WTÓRNE AUTORYTATYWNE ŹRÓDŁO CZASU	S	
SC-46	**EGZEKWOWANIE POLITYKI MIĘDZYDOMENOWEJ**	S	
SC-47	**ALTERNATYWNE ŚCIEŻKI KOMUNIKACYJNE**	O/S	
SC-48	**ROZMIESZCZENIE CZUJNIKÓW**	O/S	
SC-48(1)	DYNAMICZNE PRZEMIESZCZANIE CZUJNIKÓW LUB URZĄDZEŃ MONITORUJĄCYCH	O/S	
SC-49	**EGZEKWOWANIE SEPARACJI SPRZĘTOWEJ / POLITYKA EGZEKWOWANIA**	O/S	V
SC-50	**EGZEKWOWANIE SEPARACJI PROGRAMOWEJ / POLITYKA EGZEKWOWANIA**	O/S	V
SC-51	**OCHRONA SPRZĘTOWA**	O/S	V

TABELA C-19 KATEGORIA SI - INTEGRALNOŚCI SYSTEMU I INFORMACJI

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SI-1	**POLITYKA I PROCEDURY**	O	V
SI-2	**USUWANIE USTEREK**	O	
SI-2(1)	*ZARZĄDZANIE CENTRALNE*	W: włączone do PL-9.	
SI-2(2)	ZAUTOMATYZOWANE USUWANIE USTEREK	O	
SI-2(3)	CZAS DO USUNIĘCIA USTERKI / STANDARDY DZIAŁAŃ NAPRAWCZYCH	O	
SI-2(4)	AUTOMATYCZNE ŚCIEŻKI ZARZĄDZANIA NARZĘDZIAMI	O/S	
SI-2(5)	AUTOMATYCZNE AKTUALIZACJE APLIKACJI / OPROGRAMOWANIA UKŁADOWEGO	O/S	
SI-2(6)	USUWANIE POPRZEDNICH WERSJI APLIKACJI / OPROGRAMOWANIA UKŁADOWEGO	O/S	
SI-3	**ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM**	O/S	
SI-3(1)	*ZARZĄDZANIE CENTRALNE*	*W: włączone do PL-9.*	
SI-3(2)	*AUTOMATYCZNE AKTUALIZACJE*	*W: włączone do SI-3.*	
SI-3(3)	*NIEUPRZYWILEJOWANI UŻYTKOWNICY*	*W: włączone do AC-6(10).*	
SI-3(4)	AKTUALIZACJE WYŁĄCZNIE PRZEZ UPRAWNIONYCH UŻYTKOWNIKÓW	O/S	
SI-3(5)	*PRZENOŚNE URZĄDZENIA MAGAZYNUJĄCE*	*W: włączone do MP-7.*	
SI-3(6)	TESTOWANIE I WERYFIKACJA	O	
SI-3(7)	*WYKRYWANIE BEZSYGNATUROWE*	*W: włączone do SI-3.*	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SI-3(8)	WYKRYWANIE NIEAUTORYZOWANYCH KOMEND	S	
SI-3(9)	*ZDALNE POLECENIA AUTENTYFIKACYJNE*	*W: włączone do AC-17(10).*	
SI-3(10)	ANALIZA KODU ZŁOŚLIWEGO	O	
SI-4	**MONITOROWANIE SYSTEMU**	O/S	V
SI-4(1)	SYSTEM WYKRYWANIA WŁAMAŃ I NAPADÓW W CAŁYM SYSTEMIE	O/S	V
SI-4(2)	AUTOMATYCZNE NARZĘDZIA I MECHANIZMY ANALIZY W CZASIE RZECZYWISTYM	S	V
SI-4(3)	AUTOMATYCZNA INTEGRACJA NARZĘDZI I MECHANIZMÓW	S	V
SI-4(4)	WEJŚCIOWY / WYJŚCIOWY RUCH TELEKOMUNIKACYJNY	S	V
SI-4(5)	ALERTY SYSTEMOWE	S	V
SI-4(6)	*OGRANICZANIE NIEUPRZYWILEJOWANYCH UŻYTKOWNIKÓW*	*W: włączone do AC-6(10).*	
SI-4(7)	AUTOMATYCZNA ODPOWIEDŹ NA PODEJRZANE ZDARZENIA	S	V
SI-4(8)	*OCHRONA INFORMACJI MONITORUJĄCYCH*	*W: włączone do SI-4.*	
SI-4(9)	TESTOWANIE NARZĘDZI I MECHANIZMÓW MONITORUJĄCYCH	O	V
SI-4(10)	INSPEKCJA ZASZYFROWANYCH KOMUNIKATÓW	O	V
SI-4(11)	ANALIZA ANOMALII RUCHU TELEKOMUNIKACYJNEGO	O/S	V
SI-4(12)	AUTOMATYCZNE ALERTY GENEROWANE PRZEZ ORGANIZACJĘ	O/S	V
SI-4(13)	ANALIZA MODELU RUCHU / ZDARZEŃ TELEKOMUNIKACYJNYCH	O/S	V
SI-4(14)	WYKRYWANIE ATAKÓW BEZPRZEWODOWYCH	S	V

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SI-4(15)	TELEKOMUNIKACJA BEZPRZEWODOWA / PRZEWODOWA	S	V
SI-4(16)	KORELOWANIE INFORMACJI MONITORUJĄCYCH	O/S	V
SI-4(17)	ZINTEGROWANA ŚWIADOMOŚĆ SYTUACYJNA	O	V
SI-4(18)	ANALIZA RUCHU / ZAPOBIEGANIE EKSFILTRACJI	O/S	V
SI-4(19)	RYZYKO ZE STRONY OSÓB	O	V
SI-4(20)	UPRZYWILEJOWANI UŻYTKOWNICY	S	V
SI-4(21)	OKRESY PRÓBNE	O	V
SI-4(22)	NIEAUTORYZOWANE USŁUGI SIECIOWE	S	V
SI-4(23)	KOMPUTER GŁÓWNY (HOST)	O	V
SI-4(24)	WSKAŹNIKI RYZYKA	S	V
SI-4(25)	ANALIZY OPTYMALIZACJI RUCHU SIECIOWEGO	S	V
SI-5	**ALERTY BEZPIECZEŃSTWA, PORADY I DYREKTYWY**	O	V
SI-5(1)	AUTOMATYCZNE ALERTY I PORADY	O	V
SI-6	**WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI**	S	V
SI-6(1)	*POWIADOMIENIE O NIEUDANYCH TESTACH BEZPIECZEŃSTWA*	*W: włączone do SI-6.*	
SI-6(2)	WSPARCIE AUTOMATYZACYJNE BADAŃ ROZPROSZONYCH	S	
SI-6(3)	RAPORTZ WYNIKÓW WERYFIKACJI	O	
SI-7	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI**	O/S	V

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SI-7(1)	KONTROLE INTEGRALNOŚCI	S	V
SI-7(2)	AUTOMATYCZNE POWIADOMIENIA O NARUSZENIACH INTEGRALNOŚCI	S	V
SI-7(3)	NARZĘDZIA DO CENTRALNEGO ZARZĄDZANIA INTEGRALNOŚCIĄ	O	V
SI-7(4)	*OCHRONA PRZED NARUSZENIAMI*	W: włączone do SR-9.	
SI-7(5)	AUTOMATYCZNA ODPOWIEDŹ NA NARUSZENIA INTEGRALNOŚCI	S	V
SI-7(6)	OCHRONA KRYPTOGRAFICZNA	S	V
SI-7(7)	INTEGRACJA WYKRYWANIA I ODPOWIEDZI	O	V
SI-7(8)	ZDOLNOŚĆ AUDYTU ISTOTNYCH ZDARZEŃ	S	V
SI-7(9)	WERYFIKACJA PROCESU URUCHAMIANIA	S	V
SI-7(10)	OCHRONA URUCHAMIANIA OPROGRAMOWANIA UKŁADOWEGO	S	V
SI-7(11)	*ZAMKNIĘTE ŚRODOWISKO Z OGRANICZONYMI UPRAWNIENIAMI*	*W: włączone do CM-7(6).*	
SI-7(12)	WERYFIKACJA INTEGRALNOŚCI	O/S	V
SI-7(13)	*WYKONANIE KODU W ŚRODOWISKACH CHRONIONYCH*	*W: włączone do CM-7(7).*	
SI-7(14)	*KOD WYKONYWALNY BINARNY LUB MASZYNOWY*	*W: włączone do CM-7(8).*	
SI-7(15)	AUTORYZACJA KODU	S	V
SI-7(16)	LIMIT CZASU NA WYKONANIE PROCESU BEZ NADZORU	O	V
SI-7(17)	SAMOOCHRONA APLIKACJI ŚRODOWISKA WYKONAWCZEGO	O/S	V

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SI-8	**OCHRONA PRZED SPAMEM**	O	
SI-8(1)	*ZARZĄDZANIE CENTRALNE*	*W: włączone do PL-9.*	
SI-8(2)	AUTOMATYCZNE AKTUALIZACJE	S	
SI-8(3)	CIĄGŁA ZDOLNOŚĆ DO NAUKI	S	
SI-9	*OGRANICZENIA WPROWADZANIA INFORMACJI*	*W: włączone do AC-2, AC-3, AC-5, AC-6.*	
SI-10	**WERYFIKACJA WPROWADZANYCH INFORMACJI**	S	V
SI-10(1)	RĘCZNE ZASTĘPOWANIE	O/S	V
SI-10(2)	PRZEGLĄD / USUWANIE BŁĘDÓW	O	V
SI-10(3)	PRZEWIDYWALNE ZACHOWANIE	O/S	V
SI-10(4)	INTERAKCJE CZASOWE	S	V
SI-10(5)	OGRANICZANIE DANYCH WEJŚCIOWYCH DO ZAUFANYCH ŹRÓDEŁ I ZATWIERDZONYCH FORMATÓW	S	V
SI-10(6)	ZAPOBIEGANIE WSTRZYKIWANIU NIEZAUFANYCH DANYCH	S	V
SI-11	**OBSŁUGA BŁĘDÓW**	S	
SI-12	**ZARZĄDZANIE I RETENCJA DANYCH**	O	
SI-12(1)	OGRANICZANIE ELEMENTÓW DANYCH OSOBOWYCH	O	
SI-12(2)	MINIMALIZOWANIE WYKORZYSTYWANIA DANYCH OSOBOWYCH PODCZAS TESTÓW, SZKOLEŃ I BADAŃ	O	
SI-12(3)	USUWANIE INFORMACJI	O	
SI-13	**PRZEWIDYWANIE AWARII**	O	V

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SI-13(1)	PRZENIESIENIE ODPOWIEDZIALNOŚCI KOMPONENTÓW	O	V
SI-13(2)	*LIMIT CZASU NA WYKONANIE PROCESU BEZ NADZORU*	*W: włączone do SI-7(16).*	
SI-13(3)	RĘCZNY TRANSFER MIĘDZY SKŁADNIKAMI	O	V
SI-13(4)	INSTALACJA KOMPONENTÓW Z LISTY REZERWOWEJ / POWIADOMIENIE	O/S	V
SI-13(5)	PRZEŁĄCZANIE AWARYJNE	O	V
SI-14	**ZAPOBIEGANIE ZAAWANSOWANYM DŁUGOTRWAŁYM ATAKOM TYPU APT)**	O	V
SI-14(1)	ODŚWIEŻANIE Z ZAUFANYCH ŹRÓDEŁ	O	V
SI-14(2)	ZMIENNOŚĆ INFORMACJI	O	V
SI-14(3)	ZMIENNOŚĆ POŁĄCZEŃ	O	V
SI-15	**FILTROWANIE INFORMACJI WYJŚCIOWYCH**	S	V
SI-16	**OCHRONA PAMIĘCI**	S	V
SI-17	**PROCEDURY TESTOWANIA AWARYJNEGO „FAIL-SAFE”**	S	V
SI-18	**OPERACJE SPRAWDZAJĄCE JAKOŚĆ DANYCH OSOBOWYCH**	O/S	
SI-18(1)	AUTOMATYZACJA WSPARCIA	O/S	
SI-18(2)	ZNACZNIKI DANYCH	O/S	
SI-18(3)	ZBIERANIE DANYCH	O/S	
SI-18(4)	ZGŁOSZENIA USUNIĘCIA DANYCH	O/S	

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SI-18(5)	ZAWIADOMIENIE O KOREKCIE LUB USUNIĘCIU	O/S	
SI-19	**DE-IDENTYFIKACJA**	O/S	
SI-19(1)	ZBIERANIE DANYCH	O/S	
SI-19(2)	ARCHIWIZACJA DANYCH	O/S	
SI-19(3)	UJAWNIANIE DANYCH	O/S	
SI-19(4)	USUWANIE, MASKOWANIE, SZYFROWANIE, HASZOWANIE LUB WYMIANA IDENTYFIKATORÓW BEZPOŚREDNICH	S	
SI-19(5)	ZABEZPIECZENIE UJAWNIANIA DANYCH STATYSTYCZNYCH	O/S	
SI-19(6)	ZRÓŻNICOWANA PRYWATNOŚĆ	O/S	
SI-19(7)	ZATWIERDZONE ALGORYTMY I OPROGRAMOWANIE	O	
SI-19(8)	ZMOTYWOWANY INTRUZ	O/S	
SI-20	**SKAŻENIE**	O/S	V
SI-21	**ODŚWIEŻANIE INFORMACJI**	O/S	V
SI-22	**RÓŻNICOWANIE INFORMACJI**	O/S	V
SI-23	**FRAGMENTACJA INFORMACJI**	O/S	V

TABELA C-20 KATEGORIA SR - ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SR-1	**POLITYKA I PROCEDURY**	O	V
SR-2	**PLAN ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW**	O	V
SR-2(1)	POWOŁANIE ZESPOŁU ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW	O	V
SR-3	**ZABEZPIECZENIA I PROCESY W ŁAŃCUCHU DOSTAW**	O/S	V
SR-3(1)	ZRÓŻNICOWANA BAZA DOSTAW	O	V
SR-3(2)	OGRANICZANIE SZKODY	O	V
SR-3(3)	PODWYKONAWCY	O	V
SR-4	**POCHODZENIE**	O	V
SR-4(1)	TOŻSAMOŚĆ	O	V
SR-4(2)	ŚLEDZENIE PRZESYŁEK	O	V
SR-4(3)	POTWIERDZANIE AUTENTYCZNOŚCI I NIEZMIENNOŚCI	O	V
SR-4(4)	INTEGRALNOŚĆ ŁAŃCUCHA DOSTAW - POCHODZENIE	O	V
SR-5	**STRATEGIE, NARZĘDZIA I METODY NABYCIA**	O	V
SR-5(1)	ODPOWIEDNIE ZAOPATRZENIE	O	V
SR-5(2)	OCENY PRZED WYBOREM, AKCEPTACJĄ, MODYFIKACJĄ LUB AKTUALIZACJĄ	O	V
SR-6	**OCENY I RECENZJE DOSTAWCÓW**	O	V

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	WDROŻONE PRZEZ	WIARYGODNOŚĆ
SR-6(1)	BADANIA I ANALIZA	O	V
SR-7	**BEZPIECZEŃSTWO OPERACJI W RAMACH ŁAŃCUCHA DOSTAW**	O	V
SR-8	**UMOWY DOTYCZĄCE POWIADOMIEŃ**	O	V
SR-9	**ODPORNOŚĆ NA MANIPULACJE I WYKRYWANIE SABOTAŻU**	O	V
SR-9(1)	WIELOETAPOWY CYKL ŻYCIA SYSTEMU	O	V
SR-10	**KONTROLA SYSTEMÓW / KOMPONENTÓW**	O	V
SR-11	**AUTENTYCZNOŚĆ KOMPONENTU**	O	V
SR-11(1)	SZKOLENIE Z ZAKRESU ZAPOBIEGANIA FAŁSZERSTWOM	O	V
SR-11(2)	ZABEZPIECZENIE KONFIGURACJI SERWISOWANYCH I NAPRAWIANYCH KOMPONENTÓW	O	V
SR-11(3)	SKANOWANIE ANTYFAŁSZERSKIE	O	V
SR-12	**USUWANIE KOMPONENTÓW**	O	V