Kancelaria Prezesa
Rady Ministrów

NARODOWY STANDARD CYBERBEZPIECZEŃSTWA
NSC 800-53A wer. 1.0

21 grudnia 2022

Ocenianie środków bezpieczeństwa i ochrony prywatności w systemach informacyjnych oraz organizacjach

Tworzenie skutecznych planów oceny

Publikacja dostępna pod adresem:

Narodowe Standardy Cyberbezpieczeństwa

PREAMBUŁA

Szanowni Państwo,

oddajemy w Państwa ręce zestaw publikacji specjalnych - Narodowe Standardy Cyberbezpieczeństwa, o których mowa w interwencji 2.1 celu szczegółowego 2 Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024, Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń. Standardy zostały opracowane na podstawie publikacji amerykańskiego National Institute of Science and Technology (NIST) i posiadają mapowanie na obowiązujące w polskim systemie prawnym Polskie Normy, na których oparte jest zarządzanie bezpieczeństwem informacji w podmiotach krajowego systemu cyberbezpieczeństwa.

Standardy stanowią przewodniki metodyczne, które ułatwiają zbudowanie efektywnego systemu zarządzania bezpieczeństwem informacji w oparciu o praktykę stosowaną w tym zakresie w administracji federalnej USA.

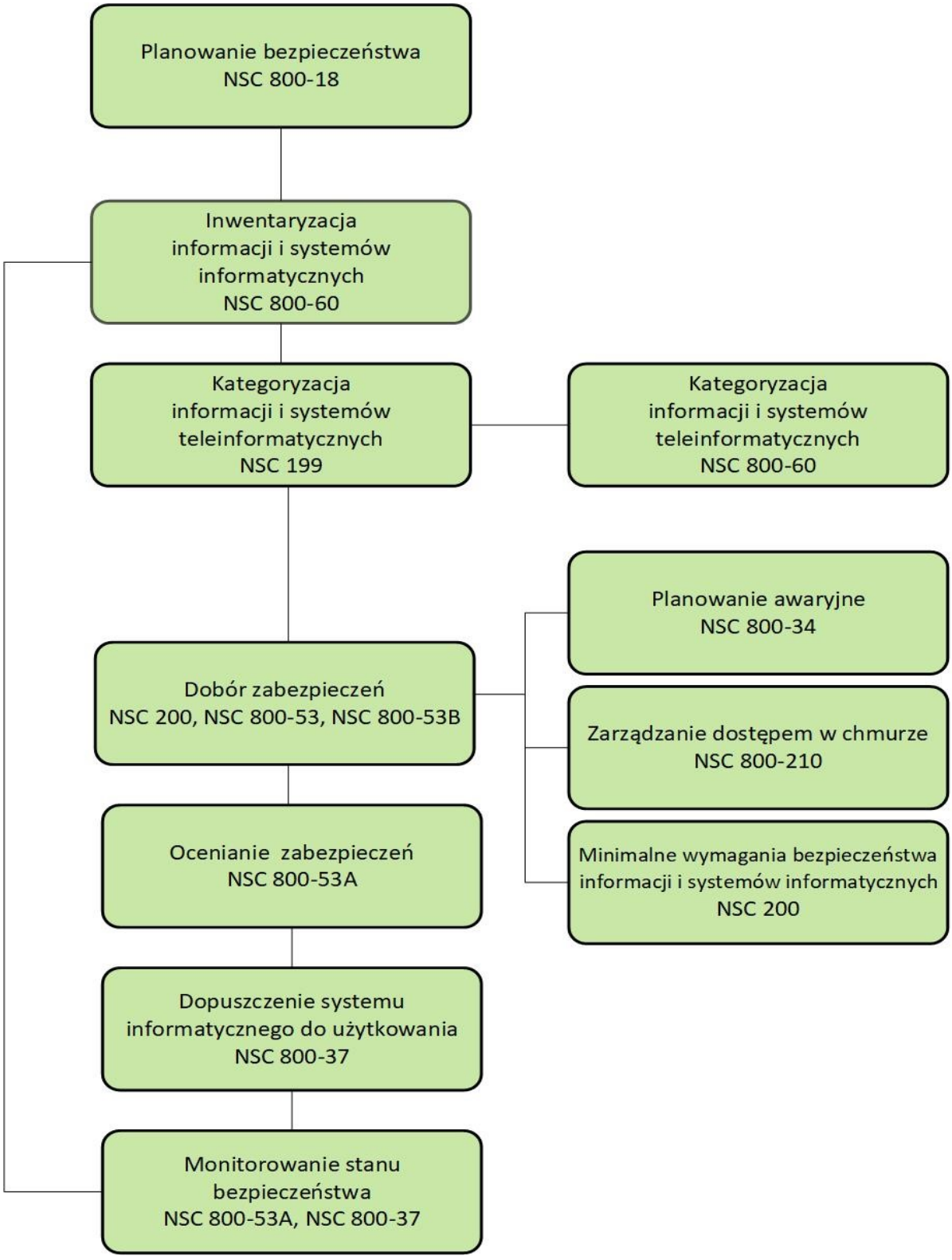
Zestaw publikacji specjalnych obejmuje następujące pozycje:

- *NSC 199, Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199.*
- *NSC 200, Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych – na podstawie FIPS 200.*
- *NSC 800-18, Przewodnik do opracowywania planów bezpieczeństwa systemów informacyjnych 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 informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu – na podstawie NIST SP 800-37.*

- *NSC 800-39, Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego – na podstawie NIST SP 800-39.*
- *NSC 800-53, Zabezpieczenia i ochrona prywatności w systemach informacyjnych oraz organizacjach – na podstawie NIST SP 800-53.*
- *NSC 800-53A, Ocenianie środków bezpieczeństwa i ochrony prywatności w systemach informacyjnych oraz organizacjach. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A.*
- *NSC 800-53B, Zabezpieczenia bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B.*
- *NSC 800-60, Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informacyjnego – 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.*

W oparciu o te publikacje można stosunkowo łatwo zbudować system zarządzania bezpieczeństwem informacji i sprawować nad nim niezbędną kontrolę.

Cykl zarządzania bezpieczeństwem informacji bazujący na publikacjach NIST wykorzystuje następujące dokumenty:



Cykl zarządzania bezpieczeństwem informacji

WSPÓLNE FUNDAMENTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

National Institute of Standards and Technology (NIST) opracował szereg standardów i wytycznych w celu zapewnienia jednolitego podejścia do problematyki bezpieczeństwa informacji i systemów informacyjnych administracji federalnej USA. Podstawową rolę w podejściu do zagadnień związanych z zapewnieniem bezpieczeństwa informacji i systemów informacyjnych oraz ochrony prywatności odgrywa elastyczny i spójny sposób zarządzania ryzykiem związanym z bezpieczeństwem i prywatnością działalności i majątku organizacji, osób fizycznych 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. Dzięki jednolitemu podejściu do zarządzania ryzykiem ułatwia także wymianę informacji i współpracę pomiędzy różnymi podmiotami.

NIST kontynuuje współpracę z sektorem publicznym i prywatnym w celu stworzenia map i relacji pomiędzy opracowanymi przez siebie standardami i wytycznymi, a tymi, które zostały opracowane przez inne organizacje (m. in. ISO[1]), 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 dopuszczone do użytku poza administracją federalną USA. Charakteryzują się pragmatycznym podejściem do zagadnień związanych z bezpieczeństwem informacji i systemów informacyjnych oraz ochrony prywatności, przez co ułatwiają podmiotom opracowanie i eksploatację systemu zarządzania tym bezpieczeństwem.

1 International Organization for Standardization (ISO) - Międzynarodowa Organizacja Normalizacyjna– organizacja pozarządowa zrzeszająca krajowe organizacje normalizacyjne.

Biorąc pod uwagę wszystkie powyższe aspekty, autorzy niniejszej publikacji polecają opracowania NIST, jako godne zaufania i rekomendują stosowanie ich przez polskie podmioty przy 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. Celem ich wskazania nie jest nakłanianie do korzystania z ww. podmiotów, urządzeń lub materiałów lub ich poparcie. Wskazanie ich nie ma również na celu sugerowania, że te podmioty, materiały lub sprzęt są najlepsze z dostępnych w danej dziedzinie.

W niniejszej publikacji mogą znajdować się odniesienia do innych opracowywanych przez nas publikacji. Informacje tu zawarte, 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 powinny obowiązywać dotychczasowe wymagania, wytyczne i procedury, jeśli takie istnieją. W ramach planowanych przez Państwa prac zalecamy śledzenie naszych prac publikacyjnych.

Aktualne informacje o prowadzonych przez nas pracach dostępne są pod adresem:

 Narodowe Standardy Cyberbezpieczeństwa

Jesteśmy również otwarci na wszelkie Państwa sugestie, które pomogą nam w dalszych pracach nad standardami cyberbezpieczeństwa i zachęcamy do kontaktu.

 +48222455922

 sekretariat.dc@mc.gov.pl

Niniejsza publikacja NSC 800-53A, ***Ocenianie środków bezpieczeństwa i ochrony prywatności w systemach informacyjnych oraz organizacjach. Tworzenie skutecznych planów oceny***, opracowana została za zgodą National Institute of Science and Technology (NIST) na podstawie specjalnej publikacji NIST SP 800-53A, Rev. 4., *Assessing Security and Privacy Controls in Federal Information Systems and Organizations. Building Effective Assessment Plans.*

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 występujące w publikacji zdefiniowane są w dokumencie NSC 7298, Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa.

Spis treści

Spis ilustracji

Spis tabel

PRZEDMOWA

Ocena środków bezpieczeństwa i ochrony prywatności nie opisuje pozycji list kontrolnych, prostych wyników pozytywny / negatywny, czy też generowania dokumentacji przeprowadzenia kontroli lub audytów, gdyż takie oceny są głównym narzędziem używanym do weryfikacji wdrożonych środków bezpieczeństwa i ochrony prywatności spełniających swoje określone cele i funkcje.

Standard NSC 800-53A został opracowany w celu ułatwienia oceny środków bezpieczeństwa i ochrony prywatności przeprowadzanych w ramach skutecznego zarządzania ryzykiem. Wyniki oceny tych środków dostarczają organizacjom:

- *dowody na skuteczność wdrożonych zabezpieczeń;*
- *ocenę jakości procesów zarządzania ryzykiem stosowanych w organizacji;*
- *informacji o mocnych i słabych stronach systemów informacyjnych, które wspierają misje organizacyjne i funkcje biznesowe w globalnym środowisku zaawansowanych i zmieniających się zagrożeń.*

Wyniki opracowane przez oceniającego (*ang. assessor*)[2] są wykorzystywane do określenia ogólnej skuteczności środków bezpieczeństwa i ochrony prywatności związanych z systemami informacyjnymi (w tym wspólnych, hybrydowych i specyficznych zabezpieczeń dla danego systemu) oraz ich środowiskach działania, a także w celu zapewnienia wiarygodnych i konstruktywnych wkładów w proces zarządzania ryzykiem w organizacji.

Poprawnie wykonana ocena: (I) pomaga określić zgodność zabezpieczeń wdrożonych w organizacyjnych systemach informacyjnych i środowiskach, z zabezpieczeniami zawartymi w planach bezpieczeństwa i planach ochrony prywatności organizacji; oraz

[2] Patrz: NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*. Dotyczy terminologii angielskiej i akronimów zawartych w całym dokumencie.

(II) ułatwia ekonomiczne podejście do korygowania niedociągnięć lub braków w systemach w sposób uporządkowany i metodyczny, zgodnie z misją organizacyjną / potrzebami biznesowymi.

NSC 800-53A wer. 1 jest publikacją wspierającą standard NSC 800-53 wer. 1[3,4]. Każda z tych publikacji zawiera wskazówki dotyczące wdrażania konkretnych kroków w ramach zarządzania ryzykiem (RMF)[5] zawartych w standardzie NSC 800-37[6]. NSC 800-53 obejmuje Krok 2 RMF zawarty w standardzie NSC 800-37. Wybór środków bezpieczeństwa i ochrony prywatności (tj. określenie, jakie zabezpieczenia są potrzebne do zarządzania ryzykiem odnoszącym się do operacji organizacyjnych i aktywów, osób fizycznych, oraz organizacji). NSC 800-53A obejmuje Krok 4 RMF, *Ocena* oraz Krok 6 RMF, *Monitor*owanie. Zawiera wskazówki dotyczące oceny bezpieczeństwa i procesów oceny prywatności. Niniejsze wskazówki obejmują sposób tworzenia skutecznych planów oceny oraz analizowanie wyników oceny i zarządzanie nimi.

NSC 800-53A umożliwia organizacjom dostosowywanie do swoich potrzeb, oraz stosownie podstawowych procedur oceny bezpieczeństwa. Pojęcia dostosowywania, użyte w tym dokumencie, są podobne do pojęć opisanych w publikacji specjalnej NSC 800-53 wer. 1. Dostosowanie polega na spersonalizowaniu procedur oceny w celu osiągnięcia dokładniejszej zgodności z charakterystyką systemu informacyjnego i jego środowiska działania. Proces dostosowywania daje organizacjom elastyczność niezbędną do unikania metod oceny, które są złożone lub kosztowne i stosowanie

[3] NSC 800-53 wer. 1 – Narodowy Standard Cyberbezpieczeństwa zawierający zasady stosowania zabezpieczeń w systemach informacyjnych podmiotów publicznych, opublikowany jako Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO) wer. 1.

[4] Ilekroć w dokumencie tym mowa jest o NSC 800-53 wer. 1, dotyczy to publikacji SCCO wer. 1.

[5] Terminologia pojęć i akronimy zawarte są w Załączniku B oraz C publikacji NSC 800-53A.

[6] NSC 800-37 - Narodowy Standard Cyberbezpieczeństwa zawierający wytyczne dotyczące zarządzania ryzykiem w systemach informacyjnych podmiotów publicznych.

metod spełniających wymogi oceny ustanowione poprzez zastosowanie podstawowych pojęć w RMF.

Dostosowywanie może również obejmować dodawanie procedur oceny lub szczegółów oceny w celu odpowiedniego zaspokojenia potrzeb organizacji w zakresie zarządzania ryzykiem (np. dodanie do wybranych zabezpieczeń informacji specyficznych dla systemu/platformy). Decyzje dotyczące dostosowywania są pozostawione w gestii organizacji w celu maksymalizacji elastyczności w opracowywaniu planów oceny — stosowania wyników ocen ryzyka w celu określenia zasięgu, rygoru i poziomu intensywności ocen. Chociaż elastyczność nadal jest ważnym czynnikiem przy opracowywaniu planów oceny bezpieczeństwa i planów oceny prywatności, ważnym czynnikiem jest również spójność ocen. Głównym celem NSC 800-53A jest zapewnienie ram oceny i wstępnego punktu wyjścia dla procedur oceny, które są niezbędne do osiągnięcia takiej spójności.

Amerykańska agencja NIST zainicjowała projekt Automatycznego Protokołu Zabezpieczeń Zawartości (*ang. Security Content Automation Protocol - SCAP*)[7], który wspiera podejście do osiągania spójnych, opłacalnych ocen środków bezpieczeństwa. Głównym celem SCAP jest standaryzacja formatu i nomenklatury używanej do przekazywania informacji o konfiguracjach i wadach zabezpieczeń. Ta standaryzacja umożliwia automatyczną ocenę konfiguracji systemu, ocenę luk w zabezpieczeniach, sprawdzanie poprawek, a także agregację raportów i interoperacyjność między produktami zabezpieczającymi obsługującymi protokół SCAP. W rezultacie SCAP umożliwia organizacjom identyfikowanie i zmniejszanie luk związanych z produktami, które nie są załatane lub są niezabezpieczone. SCAP zawiera również specyfikację listy kontrolnej otwartego języka interaktywnego (*ang. Open Checklist Interactive Language -*

[7] Publikacja specjalna NIST SP 800-126 zawiera wytyczne dotyczące specyfikacji technicznej SCAP. Dodatkowe informacje na temat inicjatywy SCAP, a także ogólnie dostępne dane referencyjne SCAP można znaleźć na stronie http://nvd.nist.gov.

OCIL)[8], która umożliwia wyrażenie deklaracji określanych w procedurach oceny bezpieczeństwa zawartych w Załączniku F tej publikacji, w ramach podstawowych zasadach, które ustanowią interoperacyjność z narzędziami obsługującymi SCAP. Oceny ochrony prywatności są omówione oddzielnie w Załączniku J niniejszego standardu NSC 800-53A.

[8] OCIL - podstawowe zasady określające zabezpieczenia, które nie mogą być oceniane bez niektórych interakcji międzyludzkich lub informacji zwrotnych. Służą do określenia stanu systemu, przedstawiając jeden lub więcej kwestionariuszy przeznaczonych dla użytkowników. Język zawiera konstrukcje pytań, instrukcje dotyczące kierowania użytkowników w kierunku udzielanych odpowiedzi, odpowiedzi na pytania, artefakty i wyniki oceny.

ROZDZIAŁ 1 - WPROWADZENIE

KONIECZNOŚĆ OCENY SKUTECZNOŚCI ŚRODKÓW BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Współczesne systemy informacyjne to złożone zespoły technologiczne (tj. sprzętu, aplikacji i oprogramowania układowego), procesów i ludzi, współpracujących ze sobą w celu zapewnienia organizacjom możliwości przetwarzania, przechowywania i przekazywania informacji w odpowiednim czasie w zakresie wspierania różnych misji i funkcji biznesowych. Stopień, w jakim organizacje uzależniły się od systemów informacyjnych w zakresie realizacji rutynowych, ważnych i krytycznych misji i funkcji biznesowych, oznacza, że bezpieczeństwo podstawowych systemów i środowisk działania ma zasadnicze znaczenie dla sukcesu działania organizacji. Wybór odpowiednich środków bezpieczeństwa i ochrony prywatności w eksploatowanym systemie informacyjnym jest ważnym procesem, który może mieć istotny wpływ na operacje i aktywa organizacji, jak również na poziom funkcjonowania jednostek . Środki bezpieczeństwa i ochrony prywatności są zabezpieczeniami lub środkami zaradczymi zalecanymi dla systemu informacyjnego lub organizacji, mającymi na celu ochronę poufności, integralności i dostępności przetwarzanych informacji.Po zaimplementowaniu w ramach systemu informacyjnego, środki bezpieczeństwa i ochrony prywatności są oceniane w celu dostarczenia informacji niezbędnych do określenia ich ogólnej skuteczności, to jest zasięgu, w jakim zabezpieczenia są wykonywane prawidłowo, działają zgodnie z przeznaczeniem i przynoszą pożądany rezultat w odniesieniu do spełnienia wymogów bezpieczeństwa i ochrony prywatności w systemie i organizacji. Zrozumienie ogólnej skuteczności wdrożonych środków bezpieczeństwa i ochrony prywatności jest niezbędne do określenia ryzyka operacji i aktywów organizacji, osób fizycznych, innych organizacji i dla Państwa, wynikającego z przetwarzania informacji w systemie.

1.1. CEL I MOŻLIWOŚĆ ZASTOSOWANIA

Celem niniejszego standardu jest przedstawienie: (I) wytycznych dotyczących tworzenia skutecznych planów oceny bezpieczeństwa i planów oceny prywatności; oraz (II) kompleksowego zestawu procedur oceny skuteczności środków bezpieczeństwa i ochrony prywatności stosowanych w systemach informacyjnych i organizacjach wspierających podmioty publiczne. Wytyczne te mają zastosowanie do środków bezpieczeństwa i ochrony prywatności określonych w standardzie NSC 800-53 wer. 1. i zostały opracowane w celu zapewnienia pomocy w osiąganiu jak najwyższego bezpieczeństwa systemów informacyjnych podmiotów publicznych, poprzez:

- *umożliwienie bardziej spójnej, porównywalnej i powtarzalnej oceny środków bezpieczeństwa i ochrony prywatności z powtarzalnymi wynikami;*
- *promowanie lepszego zrozumienia zagrożeń odnoszących się do operacji organizacyjnych, majątku organizacyjnego, osób, innych organizacji i Państwa, wynikających z działania i korzystania z systemów informacyjnych;*
- *ułatwianie bardziej opłacalnych ocen środków bezpieczeństwa i ochrony prywatności, przyczyniających się do ustalenia ogólnej skuteczności zabezpieczeń; oraz*
- *tworzenie pełniejszych, bardziej wiarygodnych i rzetelnych informacji dla personelu organizacji, w celu wspierania decyzji dotyczących zarządzania ryzykiem, wzajemności wyników oceny[9], udostępniania informacji oraz zgodności ustawami, rozporządzeniami, dyrektywami, przepisami i politykami.*

Wytyczne dotyczące bezpieczeństwa zawarte w niniejszym standardzie mają zastosowanie do systemów informacyjnych podmiotów publicznych. Zostały opracowane zasadniczo z technicznego punktu widzenia, w celu uzupełnienia stosowanych wytycznych dotyczących organizacyjnych systemów bezpieczeństwa

[9] Patrz: Załącznik F

i mogą być wykorzystywane w odniesieniu do takich systemów za zgodą upoważnionego personelu odpowiedzialnego za bezpieczeństwo tych systemów. Wytyczne zawarte w Załączniku J mogą mieć szersze zastosowanie, w zależności od wytycznych organizacyjnych i misji. Zachęca się organizacje sektora prywatnego do rozważenia wykorzystania tych wytycznych w stosownych przypadkach[10].

W celu opracowania wykonywalnych planów oceny w zakresie tworzenia i kompilacji informacji niezbędnych do określenia skuteczności środków bezpieczeństwa i ochrony prywatności stosowanych w systemie informacyjnym i organizacji, podmioty powinny korzystać z tej publikacji w połączeniu z zatwierdzonymi planami bezpieczeństwa i ochrony prywatności. Niniejsza publikacja została opracowana z myślą o umożliwieniu organizacjom dostosowania podstawowych procedur oceny. Procedury oceny są wykorzystywane, jako punkt wyjścia i wkład do planu oceny. Opracowując skuteczne plany oceny bezpieczeństwa i plany oceny prywatności, organizacje biorą pod uwagę istniejące (dostępne) informacje o zabezpieczeniach, które mają być ocenione (np. wyniki oceny ryzyka organizacji specyficzne dla danej platformy w zależności od sprzętu, aplikacji lub oprogramowania układowego oraz wszelkie procedury oceny zabezpieczeń specyficznych dla organizacji, które nie są zawarte w standardzie NSC 800-53 wer. 1)[11].

---

[10] Zgodnie z postanowieniami polityki bezpieczeństwa, gdy połączenie systemów informacyjnych podmiotów publicznych z systemami informacyjnymi zarządzanymi przez podmioty podległe, prywatne, wykonawców lub beneficjentów wiąże się z przetwarzaniem, przechowywaniem lub przekazywaniem informacji publicznych, zastosowanie mają standardy i wytyczne dotyczące bezpieczeństwa informacji opisane w niniejszej publikacji. Szczególne wymogi bezpieczeństwa informacji oraz zasady i warunki wzajemnych połączeń systemów są zawarte w protokołach uzgodnień (*ang. Memeorandum of Understending - MoU*) i umowach o bezpiecznych połączeniach sieci (*ang. Interconnection Security Agreement - ISA)* ustanowionych przez uczestniczące organizacje.

[11] Na przykład może zaistnieć potrzeba opracowania szczegółowych skryptów testowych dla konkretnego systemu operacyjnego, komponentu sieciowego, oprogramowania pośredniczącego lub aplikacji wykorzystywanej w systemie informacyjnym, aby odpowiednio ocenić pewne cechy charakterystyczne dla danego systemu bezpieczeństwa lub zabezpieczeń prywatności. Takie skrypty testowe są na niższym poziomie szczegółowości niż procedury oceny zawarte w Załącznikach F i J, a zatem wykraczają poza zakres niniejszej publikacji. Dodatkowe szczegółowe informacje dotyczące oceny znajdują się, jako uzupełnienie, w procesach oceny bezpieczeństwa opisanych w Załączniku H.

Wybór odpowiednich procedur oceny oraz rygor, intensywność i zakres oceny zależą od trzech czynników:

- *kategoryzacji bezpieczeństwa systemu informacyjnego*[12]*;*
- *wymagań dotyczących wiarygodności, które organizacja zamierza spełnić przy określaniu ogólnej skuteczności środków bezpieczeństwa i ochrony prywatności; oraz*
- *środków bezpieczeństwa i ochrony prywatności, określonych w zatwierdzonym planie bezpieczeństwa i planie ochrony prywatności*[13].

Proces oceny jest czynnością polegającą na gromadzeniu informacji, a nie działalnością związaną z bezpieczeństwem lub ochroną prywatności. Organizacje określają najbardziej efektywną kosztowo implementację tego kluczowego elementu w programach bezpieczeństwa i ochrony prywatności informacji w organizacji, stosując wyniki oceny ryzyka, biorąc pod uwagę wiarygodność i poziom jakości procesów zarządzania ryzykiem w organizacji oraz wykorzystując elastyczność koncepcji opisanych w niniejszej publikacji. Wykorzystanie NSC 800-53A, jako punktu wyjścia w procesie definiowania procedur oceny środków bezpieczeństwa i ochrony prywatności w systemach i organizacjach informatycznych, promuje spójny poziom bezpieczeństwa i prywatności oraz oferuje niezbędną elastyczność w dostosowywaniu oceny do potrzeb klienta w oparciu o politykę i wymagania organizacji, znane informacje o zagrożeniach i podatnościach, względy operacyjne, zależności systemu i platformy informatycznej oraz tolerancję ryzyka[14]. Informacje wytworzone podczas oceny zabezpieczeń mogą być wykorzystane przez organizację do:

[12] Kategoryzacja bezpieczeństwa jest dokonywana zgodnie ze standardami NSC 199 oraz NSC 800-60.

[13] Środki bezpieczeństwa i ochrony prywatności dotyczące systemu informacyjnego i organizacji są dokumentowane w planach bezpieczeństwa i planach ochrony prywatności po wstępnym wyborze i dostosowaniu zabezpieczeń zgodnie ze standardem NSC 800-53 wer. 1.

[14] W niniejszej publikacji termin "ryzyko" oznacza ryzyko dla działań organizacyjnych (tj. misji, funkcji, wizerunku i reputacji), majątku organizacji, osób, innych organizacji i społeczeństwa.

- *identyfikacji potencjalnych problemów lub braków we wdrażaniu przez organizację ram zarządzania ryzykiem (ang. Risk Frame Management - RFM);*
- *określania słabych punktów i niedociągnięć związanych z bezpieczeństwem i ochroną prywatności w systemie informacyjnym oraz w środowisku, system działa;*
- *priorytetowego traktowania decyzji ograniczających ryzyko i związanych z nimi działaniami w zakresie ograniczania ryzyka;*
- *potwierdzenia, że zidentyfikowane niedociągnięcia w zakresie bezpieczeństwa i ochrony prywatności oraz braki w systemie informacyjnym i środowisku pracy zostały usunięte;*
- *wspierania działań monitorujących oraz podnoszących świadomość sytuacji w zakresie bezpieczeństwa informacji i ochrony prywatności;*
- *wspomagania w podejmowaniu decyzji dotyczących bezpieczeństwa autoryzacji, decyzji dotyczących autoryzacji w zakresie ochrony prywatności oraz bieżących decyzji dotyczących autoryzacji; oraz*
- *informowania o decyzjach budżetowych i procesie inwestycji kapitałowych.*

Nie oczekuje się od organizacji stosowania wszystkich metod oceny i obiektów oceny zawartych w procedurach oceny określonych w niniejszej publikacji w odniesieniu do związanych z nimi środków bezpieczeństwa i ochrony prywatności stosowanych w systemach informacyjnych organizacji lub przez niedziedziczonych. Organizacje mają nieodzowną elastyczność w określaniu poziomu niezbędnego wysiłku i wiarygodności wymaganych do przeprowadzenia danej oceny (np. jakie metody i obiekty oceny są uznawane za najbardziej przydatne w uzyskaniu pożądanych wyników). Ustalenia dokonuje się na podstawie tego, co pozwoli na osiągnięcie celów oceny w sposób najbardziej efektywny kosztowo i na tyle pewny, że będzie to pomocne w późniejszym określeniu wynikającej z tego misji lub ryzyka biznesowego. Organizacje powinny zrównoważyć zasoby wydatkowane na wdrożenie środków bezpieczeństwa i ochrony prywatności (tj. zabezpieczeń i środków zaradczych wdrożonych na rzecz

bezpieczeństwa i ochrony prywatności) z zasobami ponoszonymi na określenie ogólnej skuteczności zabezpieczeń, zarówno na początku wdrożenia, jak i na bieżąco podczas eksploatacji, poprzez stosowanie programów ciągłości monitorowania.

1.2. GRUPA DOCELOWA

Niniejsza publikacja ma służyć różnorodnej grupie profesjonalistów zajmujących się systemami informacyjnymi, bezpieczeństwem informacji i ochroną prywatności, w tym:

- *osobom odpowiedzialnym za rozwój systemów informacyjnych (np. kierownicy programów, projektanci i programiści systemów, integratorzy systemów, inżynierowie bezpieczeństwa informacji);*
- *osobom odpowiedzialnym za ocenę i monitorowanie bezpieczeństwa informacji (np. osoby sprawdzające system, osoby oceniające, niezależni weryfikatorzy/ walidatorzy, audytorzy, analitycy, właściciele systemów informacyjnych, dostawcy zabezpieczeń wspólnych);*
- *osobom mającym obowiązki związane z systemem informacyjnym, bezpieczeństwem, prywatnością i zarządzaniem ryzykiem oraz nadzorem (np. AO, CIO, SISO[15], SAOP/CPO, menadżer systemów informacyjnych, menadżer ds. bezpieczeństwa informacji); oraz*
- *osobom mającym obowiązki związane z wdrażaniem bezpieczeństwa informacji oraz obowiązki operacyjne (np. właściciel systemu informacyjnego, dostawca usług wspólnych, właściciel informacji/władający informacją, właściciel misji/przedsiębiorstwa, administrator systemu, ISSO).*

1.3. POWIĄZANE PUBLIKACJE I PROCESY OCENY

Publikacja NSC 800-53A ma na celu wsparcie standardu NSC 800-37. W szczególności procedury oceny zawarte w tej publikacji oraz wytyczne dotyczące opracowywania

[15] Stanowisko znane jest także, jako senior agency information security officer - SAISO lub chief information security officer - CISO.

planów oceny bezpieczeństwa i ochrony prywatności w systemach informacyjnych i organizacji, bezpośrednio wspierają działania w zakresie oceny i monitorowania, które są integralną częścią procesu zarządzania ryzykiem. Obejmuje to dostarczanie w czasie niemal rzeczywistym informacji związanych z bezpieczeństwem i prywatnością personelowi organizacyjnemu na temat bieżącego stanu bezpieczeństwa i prywatności w systemach i organizacji.

Zachęca się organizacje, aby w miarę możliwości korzystały z wyników oceny i związanej z nią dokumentacji oceny oraz dostępnych dowodów dotyczących elementów systemu informacyjnego pochodzących z poprzednich ocen, w tym niezależnych testów, oceny i weryfikacji przeprowadzonych przez strony trzecie[16]. Testy, ocena i weryfikacja wyrobów może być przeprowadzana z wykorzystaniem modułów kryptograficznych i produktów informatycznych ogólnego przeznaczenia, takich jak systemy operacyjne, systemy baz danych, zapory sieciowe, urządzenia do wykrywania włamań, przeglądarki internetowe, aplikacje internetowe, karty inteligentne, urządzenia biometryczne, urządzenia do weryfikacji tożsamości osobistej, urządzenia sieciowe i platformy sprzętowe, z wykorzystaniem norm krajowych i międzynarodowych. Jeżeli w standardzie NSC 800-53 wer. 1 produkt stanowiący element systemu informacyjnego zostanie określony, jako zapewniający wsparcie dla wdrożenia określonego środka bezpieczeństwa lub ochrony prywatności, wówczas w zakresie, w jakim ma to zastosowanie, wykorzystuje się świadectwa uzyskane w trakcie procesów testowania, oceny i weryfikacji produktu (np. specyfikacje

[16] Wyniki oceny można uzyskać na podstawie wielu działań, które występują rutynowo w trakcie cyklu życia systemu. Na przykład, wyniki oceny są tworzone podczas testowania i oceny nowych komponentów systemu informacyjnego podczas aktualizacji systemu lub działań związanych z integracją systemu. Organizacje mogą korzystać z wcześniejszych wyników oceny, gdy tylko jest to możliwe, w celu zmniejszenia ogólnych kosztów oceny i uczynienia procesu oceny bardziej efektywnym.

bezpieczeństwa, analizy i wyniki testów, sprawozdania z weryfikacji i certyfikaty weryfikacji)[17].

Świadectwa te można połączyć z dowodami związanymi z oceną uzyskanymi w wyniku zastosowania procedur oceny zawartych w niniejszej publikacji, tak, aby efektywnie przedstawić informacje niezbędne do ustalenia, czy środki bezpieczeństwa i ochrony prywatności są skuteczne w ich stosowaniu.

1.4. STRUKTURA DOKUMENTU

Pozostała część tej publikacji jest zorganizowana w następujący sposób:

- *Rozdział drugi opisuje podstawowe pojęcia związane z oceną środków bezpieczeństwa i ochrony prywatności, w tym: (I) włączenie ocen do cyklu życia systemu; (II) znaczenie ogólnoorganizacyjnej strategii przeprowadzania ocen środków bezpieczeństwa i ochrony prywatności; (III) opracowanie skutecznych wyników wiarygodności, które pomogą zwiększyć podstawy zaufania do efektywności ocenianych środków bezpieczeństwa i ochrony prywatności; oraz (IV) format i treść procedur oceny.*
- *Rozdział trzeci opisuje proces oceny środków bezpieczeństwa i ochrony prywatności w systemach informacyjnych organizacji i ich środowiskach działania, w tym: (I) działania prowadzone przez organizacje i osoby oceniające w celu przygotowania ocen środków bezpieczeństwa i ochrony prywatności; (II) opracowywanie planów oceny bezpieczeństwa; (III) przeprowadzanie ocen środków bezpieczeństwa i ochrony*

[17] Organizacje dokonują przeglądu dostępnych informacji o komponentach produktów informatycznych w celu określenia: (I) jakie zabezpieczenia w zakresie bezpieczeństwa i ochrony prywatności są stosowane przez produkt; (II) czy te środki bezpieczeństwa spełniają zamierzone wymogi zabezpieczeń ocenianego systemu informacyjnego; (III) czy konfiguracja produktu i środowisko, w którym produkt działa, są zgodne ze środowiskiem i konfiguracją produktu podanego przez sprzedawcę i/lub dewelopera; oraz (IV) czy wymogi wiarygodności określone w specyfikacji producenta/sprzedawcy spełniają wymogi w zakresie wiarygodności oceny tych środków bezpieczeństwa. Spełnienie powyższych kryteriów stanowi racjonalne uzasadnienie tego, że produkt jest odpowiedni i spełnia zamierzone wymogi środków bezpieczeństwa i ochrony prywatności ocenianego systemu informacyjnego.

prywatności oraz analizę, dokumentowanie i zgłaszanie wyników oceny; oraz (IV) analizę sprawozdania z oceny i działania następcze prowadzone przez organizacje.

Załączniki uzupełniające zawierają szczegółowe informacje dotyczące oceny, w tym: (I) referencje; (II) słownik; (III) akronimy; (IV) opis metod oceny środków bezpieczeństwa; (V) wskazówki dotyczące testów penetracyjnych; (VI) katalog procedur oceny środków bezpieczeństwa, które można wykorzystać do opracowania planów oceny zabezpieczeń; (VII) treść sprawozdań z oceny bezpieczeństwa; (VIII) definicje, format i wykorzystanie procesów oceny bezpieczeństwa; (IX) wsparcie automatyzacji bieżących ocen; oraz (X) katalog procedur oceny, które można wykorzystać do opracowania planów oceny środków bezpieczeństwa w zakresie ochrony prywatności.

ROZDZIAŁ 2 - PODSTAWY

PODSTAWOWE POJĘCIA ZWIĄZANE Z OCENIANIEM ŚRODKÓW BEZPIECZEŃSTWA

W niniejszym rozdziale opisano podstawowe pojęcia związane z oceną środków bezpieczeństwa i ochrony prywatności w systemach informacyjnych organizacji oraz w środowiskach, w których systemy te działają, w tym: (I) włączenie ocen do cyklu życia systemu; (II) znaczenie ogólnoorganizacyjnej strategii przeprowadzania ocen środków bezpieczeństwa i ochrony prywatności; (III) opracowanie skutecznych wyników wiarygodności, które pomogą zwiększyć podstawy zaufania do efektywności ocenianych środków bezpieczeństwa i ochrony prywatności; oraz (IV) format i treść procedur oceny.

Podczas, gdy elastyczność jest nadal ważnym czynnikiem w opracowywaniu planów oceny, ciągłość oceny jest również kluczowym argumentem. Podstawowym celem standardu NSC 800-53A jest zapewnienie ram oceny i punktu wyjścia dla procedur oceny, które są niezbędne do osiągnięcia takiej spójności.

2.1. OCENY W RAMACH CYKLU ŻYCIA SYSTEMU (SDLC)

Oceny bezpieczeństwa i prywatności mogą być skutecznie przeprowadzane w różnych etapach cyklu życia systemu[18] w celu zwiększenia pewności, że środki bezpieczeństwa i ochrony prywatności stosowane w ramach systemu informacyjnego lub dziedziczone po nim są skuteczne w ich stosowaniu. Niniejsza publikacja zawiera kompleksowy zestaw procedur oceny wspierających działania w zakresie oceny bezpieczeństwa i ochrony prywatności w całym cyklu życia systemu (*ang. system development life cycle - SDLC*). Na przykład, ocena bezpieczeństwa jest rutynowo przeprowadzana przez twórców systemów i integratorów systemów w fazach opracowywania/nabywania

[18] Zazwyczaj istnieje pięć faz w ogólnym cyklu życia systemu: (I) inicjacja; (II) rozwój/nabycie; (III) wdrożenie; (IV) eksploatacja i utrzymanie; oraz (V) rozdysponowanie (usuwanie). Publikacja NIST SP 800-64 zawiera wytyczne dotyczące kwestii bezpieczeństwa w cyklu życia systemu.

i wdrażania systemu w cyklu życia. Oceny prywatności są przeprowadzane przez SAOP oraz personel ochrony prywatności również we wczesnych fazach cyklu życia systemu. Pomaga to zapewnić, że wymagane środki bezpieczeństwa i ochrony prywatności w systemie są odpowiednio zaprojektowane i opracowane, prawidłowo wdrożone i zgodne z ustaloną architekturą bezpieczeństwa informacji organizacyjnych, zanim system wejdzie w fazę eksploatacji i utrzymania. Ocena bezpieczeństwa w początkowych fazach cyklu życia systemu obejmuje np. przegląd projektu i kodu, skanowanie aplikacji i testowanie regresyjne. Oceny ochrony prywatności obejmują przeglądy mające na celu zapewnienie przestrzegania obowiązujących przepisów i polityk w zakresie ochrony prywatności oraz uwzględnienie ochrony prywatności w projektowaniu systemu. Słabe punkty i niedociągnięcia związane z bezpieczeństwem i ochroną prywatności, zidentyfikowane na wczesnym etapie cyklu życia systemu, mogą być rozwiązane szybciej i w znacznie bardziej ekonomiczny sposób przed przejściem do kolejnych faz cyklu życia. Celem oceny jest określenie środków bezpieczeństwa i ochrony prywatności we wczesnym etapie cyklu życia systemu, aby zapewnić, że projekt i testy systemu zapewniają wdrożenie tych zabezpieczeń. Procedury oceny opisane w załącznikach F oraz J wspierają oceny przeprowadzane w początkowych etapach cyklu życia systemu.

Ocenę bezpieczeństwa i ochrony prywatności przeprowadza się również w fazie eksploatacji i konserwacji w cyklu życia systemu, aby zapewnić, że środki bezpieczeństwa i ochrony prywatności będą nadal skuteczne w środowisku operacyjnym i będą mogły chronić przed stale zmieniającymi się zagrożeniami. Ocenę bezpieczeństwa przeprowadzają zazwyczaj właściciele systemów informacyjnych, dostawcy zabezpieczeń wspólnych, ISSO, niezależni oceniający i audytorzy. Ocena prywatności jest zazwyczaj przeprowadzana przez SAOP/CPO. Na przykład, organizacje oceniają podczas wstępnej autoryzacji bezpieczeństwa, wszystkie środki bezpieczeństwa i ochrony prywatności stosowane w systemie informacyjnym i odziedziczone przez ten system. Po wstępnej autoryzacji, organizacja na bieżąco ocenia wszystkie wdrożone środki bezpieczeństwa, zgodnie ze strategią

monitorowania ciągłości bezpieczeństwa informacji[19]. Ochrona prywatności jest również na bieżąco oceniana w celu zapewnienia zgodności z obowiązującymi przepisami i politykami w zakresie ochrony prywatności. Do bieżącej oceny i monitorowania środków bezpieczeństwa i ochrony prywatności wykorzystuje się procedury oceny określone w niniejszej publikacji. Częstotliwość takich ocen i monitorowania jest określana przez organizację i/lub właściciela systemu informacyjnego lub dostawcę zabezpieczeń wspólnych i zatwierdzana przez osobę zatwierdzającą. Wreszcie, na koniec cyklu życia, ocena bezpieczeństwa jest przeprowadzana w celu zapewnienia, że ważne informacje organizacyjne są usuwane z systemu informacyjnego przed jego wycofaniem z życia. Ocenę prywatności przeprowadza się również w celu zapewnienia zgodności z harmonogramami przechowywania informacji w organizacji.

2.2. STRATEGIA PRZEPROWADZANIA OCENY ZABEZPIECZEŃ

Zachęca się organizacje do opracowania szeroko zakrojonej, obejmującej całą organizację strategii przeprowadzania ocen bezpieczeństwa i ochrony prywatności, ułatwiającej bardziej opłacalne i spójne oceny we wszystkich systemach informacyjnych, w których przetwarzane są informacje organizacji.

W skali całej organizacji, strategia rozpoczyna się od zastosowania wstępnych etapów ram zarządzania ryzykiem (RFM) do wszystkich systemów informacyjnych w organizacji, z organizacyjnym spojrzeniem na proces kategoryzacji bezpieczeństwa oraz proces selekcji środków bezpieczeństwa i ochrony prywatności (w tym identyfikacji zabezpieczeń wspólnych).

Kategoryzacja systemów informacyjnych, jako działalność obejmująca całą organizację, uwzględniająca nie tylko krytyczność i wrażliwość informacji, ale także architekturę korporacyjną oraz architekturę bezpieczeństwa informacji, pomaga zapewnić, że

[19] Publikacje NSC 800-37 oraz NIST SP 800-137 zawierają wytyczne dotyczące stałego monitorowania środków bezpieczeństwa.

poszczególne systemy są kategoryzowane w oparciu o misje i cele biznesowe organizacji[20].

Maksymalizacja liczby zabezpieczeń wspólnych stosowanych w organizacji: (I) znacznie obniża koszty opracowania, wdrożenia i oceny środków bezpieczeństwa i ochrony prywatności; (II) umożliwia organizacjom centralizację i automatyzację oceny zabezpieczeń oraz amortyzację kosztów tych oszacowań we wszystkich systemach informacyjnych w całej organizacji; oraz (III) zwiększa spójność środków bezpieczeństwa i ochrony prywatności.

Wszechstronne podejście organizacji do określenia zabezpieczeń wspólnych we wczesnym etapie stosowania RMF, ułatwia bardziej globalną strategię oceny tych zabezpieczeń i dzielenia się podstawowymi wynikami oceny z właścicielami systemów informacyjnych i upoważnionym personelem.

Dzielenie się wynikami oceny pomiędzy kluczowym, upoważnionym personelem organizacji, przynosi wiele istotnych korzyści, w tym:

- *zapewnienie zdolności przeglądu wyników oceny wszystkich systemów informacyjnych oraz podejmowania decyzji związanych z misją/biznesem w zakresie działań ograniczających ryzyko zgodnie z priorytetami organizacyjnymi, kategoryzacją bezpieczeństwa systemów informacyjnych oraz oceną ryzyka;*
- *zapewnienie bardziej globalnego spojrzenia na systemowe słabości i luki występujące w systemach informacyjnych w całej organizacji oraz zdolności opracowywania kompleksowych rozwiązań problemów związanych z bezpieczeństwem informacji i ochroną prywatnością; oraz*

[20] Ochrona prywatności jest określana i wdrażana niezależnie od kategoryzacji bezpieczeństwa systemu informacyjnego.

- *zwiększanie bazy wiedzy organizacji na temat zagrożeń, słabych punktów i strategii w zakresie bardziej efektywnych kosztowo rozwiązań związanych ze wspólnymi problemami w zakresie bezpieczeństwa informacji i ochrony prywatności.*

Organizacje mogą również promować bardziej szczegółowy i efektywny kosztowo proces oceny, poprzez: (I) opracowanie bardziej szczegółowych procedur oceny dostosowanych do konkretnych środowisk działania i wymagań (zamiast przypisywania tych zadań do każdej osoby oceniającej zabezpieczenia lub zespołu oceniającego); oraz (II) dostarczanie narzędzi, szablonów i technik w celu wsparcia bardziej spójnych ocen w całej organizacji.[21]

Przeprowadzanie oceny środków bezpieczeństwa jest podstawowym obowiązkiem właścicieli systemów informacyjnych i dostawców zabezpieczeń wspólnych, nad którymi nadzór sprawuje upoważniony personel. Przeprowadzanie oceny ochrony prywatności jest podstawowym obowiązkiem SAOP/CPO oraz personelu odpowiedzialnego za prywatność. W proces oceny zaangażowane są również w znacznym stopniu inne strony w organizacji, które mają nabyte prawo do wyników oceny. Inne zainteresowane strony to na przykład właściciele misji/biznesu, właściciele informacji/zwierzchnicy (gdy te role są wypełniane przez kogoś innego niż właściciel systemu informacyjnego), wyznaczony personel ds. bezpieczeństwa informacji oraz ochrony prywatności. Konieczne jest, aby właściciele systemów informacyjnych i dostawcy zabezpieczeń wspólnych koordynowali swoje działania w organizacji z innymi stronami zainteresowanymi oceną zabezpieczeń, aby pomóc w zapewnieniu,

[21] Organizacje mogą również dostarczać plany oceny bezpieczeństwa zawierające dostosowane do potrzeb procedury oceny zewnętrznym dostawcom usług, którzy obsługują systemy informacyjne w imieniu tych organizacji. Ponadto plany te mogą rekomendować pomocnicze szablony, narzędzia i techniki, a także mogą być dalej dostosowywane do umowy z dostawcą usług, co pomaga zwiększyć spójność ocen i zmaksymalizować ponowne wykorzystanie artefaktów związanych z oceną. Takie ponowne wykorzystanie może poprawić bezpieczeństwo dzięki jednolitości i ograniczyć / usunąć niejednoznaczność umów, co skutkuje zmniejszeniem kosztów i ryzyka dla organizacji.

że podstawowe misje i funkcje biznesowe organizacji są odpowiednio uwzględnione w wyborze środków bezpieczeństwa i ochrony prywatności, które mają być ocenione.

OSTRZEŻENIE

Przy ocenie środków bezpieczeństwa i ochrony prywatności w systemach operacyjnych organizacje powinny dokładnie rozważyć potencjalne skutki stosowania procedur oceny określonych w niniejszej publikacji. Niektóre procedury oceny, w szczególności te, które mają bezpośredni wpływ na działanie lub funkcję sprzętu, aplikacji lub oprogramowania układowego systemu informacyjnego, mogą niezamierzenie wpłynąć na rutynowe przetwarzanie, przekazywanie lub przechowywanie informacji wspierających misje lub funkcje biznesowe organizacji. Na przykład, krytyczny komponent systemu informacyjnego może zostać wyłączony z eksploatacji w celu przeprowadzenia oceny lub komponent może ulec awarii lub uszkodzeniu w trakcie procesu oceny. Organizacje powinny również podjąć niezbędne środki ostrożności, aby zapewnić, że misje organizacyjne i funkcje biznesowe są nadal wspierane przez systemy informacyjne oraz, że wszelkie potencjalne skutki odnoszące się do efektywności operacyjnej, wynikające z działań oceniających, zostały rozważone z wyprzedzeniem.

2.3. BUDOWANIE SKUTECZNEGO PROCESU OCENY BEZPIECZEŃSTWA

Budowanie skutecznego poświadczenia wiarygodności dotyczącego skuteczności środków bezpieczeństwa i ochrony prywatności jest procesem, który obejmuje: (I) zebranie dowodów z różnych działań prowadzonych w trakcie cyklu życia systemu poświadczających, że zabezpieczenia stosowane w systemie informacyjnym są wdrażane prawidłowo, działają zgodnie z założeniami i dają pożądany rezultat w odniesieniu do spełniania wymogów bezpieczeństwa i prywatności w systemie i organizacji; oraz (II) przedstawienie tych dowodów w sposób, który decydenci są w stanie skutecznie wykorzystać przy podejmowaniu opartych na ryzyku decyzji dotyczących działania lub korzystania z systemu. Świadectwa opisane powyżej pochodzą z wdrożenia środków bezpieczeństwa i ochrony prywatności w systemie

informacyjnym i odziedziczonych przez system (tj. zabezpieczeń wspólnych) oraz z oceny tego wdrożenia. Najlepiej byłoby, gdyby osoba oceniająca opierała się na wcześniej opracowanych materiałach, rozpoczynających się od określenia potrzeb organizacji w zakresie bezpieczeństwa i prywatności informacji i były dalej rozwijane podczas projektowania, rozwoju i wdrażania systemu informacyjnego. Materiały te, opracowane w trakcie wdrażania środków bezpieczeństwa i ochrony prywatności w całym cyklu życia systemu informacyjnego, stanowią wstępne świadectwo (dowód) dla przypadku wiarygodności.

Oceniający uzyskują wymagane dowody podczas procesu oceny, aby umożliwić upoważnionemu personelowi dokonanie obiektywnych ustaleń, co do skuteczności środków bezpieczeństwa i ochrony prywatności oraz ogólnego stanu bezpieczeństwa i prywatności w systemie informacyjnym. Dowody oceny niezbędne do dokonania takich ustaleń można uzyskać z różnych źródeł, w tym na przykład z ocen produktów i systemów informacyjnych, a w przypadku ocen prywatności, z dokumentacji dotyczącej zgodności z zasadami ochrony prywatności (np. ocena wpływu na prywatność). Oceny produktów (zwane również testowaniem, szacowaniem i weryfikacją produktów) są zazwyczaj przeprowadzane przez niezależne, zewnętrzne organizacje testujące. Przeprowadzane oceny badają funkcje produktów w zakresie bezpieczeństwa i prywatności oraz ustalone ustawienia konfiguracyjne. Oceny mogą być przeprowadzane w celu wykazania zgodności z branżowymi, krajowymi lub międzynarodowymi standardami bezpieczeństwa informacji, standardami ochrony prywatności zawartymi w obowiązujących przepisach i politykach oraz oświadczeniach deweloperów/sprzedawców. Ponieważ wiele produktów informatycznych jest ocenianych przez komercyjne organizacje testujące, a następnie wdrażanych w szeregu systemów informacyjnych, tego typu oceny mogą być przeprowadzane na większym poziomie szczegółowości i zapewniać głębszy wgląd w bezpieczeństwo i zdolności ochrony prywatności poszczególnych produktów.

Oceny systemów są zazwyczaj przeprowadzane przez deweloperów systemów informacyjnych, integratorów systemów, właścicieli systemów informacyjnych,

dostawców zabezpieczeń wspólnych, biegłych, audytorów, oraz personel organizacji zajmujący się bezpieczeństwem informacji i ochroną prywatności. Oceniający lub zespoły oceniające zbierają dostępne informacje o systemie informacyjnym, takie jak wyniki oceny poszczególnych komponentów produktu, jeśli są dostępne, i przeprowadzają dodatkowe oceny na poziomie systemu przy użyciu różnych metod i technik. Oceny systemu są wykorzystywane do kompilacji i weryfikacji dowodów potrzebnych upoważnionemu personelowi do określenia, jak skuteczne są środki bezpieczeństwa i ochrony prywatności stosowane w systemie informacyjnym w ograniczaniu ryzyka dla operacji i aktywów organizacji, dla osób fizycznych, innych organizacji i społeczeństwa. Wyniki ocen przeprowadzonych z wykorzystaniem procedur oceny specyficznych dla danego systemu informacyjnego i organizacji, zaczerpnięte z wytycznych zawartych w niniejszej publikacji, przyczyniają się do zebrania niezbędnych dowodów w celu określenia skuteczności środków bezpieczeństwa i ochrony prywatności zgodnie z wymaganiami w zakresie zapewnienia zaufania, udokumentowanymi w planach bezpieczeństwa i prywatności.

2.4. PROCEDURY OCENY

Procedura oceny składa się z zestawu celów oceny, z których każdy zawiera powiązany zestaw potencjalnych metod oceny i obiektów oceny. Cel oceny obejmuje zestaw instrukcji, odnoszących się do konkretnego ocenianego środka bezpieczeństwa lub ochrony prywatności. Zestawy instrukcji są powiązane z treścią zabezpieczeń lub ochrony prywatności (tj. z funkcjonalnością środków bezpieczeństwa/prywatności), aby zapewnić identyfikowalność wyników oceny w odniesieniu do podstawowych wymogów zabezpieczeń. Zastosowanie procedury oceny środków bezpieczeństwa lub ochrony prywatności prowadzi do uzyskania wyników oceny. Ustalenia te odzwierciedlają lub są następnie wykorzystywane w celu określenia ogólnej skuteczności środków bezpieczeństwa lub ochrony prywatności.

Obiekty oceny identyfikują konkretne elementy podlegające ocenie i obejmują *specyfikacje*, *mechanizmy*, *działania* i *osoby*[22]. *Specyfikacje* to oparte na dokumentach artefakty (np. polityki, procedury, plany, wymagania dotyczące bezpieczeństwa i prywatności w systemie, specyfikacje funkcjonalne, projekty architektoniczne) związane z systemem informacyjnym. *Mechanizmy* to określony sprzęt komputerowy, aplikacje lub oprogramowanie układowe oraz środki zaradcze stosowane w systemie informacyjnym[23]. *Działania* to konkretne czynności związane z ochroną systemu informacyjnego, w których uczestniczą ludzie (np. wykonywanie operacji tworzenia kopii zapasowych systemu, monitorowanie ruchu sieciowego, wykonywanie planu ciągłości działania). *Osoby* lub grupy osób to ludzie stosujący opisane powyżej specyfikacje, mechanizmy lub działania.

Metody oceny określają charakter działań osoby oceniającej i obejmują *badanie*, *wywiad/rozmowę kwalifikacyjną* i *test*.

Metoda *badania* to proces przeglądu, kontroli, obserwacji, zgłębiania lub analizy jednego lub kilku obiektów oceny (tj. specyfikacji, mechanizmów lub działań). Celem metody badawczej jest ułatwienie osobie oceniającej zrozumienia, uzyskanie wyjaśnień lub uzyskanie dowodów.

Metoda *wywiadu* to proces prowadzenia rozmów z osobami lub grupami osób w organizacji w celu ponownego ułatwienia zrozumienia przez oceniającego, uzyskania wyjaśnień lub uzyskania dowodów.

Metoda *testu* to proces wykonywania jednego lub kilku przedmiotów oceny (tj. czynności lub mechanizmów) w określonych warunkach w celu porównania zachowania rzeczywistego z oczekiwanym.

---

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

[23] Mechanizmy obejmują również urządzenia ochrony fizycznej związane z systemem informacyjnym (np. zamki, klawiatury, kamery bezpieczeństwa, urządzenia przeciwpożarowe, sejfy ognioodporne itp.).

We wszystkich trzech metodach oceny, wyniki są wykorzystywane przez dokonania konkretnych ustaleń, które są wymagane w zestawach instrukcji, a tym samym do osiągnięcia celów procedury oceny. Pełny opis metod oceny i obiektów oceny znajduje się w Załączniku D.

Metody oceny posiadają zestaw powiązanych atrybutów - *szczegółowości* i *zasięgu stosowania* - które pomagają określić poziom nakładu pracy przy ocenie. Atrybuty te mają charakter hierarchiczny, zapewniając środki do określenia rygoru i zasięgu oceny w celu zwiększenia zaufania, które może być potrzebne w przypadku niektórych systemów informacyjnych.

Atrybut *szczegółowości* odnosi się do rygoru i poziomu dokładności procesów badania, wywiadu i testowania. Wartości dla atrybutu *szczegółowości* obejmują wartości *podstawowe*, *szczegółowe* i *kompleksowe*.

Atrybut *zasięgu stosowania* odnosi się do zasięgu lub rozległości stosowania procesów badania, wywiadu i testowania, w tym do liczby i rodzaju specyfikacji, mechanizmów i działań, które mają być badane lub testowane, oraz liczby i kategorii osób, z którymi mają być przeprowadzane wywiady. Podobnie jak w przypadku atrybutu szczegółowości, wartości dla atrybutu zasięgu obejmują element *podstawowy*, *szczegółowy* i *kompleksowy*.

Odpowiednie wartości atrybutu *szczegółowości* i *zasięgu stosowania* dla danej metody oceny opierają się na wymaganiach dotyczących wiarygodności określonych przez organizację[24]. Wraz ze wzrostem wymagań w zakresie zaufania w odniesieniu do opracowywania, wdrażania i funkcjonowania środków bezpieczeństwa i ochrony prywatności w ramach systemu informacyjnego lub odziedziczonych przez ten system, rośnie również rygor i zakres działań związanych z oceną (co znajduje odzwierciedlenie w wyborze metod i obiektów oceny oraz przypisywaniu wartości atrybutu

[24] W przypadku innych niż krajowe systemy bezpieczeństwa organizacje spełniają minimalne wymagania w zakresie zapewnienia bezpieczeństwa określone w publikacji NSC 800-53.

szczegółowości i zasięgu stosowania). Załącznik D zawiera szczegółowy opis atrybutów metody oceny i wartości atrybutów.

Tabela 1 ilustruje przykład procedury oceny opracowanej w celu oceny skuteczności podstawowych środków bezpieczeństwa rodziny CP-9. Cel oceny dla rodziny CP-9 wynika z bazowego zabezpieczenia opisanego w standardzie NSC 800-53 wer. 1. Do procedury oceny dodano potencjalne metody i obiekty oceny.

Tabela 1. Procedura oceny podstawowych środków bezpieczeństwa.

CP-9	**KOPIA ZAPASOWA**		
	CEL OCENY: *Określ, czy organizacja:*		
	CP-9(a)	**CP-9(a)[1]**	*definiuje częstotliwość, zgodną z celami dotyczącymi czasów odzyskiwania (RTO) i celami punktów odtworzenia danych (RPO) określonymi w planie awaryjnym systemu informacyjnego, do wykonywania kopii zapasowych informacji na poziomie użytkownika, przetwarzanych w systemie informacyjnym;*
		CP-9(a)[2]	*wykonuje kopie zapasowe informacji na poziomie użytkownika zawartych w systemie informacyjnym z częstotliwością określoną przez organizację;*
	CP-9(b)	**CP-9(b)[1]**	*definiuje częstotliwość, zgodną z celami dotyczącymi czasów odzyskiwania (RTO) i celami punktów odtworzenia danych (RPO) określonymi w planie awaryjnym systemu informacyjnego, do wykonywania kopii zapasowych informacji na poziomie systemu, przetwarzanych w systemie informacyjnym;*

CP-9	**KOPIA ZAPASOWA**		
		CP-9(b)[2]	*wykonuje kopie zapasowe informacji na poziomie systemu zawartych w systemie informacyjnym, z częstotliwością określoną przez organizację;*
	CP-9(c)	**CP-9(c)[1]**	*definiuje częstotliwość, zgodną z celami dotyczącymi czasów odzyskiwania (RTO) i celami punktów odtworzenia danych (RPO) określonymi w planie awaryjnym systemu informacyjnego, do wykonywania kopii zapasowych dokumentacji systemu informacyjnego, w tym dokumentacji związanej z bezpieczeństwem;*
		CP-9(c)[2]	*wykonuje kopie zapasowe dokumentacji, w tym dokumentacji związanej z bezpieczeństwem, z częstotliwością określoną przez organizację; oraz*
	CP-9(d)	*zapewnia poufność, integralność i dostępność kopii zapasowych w miejscach przechowywania.*	

CP-9	**KOPIA ZAPASOWA**
	POTENCJALNE METODY I PRZEDMIOTY OCENY: **Sprawdź:** [**wybierz spośród:** polityka planowania awaryjnego; procedury dotyczące tworzenia kopii zapasowych systemu informacyjnego; plan awaryjny; lokalizacje przechowywania kopii zapasowych; dzienniki lub rejestry kopii zapasowych systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [**wybierz spośród:** Personel organizacyjny odpowiedzialny za tworzenie kopii zapasowych systemu informacyjnego; personel organizacyjny z obowiązkami w zakresie bezpieczeństwa informacji]. **Test**: [**wybierz spośród:** Procesy organizacyjne do przeprowadzania kopii zapasowych systemu informacyjnego; zautomatyzowane mechanizmy wspierające i/lub wdrażające kopie zapasowe systemu informacyjnego].

Cele oceny są kolejno ponumerowane, najpierw zgodnie ze schematem numeracji zawartej w standardzie NSC 800-53 wer. 1, a następnie, w razie potrzeby, w celu dalszego podziału wymogów bezpieczeństwa lub ochrony prywatności, aby ułatwić ocenę, stosuje się kolejne numery lub litery w nawiasach kwadratowych [ ], w przeciwieństwie do nawiasów okrągłych ( ), w celu dokonania tego wyróżnienia (np. CP-9(a), CP-9(a)[1], CP-9(a)[2], CP-9(b)[1], CP-9(b)[2], CP-9(c)[1], CP-9(c)[2], CP-9(d) itd.). Początkowy znak w nawiasie kwadratowym jest zawsze liczbą. W przypadku niektórych środków bezpieczeństwa, kolumna z początkowym oznaczeniem zabezpieczenia (np. CP-9, CP-9(a), CP-9(b) i CP-9(c), jak to pokazano w tabeli 1) jest po prostu miejscem, które ułatwia rozdział zabezpieczenia przy zachowaniu schematu formatowania. Chociaż w przypadku każdej określonej metody oceny nie jest to wyraźnie zaznaczone w procedurze oceny, wartości atrybutu szczegółowości i zasięgu, opisane w Załączniku D, są przypisywane przez organizację i stosowane przez osobę oceniającą/zespół oceniający w trakcie wykonywania metody oceny w odniesieniu do obiektu oceny.

Jeżeli zabezpieczenie posiada jakiekolwiek zabezpieczenia rozszerzające (oznaczone sekwencyjnymi numerami w nawiasach okrągłych, na przykład CP-9 (3) dla trzeciego zabezpieczenia rozszerzającego zabezpieczenie CP-9), cele oceny są opracowywane dla każdego rozszerzenia przy użyciu tego samego procesu, co dla zabezpieczenia podstawowego. Wynikowe cele oceny są numerowane sekwencyjnie w taki sam sposób, jak procedura oceny zabezpieczenia podstawowego, najpierw zgodnie ze schematem numeracji zawartym w standardzie NSC 800-53 wer. 1, a następnie, aby ułatwić ocenę, przy użyciu sekwencyjnych numerów lub liter w nawiasach w celu dalszego podziału wymagań dotyczących rozszerzeń zabezpieczeń (np. CP-9(3)[1], CP-9(3)[2]). Tabela 2 ilustruje przykład procedury oceny opracowanej w celu oceny skuteczności trzeciego zabezpieczenia rozszerzającego środek bezpieczeństwa CP-9.

Tabela 2. Procedura oceny zabezpieczeń rozszerzonych.

CP-9(3) KOPIA ZAPASOWA | *SEPARACJA PRZECHOWYWANIA INFORMACJI KRYTYCZNYCH*			
	CEL OCENY: *Określ, czy organizacja:*		
	CP-9(3)[1]	**CP-9(3)[1][a]**	*definiuje aplikacje krytyczne systemu informacyjnego i inne informacje związane z bezpieczeństwem wymagające przechowywania kopii zapasowych w oddzielnym obiekcie; lub*
		CP-9(3)[1][b]	*definiuje aplikacje krytyczne systemu informacyjnego oraz inne informacje związane z bezpieczeństwem wymagające przechowywania kopii zapasowych w ognioodpornym kontenerze, który nie jest umieszczony z bieżącym systemem operacyjnym; oraz*

CP-9(3) KOPIA ZAPASOWA | *SEPARACJA PRZECHOWYWANIA INFORMACJI KRYTYCZNYCH*		
	CP-9(3)[2]	*przechowuje kopie zapasowe zdefiniowanego przez organizację oprogramowania krytycznego systemu informacyjnego i innych informacji związanych z bezpieczeństwem w oddzielnym obiekcie lub w ognioodpornym pojemniku, który nie jest połączony z systemem operacyjnym.*
	POTENCJALNE METODY I PRZEDMIOTY OCENY: **Sprawdź:** [**wybierz spośród:** polityka planowania awaryjnego; procedury dotyczące tworzenia kopii zapasowych systemu informacyjnego; plan awaryjny; lokalizacje przechowywania kopii zapasowych; dzienniki lub rejestry kopii zapasowych systemu informacyjnego; inne odpowiednie dokumenty lub rejestry]. **Wywiad:** [**wybierz spośród:** Personel organizacyjny odpowiedzialny za planowanie awaryjne i wdrażanie planów; personel organizacyjny odpowiedzialny za tworzenie kopi zapasowych systemów informacyjnych; personel organizacyjny odpowiedzialny za bezpieczeństwo informacji].	

Należy pamiętać, że liczby w nawiasach bezpośrednio po oznaczeniu zabezpieczenia podstawowego (Tabela 2) wskazują numer zabezpieczenia rozszerzonego, podczas gdy litery w nawiasach bezpośrednio po oznaczeniu zabezpieczenia podstawowego (Tabela 1) wskazują podział zabezpieczania podstawowego na oddzielne wymagania dotyczące tego zabezpieczenia. W przypadku, gdy w celu wsparcia oceny konieczny jest dalszy podział zabezpieczenia, stosuje się znaki w nawiasach kwadratowych, które występują na przemian w postaci liczb i liter (np. CP-9(3)[1][a], CP-9(3)[1][b]), przy czym początkowy nawias kwadratowy jest zawsze liczbą, niezależnie od tego, czy występuje po umieszczonej w nawiasie literze (zabezpieczenie podstawowe, np. CP-9(a)[1}, CP-9(b)[2]), czy po umieszczonej w nawiasie cyfrze (zabezpieczenie rozszerzone, np. CP-9(3)[1][a], CP-9(3)[2]).

Automatyczny Protokół Zabezpieczeń Zawartości (*ang. Security Content Automation Protocol - SCAP*) wspiera proces oceny środków bezpieczeństwa i umożliwia bardziej wydajne i opłacalne oceny. SCAP jest zbiorem powiązanych standardów służących do zautomatyzowanego zarządzania podatnościami, pomiarem i oceną zgodności z zasadami systemów wdrożonych w organizacji. Specyfikacje SCAP określają formaty, za pomocą których kryteria oceny, zwane również treścią SCAP, mogą być wymieniane i udostępniane narzędziom oceny. Zawartość ta może być wykorzystywana do automatyzacji gromadzenia i oceny materiału dowodowego pochodzącego zarówno z artefaktów maszynowych, jak i ludzkich. SCAP definiuje również formaty, które przechwytują i umożliwiają wymianę wyników gromadzenia i oceny artefaktów. Zazwyczaj artefakty maszynowe, które mogą być zbierane i oceniane za pomocą SCAP, odnoszą się do mechanizmów (np. ustawienia konfiguracji, zainstalowany sprzęt/aplikacje, stan bieżący środków przeciwdziałania). Dodatkowo, artefakty zorientowane na człowieka, takie jak te, które odnoszą się do specyfikacji i działań, mogą być zbierane za pomocą listy kontrolnej otwartego języka interaktywnego (*ang. Open Checklist Interactive Language - OCIL*). OCIL jest komponentem specyfikacji SCAP, umożliwiając zbieranie i przedstawianie danych z wywiadu/rozmowy kwalifikacyjnej w formacie opartym na standardach. Oparty na treści charakter rozwiązań automatyzacji obsługiwanych przez SCAP może wspierać elastyczną i spójną ocenę środków bezpieczeństwa i ochrony prywatności.

ROZDZIAŁ 3 - PROCES

PRZEPROWADZANIE SKUTECZNYCH OCEN ŚRODKÓW BEZPIECZEŃSTWA

Niniejszy rozdział opisuje proces oceny środków bezpieczeństwa i ochrony prywatności w systemach informacyjnych organizacji i środowiskach eksploatacji, w tym: (I) działania prowadzone przez organizacje i osoby oceniające w celu przygotowania ocen środków bezpieczeństwa i ochrony prywatności; (II) opracowywanie planów oceny bezpieczeństwa i ochrony prywatności; (III) przeprowadzanie ocen zabezpieczeń oraz analiza, dokumentowanie i sprawozdawczość dotycząca wyników oceny; oraz (IV) analiza sprawozdania z oceny i prowadzenie działań następczych.

3.1. PRZYGOTOWANIE DO OCENY ŚRODKÓW BEZPIECZEŃSTWA

Przeprowadzanie ocen środków bezpieczeństwa i ochrony prywatności we współczesnym rozbudowanym środowisku złożonym z zaawansowanej infrastruktury informatycznej i wysoce postrzegalnych, krytycznych dla misji aplikacji, może być trudne, stanowić wyzwanie i wymagać dużych zasobów. Oceny środków bezpieczeństwa i ochrony prywatności mogą być przeprowadzane przez różne jednostki organizacyjne o różnych obowiązkach nadzorczych. Sukces wymaga jednak współpracy oraz współdziałania wszystkich stron, które są żywotnie zainteresowane bezpieczeństwem informacji lub zachowaniem prywatności w organizacji, w tym właścicieli systemów informacyjnych, dostawców zabezpieczeń wspólnych, osób autoryzujących, CIO, SISO, SAOP/CPO, kierowników jednostek organizacyjnych, dyrektorów generalnych, personelu ds. bezpieczeństwa i ochrony prywatności oraz osób odpowiedzialnych za zarządzanie i budżet. Ustanowienie odpowiedniego zestawu oczekiwań: przed; w trakcie; i po dokonaniu oceny, ma zasadnicze znaczenie dla osiągnięcia akceptowalnego wyniku, tj. przedstawienia informacji niezbędnych do udzielenia osobie autoryzującej pomocy w podjęciu wiarygodnej, opartej na ryzyku decyzji o uruchomieniu lub kontynuacji działania systemu informacyjnego.

Gruntowne przygotowanie się przez organizację i osoby oceniające jest ważnym aspektem prowadzenia skutecznych ocen środków bezpieczeństwa i ochrony prywatności. Działania przygotowawcze dotyczą szeregu zagadnień związanych z kosztami, harmonogramem i wykonaniem oceny. Z punktu widzenia organizacji, przygotowanie do oceny środków bezpieczeństwa lub ochrony prywatności obejmuje następujące kluczowe działania:

- *zapewnienie istnienia i zrozumienia przez wszystkie zainteresowane struktury organizacji odpowiednich polityk dotyczących odpowiednio oceny środków bezpieczeństwa i ochrony prywatności;*
- *zapewnienie, aby przed etapem oceny bezpieczeństwa lub ochrony prywatności, wszystkie kroki zawarte w ramach zarządzania ryzykiem RMF[25] (standard NSC 800-37) zostały pomyślnie zakończone i uzyskały odpowiedni nadzór ze strony kierownictwa[26];*
- *ustalenie przedmiotu i zasięgu ocen (tj. celu ocen i tego, co jest oceniane);*
- *powiadamianie kluczowego personelu organizacji o zbliżających się ocenach i przydzielanie zasobów niezbędnych do ich przeprowadzenia;*
- *ustalenie ram czasowych przeprowadzania ocen i punktów kluczowych decyzji wymaganych przez organizację w celu skutecznego zarządzania ocenami;*

[25] Chociaż RMF może być wykorzystywany do ochrony prywatności, wybór zabezpieczeń prywatności jest dokonywany niezależnie od kategorii bezpieczeństwa systemów informacyjnych organizacji.

[26] Przeprowadzanie ocen środków bezpieczeństwa równolegle z fazami rozwoju/nabycia i wdrażania w cyklu życia systemu, pozwala na wczesne wykrycie słabych punktów i niedociągnięć oraz stanowi najbardziej opłacalną metodę inicjowania działań naprawczych. Problemy stwierdzone podczas tych ocen mogą być w stosownych przypadkach kierowane do upoważnionego personelu, celem wczesnego ich usunięcia. Wyniki ocen środków bezpieczeństwa przeprowadzonych podczas opracowywania i wdrażania systemu, mogą być również wykorzystane (zgodnie z kryteriami ponownego wykorzystania) podczas procesu autoryzacji bezpieczeństwa w celu uniknięcia opóźnień w tworzeniu systemu lub kosztownych powtórzeń ocen.

- *zapewnienie, aby środki bezpieczeństwa i ochrony prywatności określone, jako zabezpieczenia wspólne (oraz wspólna część zabezpieczeń hybrydowych) zostały przydzielone odpowiednim jednostkom organizacyjnym (tj. dostawcom zabezpieczeń wspólnych) w celu opracowania i wdrożenia[27];*
- *ustanowienie odpowiednich kanałów komunikacji pomiędzy jednostkami organizacyjnymi zainteresowanymi ocenami[28];*
- *identyfikacja i wybór kompetentnych osób oceniających/zespołów oceniających, którzy będą odpowiedzialni za przeprowadzanie ocen, z uwzględnieniem kwestii niezależności osób oceniających;*
- *gromadzenie artefaktów, które należy udostępnić osobom oceniającym/zespołom oceniającym (np. polityki, procedury, plany, specyfikacje, projekty, rejestry, podręczniki administratora/operatora, dokumentacja systemu informacyjnego, umowy o wzajemnym połączeniu, wcześniejsze wyniki oceny, wymogi prawne);*
- *ustanowienie mechanizmu współpracy pomiędzy organizacją, a oceniającymi i/lub zespołami oceniającymi w celu zminimalizowania niejasności lub nieporozumień dotyczących wdrażania środków bezpieczeństwa lub ochrony prywatności oraz słabości/niedociągnięć w zakresie środków bezpieczeństwa/ochrony prywatności zidentyfikowanych podczas ocen.*

Osoby oceniające bezpieczeństwo i ochronę prywatności/zespoły oceniające rozpoczynają przygotowania do swoich ocen poprzez:

[27] Oceny środków bezpieczeństwa i ochrony prywatności obejmują zabezpieczenia wspólne, za które odpowiedzialne są jednostki organizacyjne inne niż właściciel systemu informacyjnego, zabezpieczenia dziedziczone lub zabezpieczenia hybrydowe, w przypadku, gdy istnieje wspólna odpowiedzialność właściciela systemu (lub programu) i wyznaczonych jednostek organizacyjnych.

[28] W zależności od tego, czy oceniane są środki bezpieczeństwa lub ochrony prywatności, osoby te zazwyczaj obejmują upoważniony personel, właścicieli systemów informacyjnych (lub programów), dostawców zabezpieczeń wspólnych, właścicieli misji/przedsiębiorstw, właścicieli informacji/władających informacją, CIO, SISO, SAOP/CPO, ISSO, użytkowników z organizacji, która system informacyjny obsługuje, oraz osoby oceniające.

- *uzyskanie ogólnej wiedzy na temat działalności organizacji (w tym misji, funkcji i procesów biznesowych) oraz sposobu, w jaki system informacyjny będący przedmiotem danej oceny, wspiera działania organizacji;*
- *uzyskanie wiedzy na temat struktury systemu informacyjnego (tj. architektury systemu) oraz ocenianych środków bezpieczeństwa i ochrony prywatności (w tym zabezpieczeń specyficznych dla danego systemu, hybrydowych i wspólnych);*
- *zidentyfikowanie jednostek organizacyjnych odpowiedzialnych za opracowanie i wdrożenie zabezpieczeń wspólnych (lub wspólnej części zabezpieczeń hybrydowych) wspierających system informacyjny;*
- *organizację spotkań z upoważnionym kompetentnym personelem, w celu zapewnienia wspólnego zrozumienia celów oceny oraz proponowanego rygoru i zasięgu oceny;*
- *uzyskanie artefaktów niezbędnych do przeprowadzenia oceny (np. polityki, procedury, plany, specyfikacje, projekty, rejestry, podręczniki administratora i operatora, dokumentacja systemu informacyjnego, umowy o połączeniu międzysystemowym, wcześniejsze wyniki oceny);*
- *utworzenie odpowiednich organizacyjnych punktów kontaktowych niezbędnych do przeprowadzenia oceny;*
- *pozyskanie wyników poprzednich ocen, które mogą zostać odpowiednio wykorzystane do bieżącej oceny (np. sprawozdania ogólne, audyty, skanowanie podatności, środki bezpieczeństwa fizycznego, wcześniejsze oceny bezpieczeństwa lub prywatności, testy i ocena rozwojowa, działania naprawcze dostawcy, oceny ISO/IEC 15408 [wspólne kryteria]);*
- *opracowywanie planów oceny bezpieczeństwa i ochrony prywatności, które mogą być zintegrowane w jednym planie lub opracowane oddzielnie.*

W ramach przygotowań do oceny środków bezpieczeństwa lub ochrony prywatności, gromadzi się niezbędne informacje podstawowe i udostępnia je osobom oceniającym

lub zespołowi oceniającemu[29]. W zakresie niezbędnym do wsparcia konkretnej oceny oraz w zależności od tego, czy oceniane są środki bezpieczeństwa czy ochrony prywatności, organizacja identyfikuje i organizuje dostęp do: (I) elementów organizacji odpowiedzialnych za opracowywanie, dokumentowanie, rozpowszechnianie, przegląd i aktualizację wszystkich polityk bezpieczeństwa lub ochrony prywatności i związanych z nimi procedur wdrażania zabezpieczeń zgodnie z ustanowioną polityką; (II) polityk bezpieczeństwa lub ochrony prywatności dla systemu informacyjnego i związanych z nimi procedur wdrażania; (III) osób lub grup odpowiedzialnych za opracowywanie, wdrażanie, funkcjonowanie i utrzymanie środków bezpieczeństwa lub ochrony prywatności; (IV) wszelkich materiałów (np. plany bezpieczeństwa lub ochrony prywatności, rejestry, harmonogramy, sprawozdania z oceny, sprawozdania z działań następczych, umowy, pakiety autoryzacyjne) związane z wdrażaniem i funkcjonowaniem środków bezpieczeństwa lub ochrony prywatności, które mają być ocenione; oraz (V) konkretne obiekty, które mają być ocenione[30]. Dostępność niezbędnej dokumentacji, jak również dostęp do kluczowego personelu organizacyjnego i ocenianego systemu informacyjnego mają zasadnicze znaczenie dla powodzenia przeprowadzenia oceny.

Organizacje biorą pod uwagę zarówno wiedzę techniczną, jak i poziom niezależności wymagany przy wyborze osób oceniających środki bezpieczeństwa lub ochrony prywatności. Organizacje dbają o to, by osoby oceniające posiadały wymagane umiejętności i wiedzę techniczną, aby z powodzeniem przeprowadzać oceny zabezpieczeń specyficznych dla danego systemu, zabezpieczeń hybrydowych oraz

[29] Właściciele systemów informacyjnych (lub programów) i jednostki organizacyjne opracowujące, wdrażające i/lub administrujące zabezpieczenia wspólne (tj. dostawcy zabezpieczeń wspólnych) są odpowiedzialni za dostarczenie niezbędnych informacji osobom oceniającym.

[30] W sytuacjach, w których w organizacji prowadzonych lub planowanych jest wiele ocen bezpieczeństwa lub ochrony prywatności, dostęp do elementów organizacyjnych, osób i artefaktów wspierających te oceny jest zarządzany centralnie przez organizację w celu zapewnienia efektywnego kosztowo wykorzystania czasu i zasobów.

zabezpieczeń wspólnych. Obejmuje to wiedzę i doświadczenie w zakresie specyficznego sprzętu, aplikacji i elementów oprogramowania układowego wykorzystywanych przez organizację. Niezależna osoba oceniająca, to każda osoba zdolna do przeprowadzenia bezstronnej oceny środków bezpieczeństwa i ochrony prywatności stosowanych w systemie informacyjnym lub odziedziczonych przez ten system. Bezstronność oznacza, że osoby oceniające środki bezpieczeństwa i ochrony prywatności są wolne od wszelkich postrzeganych lub rzeczywistych konfliktów interesów w odniesieniu do rozwoju, działania i/lub zarządzania systemem informacyjnym lub określania skuteczności środków bezpieczeństwa i ochrony prywatności[31]. Upoważniający personel określa wymagany poziom niezależności osób oceniających w oparciu o wyniki procesu kategoryzacji bezpieczeństwa systemu informacyjnego (w przypadku oceny środków bezpieczeństwa) oraz ryzyko dla operacji organizacyjnych i aktywów, osób fizycznych, innych organizacji i społeczeństwa. Upoważniający określa, czy poziom niezależności osoby oceniającej jest wystarczający, aby zapewnić pewność, że uzyskane wyniki oceny są rzetelne i mogą być wykorzystane do podjęcia, opartej na ryzyku, decyzji o uruchomieniu systemu informacyjnego lub kontynuacji jego funkcjonowania.

Niezależne usługi oceny środków bezpieczeństwa i ochrony prywatności można uzyskać z innych komórek w ramach organizacji lub zlecić ich wykonanie podmiotowi sektora publicznego lub prywatnego spoza organizacji. W szczególnych sytuacjach, na przykład, gdy organizacja będąca właścicielem systemu informacyjnego jest niewielka lub gdy struktura organizacyjna wymaga, aby ocena środków bezpieczeństwa lub ochrony prywatności była dokonywana przez osoby będące w łańcuchu rozwojowym, operacyjnym i/lub zarządczym właściciela systemu, niezależność w procesie oceny

[31] Zakontraktowane usługi oceny są uważane za niezależne, jeżeli właściciel systemu (lub programu) informacyjnego nie jest bezpośrednio zaangażowany w proces zawierania umowy lub nie może nadmiernie wpłynąć na niezależność osoby (osób) oceniającej (oceniających) przeprowadzającej (prowadzących) ocenę bezpieczeństwa lub ochrony prywatności.

może być osiągnięta poprzez zapewnienie, że wyniki oceny są dokładnie przeglądane i analizowane przez niezależny zespół ekspertów, w celu potwierdzenia kompletności, spójności i rzetelności wyników[32].

3.2. OPRACOWYWANIE PLANÓW OCENY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Plan oceny bezpieczeństwa i *plan oceny ochrony prywatności* zawierają cele dotyczące odpowiednio oceny środków bezpieczeństwa i ochrony prywatności oraz szczegółowy plan działania dotyczący sposobu przeprowadzania takich ocen. Plany te mogą być opracowywane, jako jeden zintegrowany plan lub jako odrębne plany, w zależności od potrzeb organizacyjnych. Poniższe kroki są brane pod uwagę przez osoby oceniające przy opracowywaniu planów oceny środków bezpieczeństwa i ochrony prywatności w systemach informacyjnych organizacji lub odziedziczonych przez te systemy:

- *określenie, które środki bezpieczeństwa i ochrony prywatności/zabezpieczenia je rozszerzające, mają być włączone do oceny w oparciu o treść planu bezpieczeństwa i ochrony prywatności oraz cel i zakres oceny;*
- *wybranie odpowiednich procedur oceny, które mają być stosowane podczas ocen mechanizmów środków bezpieczeństwa i ochrony prywatności oraz zabezpieczeń rozszerzonych i które mają być uwzględnione w ocenach;*
- *dostosowanie wybranych procedur oceny (np. wybranie odpowiednich metod i przedmiotów oceny, przypisanie wartości atrybutów szczegółowości i zasięgu stosowania);*

[32] Osoba autoryzująca konsultuje się z SISO, SAOP/CPO, CIO, w zależności od przypadku, w celu omówienia skutków wszelkich decyzji dotyczących niezależności osoby oceniającej w opisanych powyżej szczególnych okolicznościach.

- *opracowanie dodatkowych procedur oceny w celu uwzględnienia wszelkich wymogów bezpieczeństwa i ochrony prywatności lub środków bezpieczeństwa, które nie są uwzględnione w wystarczający sposób w standardzie NSC 800-53 wer. 1;*
- *optymalizację procedur oceny w celu ograniczenia powielania działań (np. sekwencjonowanie i konsolidacja procedur oceny) oraz zapewnienie opłacalnych rozwiązań w zakresie oceny; oraz*
- *sfinalizowanie planów oceny i uzyskanie niezbędnych zezwoleń na ich wykonanie.*

3.2.1. OKREŚLENIE ŚRODKÓW BEZPIECZEŃSTWA PODLEGAJĄCYCH OCENIE

Plan bezpieczeństwa i ochrony prywatności zawiera przegląd wymogów bezpieczeństwa i ochrony prywatności odpowiednio dla systemu informacyjnego i organizacji oraz opisuje środki bezpieczeństwa i ochrony prywatności istniejące lub planowane w celu spełnienia tych wymogów. Oceniający rozpoczyna analizę od środków bezpieczeństwa i ochrony prywatności opisanych w planie bezpieczeństwa i prywatności i rozważa cel oceny. Ocena środków bezpieczeństwa lub ochrony prywatności może być pełną oceną wszystkich środków bezpieczeństwa w systemie informacyjnym lub odziedziczonych przez system (np. podczas wstępnego procesu zatwierdzania bezpieczeństwa lub prywatności) lub częściową oceną środków bezpieczeństwa w systemie informacyjnym lub odziedziczonych przez system (np. podczas opracowywania systemu w ramach ukierunkowanej oceny wynikającej ze zmian mających wpływ na konkretne środki bezpieczeństwa lub w przypadku, gdy zabezpieczenia te zostały wcześniej ocenione, a wyniki zaakceptowane w procesie zasad wzajemności).

W przypadku oceny częściowej, właściciele systemów informacyjnych i dostawcy zabezpieczeń wspólnych współpracują z upoważnionym personelem organizacji zaangażowanym w oceną (np. SISO, SAOP/CPO, właściciel misji/procesu biznesowego, osoba autoryzująca) w celu ustalenia, które z tych zabezpieczeń mają zostać poddane ocenie pod względem bezpieczeństwa lub ochrony prywatności. Określenie zabezpieczeń, które mają zostać poddane ocenie, zależy od celu oceny. Na przykład

w początkowych fazach cyklu życia systemu, można wybrać do oceny konkretne zabezpieczenia, aby rekomendować wczesne wykrywanie słabych punktów i niedociągnięć oraz bardziej efektywne kosztowo podejście do ograniczania ryzyka. Po udzieleniu wstępnego zezwolenia na eksploatację, może zaistnieć potrzeba przeprowadzenia szczegółowych ocen w przypadku wprowadzenia zmian w systemie, w poszczególnych środkach bezpieczeństwa lub ochrony prywatności, lub w środowisku eksploatacji. W takich przypadkach ocena koncentruje się na środkach bezpieczeństwa lub ochrony prywatności, na które zmiana mogłaby mieć wpływ.

3.2.2. WYBÓR PROCEDUR OCENY BEZPIECZEŃSTWA

Standard NSC 800-53A zawiera procedury oceny każdego zabezpieczenia podstawowego oraz zabezpieczenia rozszerzonego w zakresie bezpieczeństwa i ochrony prywatności zawartych w standardzie NSC 800-53 wer. 1. Dla każdego środka bezpieczeństwa i ochrony prywatności umieszczonego w planie bezpieczeństwa i ochrony prywatności, który ma być włączony do oceny, osoby oceniające wybierają odpowiednią procedurę oceny z Załącznika F (Procedury oceny bezpieczeństwa) lub Załącznika J (Procedury oceny prywatności). Wybrane procedury oceny mogą się różnić w zależności od oceny opartej o aktualną zawartość planów bezpieczeństwa i ochrony prywatności oraz celu oceny (np. ocena pełna, ocena częściowa).

3.2.3. DOSTOSOWYWANIE PROCEDUR OCENY

Podobnie jak w przypadku środków bezpieczeństwa i ochrony prywatności opisanych w standardzie NSC 800-53 wer. 1, które są dostosowane do misji organizacji, funkcji biznesowych, charakterystyki systemu informacyjnego i środowiska pracy, organizacje dostosowują procedury oceny wymienione w załącznikach F oraz J do konkretnych potrzeb organizacyjnych. Organizacje mają możliwość elastycznego przeprowadzania procesu dostosowania na poziomie organizacji, w odniesieniu do wszystkich systemów informacyjnych, na poziomie poszczególnych systemów informacyjnych lub przy zastosowaniu kombinacji podejścia na poziomie organizacji i specyficznego dla danego

systemu. Osoby oceniające środki bezpieczeństwa i ochrony prywatności określają, czy przed rozpoczęciem procesu dostosowania organizacja zapewnia dodatkowe wskazówki dotyczące tego procesu. Procedury oceny są dostosowywane przez:

- *wybór odpowiednich metod i obiektów oceny niezbędnych do osiągnięcia wyznaczonych celów oceny;*
- *wybór odpowiednich wartości atrybutów szczegółowości i zasięgu stosowania w celu określenia rygoru i zasięgu oceny;*
- *określenie zabezpieczeń wspólnych, które zostały ocenione za pomocą oddzielnie udokumentowanego planu oceny bezpieczeństwa lub planu oceny prywatności i nie wymagają wielokrotnego wykonywania procedur oceny;*
- *opracowanie procedur oceny specyficznych dla systemu informacyjnego/platformy oraz specyficznych dla organizacji (które mogą być dostosowane do procedur określonych w załącznikach F oraz J);*
- *włączenie wyników oceny z poprzednich ocen, jeżeli wyniki te zostaną uznane za właściwe; oraz*
- *dokonanie odpowiednich dostosowań w procedurach oceny, aby móc uzyskać wymagane dowody oceny od dostawców zewnętrznych.*

Metoda oceny i kwestie związane z ocenianym obiektem

Uznaje się, że organizacje mogą określać, dokumentować i konfigurować swoje systemy informacyjne na różne sposoby oraz, że zawartość i zastosowanie istniejących dowodów oceny będzie się różnić. Może to prowadzić do konieczności stosowania odmiennych metod oceny różnych przedmiotów oceny w celu wygenerowania materiału dowodowego potrzebnego do określenia, czy środek bezpieczeństwa lub ochrony prywatności jest skuteczny w swoim zastosowaniu. Dlatego też metody i przedmioty oceny dostarczane w ramach każdej procedury oceny, określa się jako *metody potencjalnie* odzwierciedlające potrzebę zdolności wyboru metod i przedmiotów najbardziej odpowiednich dla konkretnej oceny. Wybrane metody

i obiekty oceny to metody i przedmioty uznane za niezbędne do przedstawienia dowodów koniecznych do dokonania ustaleń opisanych w ustalonych sprawozdaniach. Potencjalne metody i przedmioty w procedurze oceny są dostarczane, jako źródło pomocy w wyborze odpowiednich metod i przedmiotów, a nie z zamiarem ograniczenia wyboru. Organizacje wykorzystują swoją ocenę przy wyborze potencjalnych metod oceny oraz listy obiektów oceny związane z każdą z wybranych metod. Organizacje wybierają te metody i obiekty, które w sposób najbardziej efektywny kosztowo przyczyniają się do dokonania ustaleń związanych z celem oceny[33]. Miarą jakości wyników oceny jest trafność przedstawionych przesłanek, a nie określony zbiór stosowanych metod i obiektów. W większości przypadków, w celu uzyskania pożądanych wyników oceny, nie będzie konieczne stosowanie każdej metody oceny w odniesieniu do każdego ocenianego obiektu. W przypadku niektórych ocen może być właściwe zastosowanie metody, która nie jest obecnie wymieniona w zestawie potencjalnych metod.

Czynniki związane z atrybutem szczegółowości i zasięgu (zakresem stosowania)

Oprócz wyboru odpowiednich metod i przedmiotów oceny, każda metoda oceny (tj. badanie, rozmowa kwalifikacyjna/wywiad i test) wiąże się z cechami szczegółowości i zakresu stosowania, które zostały opisane w załączniku D. Wartości tych atrybutów określają rygor (tryb postępowania) oraz zakres procedur oceny wykonywanych przez osobę oceniającą. Wartości wybrane przez organizację opierają się na charakterystyce ocenianego systemu informacyjnego (w tym wymaganiach dotyczących wiarygodności) oraz na konkretnych ustaleniach, które należy dokonać. Wartości atrybutów szczegółowości i zasięgu (zakresu stosowania) są związane z wymogami dotyczącymi wiarygodności określonymi przez organizację (tzn. rygor i zakres oceny zwiększają się w bezpośrednim związku z wymogami dotyczącymi wiarygodności). W przypadku

[33] Wybór metod i przedmiotów oceny (w tym liczba i rodzaj przedmiotów oceny) może być istotnym czynnikiem w efektywnym kosztowo osiąganiu celów oceny.

środków bezpieczeństwa, listy kontrolne SCAP stanowią profilowy mechanizm, który umożliwia dopasowanie wartości atrybutów i wybór konkretnych wymaganych zabezpieczeń w oparciu o pożądany poziom wiarygodności wymagany dla systemu informacyjnego. Te listy kontrolne umożliwiają konfigurowalną, automatyczną ocenę przy użyciu produktów zatwierdzonych przez SCAP.

Czynniki związane z zabezpieczeniami wspólnymi

Osoby dokonujące oceny odnotowują, które środki bezpieczeństwa lub ochrony prywatności (lub części takich zabezpieczeń) w planach bezpieczeństwa lub planach ochrony prywatności są wyznaczone, jako zabezpieczenia wspólne[34]. Ponieważ ocena zabezpieczeń wspólnych leży w gestii jednostki organizacyjnej, która je opracowała i wdrożyła (tj. dostawcy zabezpieczeń wspólnych), procedury oceny zawarte w załącznikach F oraz J stosowane do oceny tych zabezpieczeń, uwzględniają wyniki oceny tej jednostki organizacyjnej. Zabezpieczenia wspólne mogą być wcześniej ocenione, jako część programu bezpieczeństwa informacji lub programu ochrony w ci organizacji lub jako część systemu informacyjnego zapewniającego zabezpieczenia wspólne odziedziczone przez inne systemy organizacyjne. Mogą również istnieć oddzielne plany oceny zabezpieczeń wspólnych. W obu sytuacjach właściciele systemów informacyjnych koordynują ocenę zabezpieczeń wspólnych z odpowiednimi osobami uprawnionymi (np. CIO, SISO, SAOP/CPO, właściciel misji/informacji, osoba autoryzująca), uzyskując wyniki ocen zabezpieczeń wspólnych lub, jeżeli zabezpieczenia wspólne nie zostały ocenione lub mają zostać poddane ponownej

[34] Zabezpieczenia wspólne wspierają wiele systemów informacyjnych w ramach organizacji, a środki bezpieczeństwa zapewniane przez te zabezpieczenia są dziedziczone przez poszczególne systemy. W związku z tym, organizacja określa odpowiedni zestaw zabezpieczeń wspólnych w celu zapewnienia, że zarówno siła zabezpieczeń (tj. zdolności w zakresie bezpieczeństwa), jak i poziom rygoru i intensywności oceny zabezpieczeń są współmierne do krytyczności i/lub wrażliwości poszczególnych systemów informacyjnych, które te zabezpieczenia odziedziczyły. Niedociągnięcia lub braki w zabezpieczeniach wspólnych mogą mieć negatywny wpływ na dużą część organizacji i w związku z tym wymagają znacznej uwagi.

ocenie, dokonując niezbędnych ustaleń w celu włączenia lub odniesienia wyników oceny zabezpieczeń wspólnych do bieżącej oceny[35].

Innym czynnikiem branym pod uwagę przy ocenie zabezpieczeń wspólnych jest fakt, że czasami istnieją specyficzne dla danego systemu aspekty zabezpieczeń wspólnych, które nie są objęte przez jednostki organizacyjne odpowiedzialne za aspekty zabezpieczeń wspólnych. Te rodzaje zabezpieczeń określane są jako zabezpieczenia hybrydowe. Na przykład rodzina zabezpieczeń CP-2, Plan ciągłości działania, może być uznana przez organizację za zabezpieczenie hybrydowe, jeżeli istnieje plan ciągłości działania opracowany przez organizację dla wszystkich systemów informacyjnych organizacji. W następstwie wstępnego planu ciągłości działania oczekuje się, że właściciele systemów informacyjnych dostosują lub zmodyfikują plan ciągłości działania do potrzeb, jeżeli istnieją szczególne aspekty planu, które muszą być określone dla danego systemu, w którym stosowane jest to zabezpieczenie. W przypadku każdego zabezpieczenia hybrydowego, osoby oceniające włączają do planów oceny bezpieczeństwa lub planów oceny prywatności te części procedur oceny z załączników F lub J, które odnoszą się do tych części zabezpieczeń, które są specyficzne dla danego systemu, aby zapewnić, że uzyskane wyniki oceny zabezpieczeń wspólnych zawierają oszacowanie wszystkich aspektów zabezpieczeń.

Czynniki związane z systemem/platformą i organizacją

Procedury oceny zawarte w standardzie NSC 800-53A mogą być dostosowane do wymagań specyficznych dla systemu i platformy lub organizacji. Na przykład, ocena implementacji UNIX-owej zabezpieczenia IA-2, Identyfikacja i uwierzytelniania użytkowników organizacyjnych, może obejmować jednoznaczne badanie pliku *.rhosts* dla systemów UNIX, ponieważ niewłaściwe wpisy w tym pliku mogą spowodować

[35] Jeżeli wyniki oceny nie są obecnie dostępne dla zabezpieczeń wspólnych, bierze się pod uwagę plany oceny ocenianych systemów informacyjnych, które to plany zależą od stosowanych zabezpieczeń. Oceny nie można uznać za kompletną, dopóki wyniki oceny zabezpieczeń wspólnych nie zostaną udostępnione właścicielom systemów informacyjnych.

ominięcie uwierzytelniania użytkowników. Ostatnie wyniki testów mogą mieć również zastosowanie do bieżącej oceny, jeśli te metody testowania zapewniają wysoki stopień przejrzystości/zrozumiałości (np. co było testowane, kiedy było testowane, jak było testowane). Protokoły testowe oparte na standardach, takie jak SCAP, stanowią przykład tego, w jaki sposób organizacje mogą pomóc osiągnąć ten poziom przejrzystości. SCAP zapewnia przejrzystość poprzez wykorzystanie znormalizowanej zawartości, która definiuje metody testowania oraz poprzez znormalizowane wyniki, które wskazują, jaka zawartość została użyta, jaki stan systemu został przetestowany, jaki stan został znaleziony, jakie narzędzie zostało użyte do przeprowadzenia testu oraz kiedy test został przeprowadzony.

Ponowna ocena czynników związanych z dowodami

Ponowne wykorzystanie wyników oceny z wcześniej zaakceptowanych lub zatwierdzonych ocen jest uwzględniane w materiale dowodowym w celu określenia ogólnej skuteczności w zakresie środków bezpieczeństwa lub ochrony prywatności. Wcześniej zaakceptowane lub zatwierdzone oceny obejmują: (I) oceny zabezpieczeń wspólnych, które są zarządzane przez organizację i obsługują wiele systemów informacyjnych; (II) oceny środków bezpieczeństwa lub ochrony prywatności, które są przeglądane w ramach wdrażania zabezpieczeń (np. CP-2 wymaga przeglądu planu ciągłości działania); lub (III) informacje dotyczące bezpieczeństwa generowane przez program (strategię) ciągłego monitorowania bezpieczeństwa informacji organizacji (*ang. Information Security Continuous Monitoring - ISCM*). Dopuszczalność wykorzystania wyników poprzedniej oceny środków bezpieczeństwa lub ochrony prywatności jest koordynowana i zatwierdzana przez użytkowników wyników oceny. Istotne jest, aby właściciele systemów informacyjnych i dostawcy zabezpieczeń wspólnych, współpracowali z upoważnionym personelem i innymi odpowiednimi osobami autoryzującymi, przy ustalaniu dopuszczalności wykorzystania wyników wcześniejszej oceny. Rozważając ponowne wykorzystanie wyników poprzedniej oceny oraz wartość tych wyników do bieżącej oceny, osoby oceniające określają: (I) wiarygodność dowodów oceny; (II) stosowność wcześniejszej analizy; oraz (III) możliwość

zastosowania dowodów oceny do bieżących warunków funkcjonowania systemu informacyjnego. W przypadku ponownego wykorzystania wyników poprzedniej oceny, datę pierwotnej oceny i rodzaj oceny dokumentuje się w planie oceny bezpieczeństwa lub planie oceny ochrony prywatności oraz w sprawozdaniu z oceny bezpieczeństwa lub sprawozdaniu z oceny ochrony prywatności. W stosownych przypadkach, znormalizowane wyniki oceny bezpieczeństwa dostarczone przez narzędzia SCAP, mogą być ponownie wykorzystane przez wiele stron.

W niektórych sytuacjach konieczne może okazać się uzupełnienie wyników wcześniejszej oceny, które są rozważane do ponownego wykorzystania, dodatkowymi działaniami oceniającymi, aby w pełni zrealizować cele oceny. Na przykład, jeżeli niezależna ocena produktu informatycznego nie badała konkretnego ustawienia konfiguracyjnego, które jest stosowane przez organizację w systemie informacyjnym, wówczas osoba oceniająca może być zmuszona do uzupełnienia pierwotnych wyników badań dodatkowymi badaniami, w celu uwzględnienia tego ustawienia konfiguracyjnego dla bieżącego środowiska systemu informacyjnego. Decyzja o ponownym wykorzystaniu wyników oceny jest udokumentowana w planie oceny bezpieczeństwa lub planie oceny prywatności oraz w końcowym raporcie oceny bezpieczeństwa lub raporcie oceny prywatności i powinna być zgodna z krajowym ustawodawstwem, polityką, dyrektywami, normami i wytycznymi.

Przy zatwierdzaniu wyników poprzedniej oceny w celu ponownego ich użycia, brane są pod uwagę następujące elementy:

- ***Zmieniające się z czasem warunki związane ze środkami bezpieczeństwa i ochrony prywatności.***

Środki bezpieczeństwa i ochrony prywatności, które zostały uznane za skuteczne podczas poprzednich ocen, mogły stać się nieskuteczne z powodu zmieniających się warunków w systemie informacyjnym lub środowisku jego działania, w tym informacji o pojawiających się zagrożeniach. Wyniki oceny, które zostały wcześniej uznane za możliwe do zaakceptowania, mogą nie stanowić już wiarygodnego dowodu na

określenie skuteczności środków bezpieczeństwa i ochrony prywatności, co spowoduje konieczność przeprowadzenia ponownej oceny. Zastosowanie wyników poprzedniej oceny do bieżącej oceny wymaga określenia wszelkich zmian, które nastąpiły od czasu poprzedniej oceny, oraz wpływu tych zmian na poprzednie wyniki. Na przykład, ponowne wykorzystanie wyników poprzedniej oceny z badania polityki i procedur bezpieczeństwa lub ochrony prywatności organizacji może być dopuszczalne, jeżeli zostanie stwierdzone, że nie nastąpiły żadne istotne zmiany w określonych politykach i procedurach. Ponowne wykorzystanie wyników oceny uzyskanych podczas poprzedniej autoryzacji systemu informacyjnego jest efektywną kosztowo metodą wsparcia działań monitorujących ciągłego monitorowania i wymogów w zakresie sprawozdawczości, gdy związane z nimi zabezpieczenia nie uległy zmianie i istnieją odpowiednie podstawy, by mieć zaufanie do ich dalszego stosowania.

- ***Okres czasu, który upłynął od poprzednich ocen.***

Ogólnie rzecz biorąc, wraz ze zwiększaniem się okresu czasu między bieżącą, a poprzednią oceną, wiarygodność i użyteczność wyników poprzedniej oceny maleje. Wynika to przede wszystkim z faktu, że system informacyjny lub środowisko, w którym działa system informacyjny, z biegiem czasu może ulec zmianie, co może spowodować unieważnienie pierwotnych warunków lub założeń, na których opierała się poprzednia ocena.

- ***Stopień niezależności poprzednich ocen.***

Niezależność oceniającego może być krytycznym czynnikiem w niektórych rodzajach ocen. Stopień niezależności wymagany przy poszczególnych ocenach powinien być spójny. Na przykład, nie jest właściwe ponowne wykorzystanie wyników poprzedniej samooceny w bieżącej ocenie wymagającej większego stopnia niezależności w przypadku, gdy nie była wymagana niezależność oceniającego.

Czynniki związane z zewnętrznym systemem informacyjnym

Procedury oceny zawarte w załącznikach F oraz J należy odpowiednio dostosować w celu uwzględnienia oceny zewnętrznych systemów informacyjnych[36]. Ponieważ organizacja nie zawsze ma bezpośrednią kontrolę nad środkami bezpieczeństwa lub ochrony prywatności stosowanymi w zewnętrznych systemach informacyjnych, lub nie ma wystarczającej możliwości w zakresie opracowywania, wdrażania i oceny tych zabezpieczeń, konieczne może być zastosowanie alternatywnych podejść do oceny, co spowoduje konieczność dostosowania procedur oceny opisanych w załącznikach F oraz J. W przypadku, gdy wymagana wiarygodność uzgodnionych środków bezpieczeństwa lub ochrony prywatności w ramach systemu informacyjnego lub odziedziczonych przez system jest udokumentowana w umowach lub porozumieniach gwarancji świadczenia usług (*ang. Service Level Agreement - SLA*), osoby oceniające dokonują przeglądu tych umów lub porozumień oraz, w stosownych przypadkach, dostosowują procedury oceny w celu oceny środków bezpieczeństwa lub ochrony prywatności lub wyników oceny środków bezpieczeństwa lub ochrony prywatności, dostarczonych w ramach tych umów. Ponadto osoby oceniające biorą pod uwagę wszelkie inne oceny zewnętrznych systemów informacyjnych, które zostały przeprowadzone lub są w trakcie przeprowadzania, na których opiera się ochrona ocenianego systemu informacyjnego. Stosowne informacje pochodzące z tych ocen, jeżeli zostaną uznane za wiarygodne, są włączane do sprawozdania z oceny bezpieczeństwa lub sprawozdania z oceny ochrony prywatności, stosownie do przypadku.

[36] Zewnętrzny system informacyjny jest systemem informacyjnym lub częścią składową systemu informacyjnego, który znajduje się poza granicą autoryzacji ustanowioną przez organizację i w odniesieniu do którego organizacja zazwyczaj nie ma bezpośredniej kontroli nad stosowaniem wymaganych środków bezpieczeństwa i ochrony prywatności lub oceną skuteczności środków bezpieczeństwa i ochrony prywatności. Standardy NSC 800-37 i NSC 800-53 wer. 1 zawierają dodatkowe wskazówki dotyczące zewnętrznych systemów informacyjnych i skutków stosowania środków bezpieczeństwa w tych typach środowisk.

3.2.4. OPRACOWANIE PROCEDUR OCENY ZABEZPIECZEŃ SPECYFICZNYCH DLA ORGANIZACJI

W oparciu o zasady organizacyjne, misje lub wymagania dotyczące funkcji biznesowych oraz ocenę ryzyka, organizacje mogą zdecydować się na opracowanie i wdrożenie w swoich systemach informacyjnych dodatkowych (specyficznych dla danej organizacji) środków bezpieczeństwa lub ochrony prywatności, a także zabezpieczeń rozszerzających, które wykraczają poza zakres standardu NSC 800-53 wer. 1. Takie zabezpieczenia są dokumentowane w planie bezpieczeństwa lub ochrony prywatności, jako środki bezpieczeństwa, które nie są zawarte w standardzie NSC 800-53 wer. 1. Aby w tej sytuacji ocenić środki bezpieczeństwa lub ochrony prywatności, osoby oceniające korzystają z wytycznych zawartych w rozdziale drugim tej publikacji, w celu opracowania procedur oceny tych zabezpieczeń i zabezpieczeń rozszerzonych. Opracowane procedury oceny są następnie włączane, w stosownych przypadkach, do planu oceny bezpieczeństwa lub planu oceny ochrony prywatności.

3.2.5. OPTYMALIZACJA WYBRANYCH PROCEDUR OCENY W CELU ZAPEWNIENIA MAKSYMALNEJ WYDAJNOŚCI

Oceniający mają dużą elastyczność w organizowaniu planów oceny, które odpowiadają potrzebom organizacji i dają najlepszą możliwość uzyskania niezbędnych dowodów w celu określenia skuteczności środków bezpieczeństwa lub ochrony prywatności, przy jednoczesnym obniżeniu ogólnych kosztów oceny. Łączenie i konsolidacja procedur oceny jest jednym z obszarów, w którym można zastosować tę elastyczność. Podczas oceny systemu informacyjnego, metody oceny są wielokrotnie stosowane do różnych przedmiotów oceny w ramach danej rodziny środków bezpieczeństwa lub ochrony prywatności. Aby zaoszczędzić czas, zmniejszyć koszty oceny i zmaksymalizować użyteczność wyników oceny, osoby oceniające dokonują przeglądu wybranych procedur oceny w odniesieniu do rodzin środków bezpieczeństwa lub ochrony prywatności i łączą lub konsolidują procedury (lub ich części), gdy jest to możliwe lub wykonalne. Na przykład, osoby oceniające mogą skonsolidować wywiady z kluczowym

personelem organizacji zajmującym się różnymi zagadnieniami związanymi z bezpieczeństwem lub prywatnością. Oceniający mogą mieć inne zdolności znacznej konsolidacji i oszczędności kosztów poprzez jednoczesne badanie wszystkich polityk i procedur z rodzin środków bezpieczeństwa i ochrony prywatności lub poprzez organizowanie grup powiązanych polityk i procedur, które mogłyby być badane jako jednolita jednostka. Uzyskanie i zbadanie konfiguracji ustawień z podobnych komponentów sprzętu i aplikacji w ramach systemu informacyjnego, jest kolejnym przykładem, który może zapewnić znaczącą efektywność oceny.

Dodatkowym obszarem do rozważenia przy optymalizacji procesu oceny jest kolejność, w jakiej oceniane są środki bezpieczeństwa lub ochrony prywatności. Ocena niektórych środków bezpieczeństwa i ochrony prywatności przed innymi zabezpieczeniami, może dostarczyć użytecznych informacji, które ułatwią zrozumienie i bardziej efektywną ocenę innych zabezpieczeń. Na przykład, środki bezpieczeństwa, takie jak CM-2 (Konfiguracja podstawowa), CM-8 (Inwentaryzacja komponentów systemu informacyjnego), PL-2 (Plan bezpieczeństwa systemu), RA-2 (Kategoryzacja bezpieczeństwa) i RA-3 (Ocena ryzyka), dają ogólny opis systemu informacyjnego. Ocena tych środków bezpieczeństwa na wczesnym etapie procesu oceny może dostarczyć podstawowej wiedzy na temat systemu informacyjnego, która może pomóc w ocenie innych środków bezpieczeństwa. Dodatkowe wskazówki dotyczące wielu środków bezpieczeństwa i ochrony prywatności określają również powiązane zabezpieczenia, które mogą dostarczyć użytecznych informacji przy organizowaniu procedur oceny. Na przykład AC-19 (Kontrola dostępu realizowanego z urządzeń przenośnych (mobilnych)) wymienia środki bezpieczeństwa MP-4 (Przechowywanie nośników) i MP-5 (Transport nośników) jako zabezpieczenia powiązane z zabezpieczeniem AC-19. Ponieważ AC-19 jest powiązany z MP-4 i MP-5, sekwencja, w której przeprowadzane są oceny dla AC-19, MP-4 i MP-5, może ułatwić ponowne wykorzystanie informacji o ocenie jednego zabezpieczenia przy ocenie innych powiązanych zabezpieczeń.

3.2.6. OPRACOWANIE OSTATECZNEGO PLANU OCENY I UZYSKANIE ZGODY NA JEGO WPROWADZENIE W ŻYCIE.

Po wybraniu procedur oceny (w tym opracowaniu niezbędnych procedur nieujętych w katalogu procedur standardu NSC 800-53A), dostosowaniu procedur do warunków specyficznych dla systemu/platformy informatycznej i organizacji, optymalizacji procedur pod kątem efektywności oraz uwzględnieniu zdolności wystąpienia nieoczekiwanych zdarzeń mających wpływ na ocenę, plan oceny jest finalizowany, a harmonogram oceny jest ustalany z uwzględnieniem kluczowych etapów procesu oceny. Po ukończeniu planu oceny bezpieczeństwa lub planu oceny ochrony prywatności, plan jest poddawany przeglądowi i zatwierdzany przez właściwy personel organizacji[37] w celu zapewnienia, że plan jest: (I) kompletny; (II) zgodny z celami organizacji w zakresie bezpieczeństwa lub ochrony prywatności, w stosownych przypadkach, oraz z oceną ryzyka dokonaną przez organizację; oraz (III) wydajny w odniesieniu do zasobów przydzielonych do oceny.

3.3. PRZEPROWADZANIE OCENY ŚRODKÓW BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Po zatwierdzeniu planu oceny bezpieczeństwa lub planu oceny prywatności przez organizację, osoba oceniająca lub zespół oceniający wykonuje plan zgodnie z ustalonym harmonogramem. Ustalenie wielkości i składu organizacyjnego zespołu oceniającego (tj. zestawu umiejętności, wiedzy technicznej i doświadczenia w ocenie osób wchodzących w jego skład) jest częścią decyzji dotyczących zarządzania ryzykiem podejmowanych przez organizację zgłaszającą wniosek o ocenę i inicjującą ją. Wyniki oceny środków bezpieczeństwa i ochrony prywatności są dokumentowane odpowiednio w raportach oceny bezpieczeństwa i raportach oceny prywatności, które

[37] Organizacje ustanawiają proces zatwierdzania planów oceny bezpieczeństwa i ochrony prywatności z określonym personelem organizacyjnym (np. właścicielami systemów informacyjnych, dostawcami zabezpieczeń wspólnych, ISSO, SISO, SAOP/CPO, osobą autoryzującą) wyznaczonymi, jako organy zatwierdzające.

są kluczowym wkładem do pakietu autoryzacji bezpieczeństwa, opracowanego przez właścicieli systemów informacyjnych oraz dostawców zabezpieczeń wspólnych i przedstawianego osobie autoryzującej[38]. Raporty z oceny bezpieczeństwa i raporty z oceny prywatności zawierają informacje od osób oceniających (w formie wyników oceny) niezbędne do określenia skuteczności środków bezpieczeństwa lub ochrony prywatności, stosowanych w systemie informacyjnym lub przez niego dziedziczonych. Te raporty oceniające są kluczowym czynnikiem przy określaniu ryzyka przez personel zatwierdzający. Organizacje mogą zdecydować się na opracowanie podsumowania oceny na podstawie szczegółowych ustaleń, które są generowane przez osoby oceniające podczas ocen środków bezpieczeństwa i ochrony prywatności. Podsumowanie oceny może zapewnić upoważnionemu urzędnikowi skróconą wersję raportu oceniającego, koncentrującego się na najważniejszych punktach oceny, streszczeniu najważniejszych ustaleń oraz zaleceniach dotyczących usunięcia słabych punktów i niedociągnięć w ocenianych systemach środków bezpieczeństwa i ochrony prywatności. Załącznik G zawiera informacje na temat zalecanej treści sprawozdań z oceny bezpieczeństwa i ochrony prywatności.

Cele oceny są osiągane poprzez zastosowanie określonych metod oceny do wybranych obiektów oceny oraz zebranie/przedstawienie dowodów niezbędnych do dokonania ustaleń związanych z każdym celem oceny. Każdy zestaw instrukcji dotyczący ustalenia, zawarty w procedurze oceny przeprowadzanej przez osobę oceniającą, prowadzi do jednego z następujących wniosków: (I) *satysfakcjonujące* (S); lub (II) *niesatysfakcjonujące* (N). Stwierdzenie *satysfakcjonujący* oznacza, że w odniesieniu do części środków bezpieczeństwa lub ochrony prywatności, której dotyczy stwierdzenie ustalające, uzyskane informacje oceniające (tj. zebrane dowody) wskazują, że cel oceny w zakresie bezpieczeństwa został osiągnięty, dając w pełni akceptowalny wynik.

[38] Zgodnie ze standardem NSC 800-37, pakiet autoryzacji bezpieczeństwa składa się z planu bezpieczeństwa (*ang. security plan*), raportu z oceny bezpieczeństwa (*ang. security assessment report*) oraz planu i etapów działania/kamieni milowych (*ang. plan of action and milestones - POAM*).

Ustalenie *niesatysfakcjonujące* wskazuje, że w odniesieniu do części środków bezpieczeństwa lub ochrony prywatności, której dotyczy oświadczenie o ustalanych wynikach, uzyskane informacje oceniające wskazują na potencjalne nieprawidłowości w działaniu lub realizacji zabezpieczeń, którymi organizacja może być zmuszona się zająć. Ustalenie *niesatysfakcjonujące* może również wskazywać, że z powodów określonych w sprawozdaniu z oceny, osoba oceniająca nie była w stanie uzyskać informacji wystarczających do dokonania konkretnego wymaganego ustalenia. W przypadku ustaleń oceny jako *niesatysfakcjonujące*, organizacje mogą zdecydować się na zdefiniowanie podkategorii ustaleń wskazujących na wagę i/lub krytyczność wykrytych słabości lub braków oraz potencjalny niekorzystny wpływ na działalność organizacji (tj. misje, funkcje, wizerunek lub reputację), aktywa organizacji, osoby, inne organizacje i społeczeństwo. Zdefiniowanie takich podkategorii może pomóc w ustaleniu priorytetów niezbędnych działań ograniczających ryzyko.

Wyniki oceny stanowią obiektywną, rzeczową informację o tym, co zostało stwierdzone w odniesieniu do ocenianego środka bezpieczeństwa lub ochrony prywatności. Dla każdego z ustaleń innych niż *satysfakcjonujące*, oceniający wskazują, na które części środków bezpieczeństwa lub ochrony prywatności mają wpływ ustalenia (tj. na te aspekty zabezpieczeń, które zostały uznane za niezadowalające lub nie mogły być ocenione) oraz opisują, w jaki sposób zabezpieczenie różni się od stanu planowanego lub oczekiwanego. W raporcie z oceny bezpieczeństwa lub ochrony prywatności, osoba oceniająca zwraca również uwagę na możliwość naruszenia poufności, integralności i dostępności z powodu innych niż zadowalające ustaleń. Zapis ten odzwierciedla brak określonej ochrony, a w rezultacie możliwość wykorzystania tej podatności (tj. dostępu do stacji roboczej, zbioru danych, dostępu na poziomie root-a). Działania związane z określaniem i akceptacją ryzyka są prowadzone przez organizację po dokonaniu oceny, jako część strategii zarządzania ryzykiem ustanowionej przez organizację. Te działania w zakresie zarządzania ryzykiem obejmują wyższe kierownictwo organizacji, w tym na przykład kierowników jednostek organizacyjnych, właścicieli misji/biznesu, właścicieli informacji/władających informacją, funkcję

zarządzania ryzykiem (*ang. risk executive function*), osoby autoryzujące w porozumieniu z odpowiednim personelem wsparcia organizacyjnego (np. SISO, SAOP/CPO, CIO, właścicielami systemów informacyjnych, dostawcami zabezpieczeń wspólnych oraz osobami oceniającymi). Wyniki oceny środków bezpieczeństwa i ochrony prywatności są dokumentowane na poziomie szczegółowości właściwym dla danej oceny, zgodnie z formatem raportowania określonym w polityce organizacyjnej. Format raportowania jest odpowiedni dla rodzaju przeprowadzonej oceny (np. samoocena przez właścicieli systemów informacyjnych i dostawców zabezpieczeń wspólnych, niezależna weryfikacja i ocena, niezależne oceny wspierające proces autoryzacji, oceny automatyczne lub niezależne audyty lub inspekcje).

Właściciele systemów informacyjnych i dostawcy zabezpieczeń wspólnych polegają na wiedzy fachowej i ocenie technicznej osób oceniających, w zakresie: (I) oceny środków bezpieczeństwa i ochrony prywatności w systemie informacyjnym oraz odziedziczonych przez ten system; oraz (II) przedstawienia zaleceń dotyczących sposobu skorygowania słabych punktów lub niedociągnięć zabezpieczeń oraz ograniczenia lub wyeliminowania zidentyfikowanych słabych punktów. Wyniki oceny przedstawione przez osobę oceniającą (tj. ustalenia *satysfakcjonujące* lub *niesatysfakcjonujące*, określenie tych części środków bezpieczeństwa lub ochrony prywatności, które nie przyniosły zadowalających wyników, oraz opis wynikającej z nich zdolności narażenia systemu informacyjnego lub środowiska, w którym funkcjonuje) są przekazywane właścicielom systemów informacyjnych i dostawcom zabezpieczeń wspólnych we wstępnych sprawozdaniach z oceny bezpieczeństwa i sprawozdaniach z oceny prywatności. Właściciele systemów i dostawcy zabezpieczeń wspólnych mogą zdecydować się na działania zgodnie z wybranymi zaleceniami osoby oceniającej przed sfinalizowaniem raportów oceniających, jeżeli istnieją konkretne zdolności skorygowania słabych punktów lub niedociągnięć w zakresie środków bezpieczeństwa lub ochrony prywatności, albo skorygowanie lub wyjaśnienie

nieporozumień lub interpretacji wyników oceny[39]. Środki bezpieczeństwa lub ochrony prywatności, które są modyfikowane, ulepszane lub dodawane w trakcie tego procesu, są ponownie oceniane przez osobę oceniającą przed sporządzeniem sprawozdania z oceny końcowej.

3.4. ANALIZA WYNIKÓW RAPORTU Z OCENY

Wyniki oceny środków bezpieczeństwa i ochrony prywatności mają ostatecznie wpływ na realizację zabezpieczeń, treść planów bezpieczeństwa i planów ochrony prywatności, a także na odpowiednie plany i etapy działania. W związku z tym, właściciele systemów informacyjnych i dostawcy zabezpieczeń wspólnych dokonują przeglądu raportów z oceny bezpieczeństwa i raportów z oceny prywatności oraz zaktualizowanej oceny ryzyka, a także przy współudziale wyznaczonego personelu upoważnionego organizacji (np. osoba autoryzująca, CIO, SISO, SAOP/CPO, właściciele informacji/misji), określają odpowiednie kroki wymagane do zareagowania na te słabe punkty i niedociągnięcia zidentyfikowane podczas oceny. Stosując oznaczenia *satysfakcjonujące* oraz *niesatysfakcjonujące*, format sprawozdania z wyników oceny zapewnia personelowi organizacyjnemu wgląd w konkretne słabości i braki w zakresie środków bezpieczeństwa lub ochrony prywatności w ramach systemu informacyjnego lub odziedziczonych przez system oraz ułatwia zdyscyplinowane i ustrukturyzowane podejście do reagowania na ryzyko zgodnie z priorytetami organizacyjnymi. Na przykład, właściciele systemów informacyjnych lub dostawcy zabezpieczeń wspólnych

[39] Korekta słabych punktów lub niedociągnięć w zakresie środków bezpieczeństwa, ochrony prywatności lub wykonywanie zaleceń podczas przeglądu wstępnych raportów z oceny bezpieczeństwa lub raportów z oceny prywatności przez właścicieli systemów informacyjnych lub dostawców zabezpieczeń wspólnych, nie ma na celu zastąpienia formalnego procesu reagowania na ryzyko przez organizację, który następuje po dostarczeniu raportów końcowych. Daje to raczej właścicielowi systemu informacyjnego lub dostawcy zabezpieczeń wspólnych możliwość usunięcia słabych punktów lub niedociągnięć, które mogą być szybko skorygowane. Jednakże w sytuacjach, w których istnieją ograniczone zasoby na usuwanie słabych punktów i niedociągnięć wykrytych podczas oceny środków bezpieczeństwa lub oceny zabezpieczeń prywatności, organizacje mogą zdecydować bez uszczerbku, że lepszym sposobem działania jest oczekiwanie na ocenę ryzyka w celu nadania priorytetu działaniom naprawczym.

w porozumieniu z wyznaczonym personelem organizacyjnym, mogą zdecydować, że niektóre wyniki oceny oznaczone jako inne niż zadowalające, mają charakter nieistotny i nie stanowią istotnego ryzyka dla organizacji. Z drugiej strony, właściciele systemów informacyjnych lub dostawcy zabezpieczeń wspólnych, mogą zdecydować, że niektóre ustalenia oceny oznaczone, jako *niesatysfakcjonujące*, są istotne i wymagają natychmiastowych działań naprawczych. We wszystkich przypadkach organizacja dokonuje przeglądu każdego ustalenia osoby oceniającej, które nie zostało uznane za *satysfakcjonujące*, i stosuje swoją ocenę w odniesieniu do jego wagi lub powagi oraz tego, czy ustalenie jest wystarczająco istotne i zasługuje na dalsze zbadanie lub podjęcie działań naprawczych[40].

Zaangażowanie kadry kierowniczej wyższego szczebla w proces ograniczania skutków, może być konieczne w celu zapewnienia, że zasoby organizacji są efektywnie przydzielane zgodnie z priorytetami organizacji, zapewniając najpierw zasoby w systemach informacyjnych, które wspierają najbardziej krytyczne i wrażliwe misje organizacji lub korygując braki, które stwarzają największe ryzyko. Ostatecznie, wyniki oceny i wszelkie późniejsze działania ograniczające (oparte na uaktualnionej ocenie ryzyka), zainicjowane przez właścicieli systemów informacyjnych lub dostawców zabezpieczeń wspólnych we współpracy z wyznaczonym personelem organizacyjnym, powodują aktualizację kluczowych dokumentów wykorzystywanych przez upoważniony personel do określenia statusu bezpieczeństwa lub prywatności w systemie informacyjnym i jego przydatności do działania. Dokumenty te obejmują plany bezpieczeństwa i plany ochrony prywatności, raporty z oceny bezpieczeństwa i raporty z oceny prywatności oraz odpowiednie plany i etapy działań.

[40] Potencjalne działania w zakresie reagowania na ryzyko obejmują akceptację ryzyka, ograniczanie ryzyka, odrzucenie ryzyka oraz przeniesienie/podział ryzyka. Publikacja NIST SP 800-39 zawiera wytyczne dotyczące działań w zakresie reagowania na ryzyko z perspektywy zarządzania ryzykiem.

3.5. OCENA WYDAJNOŚCI ŚRODKÓW BEZPIECZEŃSTWA

Zgodnie ze standardem NSC 800-53 wer. 1, organizacje mogą zdefiniować zestaw zdolności w zakresie zapewnienia bezpieczeństwa lub ochrony prywatności, jako prekursora procesu środków bezpieczeństwa lub ochrony prywatności.

W pojęciu *zdolność*[41] przyjmuje się, że ochrona informacji przetwarzanych, przechowywanych lub przesyłanych przez systemy informacyjne, zazwyczaj nie wynika z jednego zabezpieczenia lub środka zaradczego. W większości przypadków ochrona taka wynika z wyboru i wdrożenia zestawu wzajemnie wzmacniających się środków bezpieczeństwa i ochrony prywatności. Każde zabezpieczenie przyczynia się do osiągnięcia ogólnej zdolności zdefiniowanej przez organizację - przy czym niektóre zabezpieczenia potencjalnie przyczyniają się w większym, a inne w mniejszym stopniu do osiągnięcia tej zdolności. Na przykład, organizacje mogą chcieć zdefiniować zdolność do bezpiecznego uwierzytelniania zdalnego. Zdolność tę można osiągnąć poprzez wdrożenie zestawu środków bezpieczeństwa ze standardu NSC 800-53 wer. 1 (tj. IA-2[1], IA-2[2], IA-2[8], IA-2[9] i SC-8[1]).

Zdolność do ochrony lub zdolność do ochrony prywatności mogą dotyczyć różnych obszarów, które mogą obejmować środki techniczne, środki fizyczne, środki proceduralne lub dowolną ich kombinację. Stosując koncepcję *zdolności*, organizacje mogą uzyskać większą przejrzystość i lepsze zrozumienie: (I) związków (tj. zależności) między zabezpieczeniami; (II) skutków specyficznych niepowodzeń (niewydolności) w zakresie zabezpieczeń zdolności określonych przez organizację; oraz (III) potencjalnej wagi słabości lub braków w zakresie zabezpieczeń. Podejście to może jednak zwiększyć złożoność ocen i spowodować konieczność przeprowadzenia analizy

[41] *Zdolność do osiągnięcia bezpieczeństwa* lub *zdolność do ochrony prywatności* jest połączeniem wzajemnie wzmacniających się środków bezpieczeństwa lub ochrony prywatności (tj. zabezpieczeń i środków zaradczych) wdrażanych za pomocą środków technicznych (tj. funkcjonalności sprzętu, aplikacji i oprogramowania układowego), środków fizycznych (tj. urządzeń fizycznych i środków ochronnych) oraz środków proceduralnych (tj. procedur wykonywanych przez osoby fizyczne).

pierwotnej przyczyny niepowodzenia w przypadku, gdy określone zdolności są dotknięte niepowodzeniem w zakresie środków bezpieczeństwa lub ochrony prywatności w celu ustalenia, które zabezpieczenie lub zabezpieczenia przyczyniają się do tego niepowodzenia. Im większa jest liczba zabezpieczeń wchodzących w skład zdolności określonej przez organizację, tym trudniejsze może być ustalenie pierwotnej przyczyny niepowodzenia. Mogą również występować interakcje pomiędzy zdefiniowanymi zdolnościami, które mogą przyczyniać się do złożoności ocen. Jeśli okaże się, że zabezpieczenie nie przyczynia się do zdefiniowanej zdolności ani do ogólnego bezpieczeństwa systemu, organizacja wraca do etapu 2 ram zarządzania ryzykiem RMF (patrz: NSC 800-37), dostosowując zestaw zabezpieczeń i dokumentując uzasadnienie w bezpieczeństwie planu.

Tradycyjnie, oceny były przeprowadzane na zasadzie "zabezpieczenie po zabezpieczeniu" i dawały wyniki, które były określane, jako pozytywne (tzn. zabezpieczenie satysfakcjonujące) lub negatywne (tzn. zabezpieczenie niesatysfakcjonujące). Jednakże niepowodzenie (niewydolność) pojedynczego zabezpieczenia lub w niektórych przypadkach niewydolność wielu zabezpieczeń, może nie mieć wpływu na ogólne zdolności w zakresie bezpieczeństwa lub ochrony prywatności wymagane przez organizację. Nie oznacza to, że takie zabezpieczenia nie przyczyniają się do bezpieczeństwa lub ochrony prywatności w systemie i/lub organizacji (określonych przez wymogi bezpieczeństwa i ochrony prywatności w fazie początkowej cyklu życia systemu), ale raczej, że takie zabezpieczenia mogą nie wspierać konkretnej zdolności w zakresie bezpieczeństwa lub ochrony prywatności. Co więcej, każdy wdrożony środek bezpieczeństwa lub ochrony prywatności niekoniecznie musi obsługiwać lub nie musi obsługiwać zdolności określonej przez organizację.

Jeżeli organizacje stosują *koncepcję zdolności*, zarówno oceny zautomatyzowane, jak i ręczne uwzględniają wszystkie środki bezpieczeństwa i ochrony prywatności, które obejmują zdolności w zakresie bezpieczeństwa lub ochrony prywatności. Oceniający są świadomi tego, w jaki sposób zabezpieczenia te współdziałają ze sobą, aby zapewnić

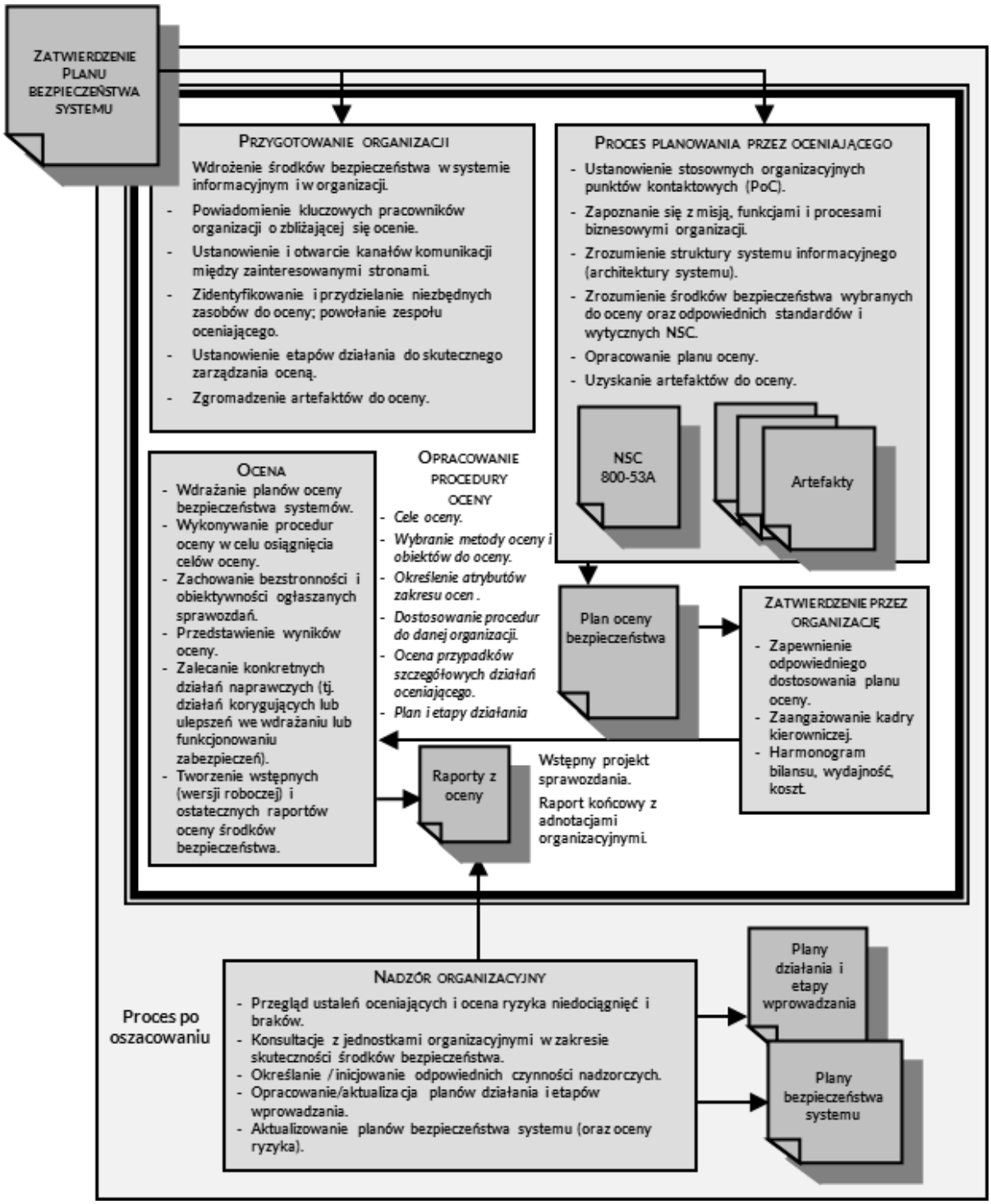
takie zdolności. W ten sposób, gdy ocena zidentyfikuje niepowodzenie zdolności, można przeprowadzić analizę pierwotnej przyczyny w celu określenia konkretnego zabezpieczenia lub zabezpieczeń, które są odpowiedzialne za niewydolność, w oparciu o ustalone relacje między zabezpieczeniami. Ponadto, zastosowanie szerszej konstrukcji zdolności pozwala organizacjom na ocenę ważności luk wykrytych w ich systemach i organizacjach oraz określenie, czy niepowodzenie określonego środka bezpieczeństwa lub ochrony prywatności (związane z luką) lub decyzja o niestosowaniu określonego zabezpieczenia podczas wstępnego procesu dostosowywania (krok RMF - Wybór), wpływa na ogólną zdolność niezbędną do ochrony misji/biznesu. Na przykład, niepowodzenie środków bezpieczeństwa uznanych za krytyczną dla danej zdolności w zakresie ochrony, może zostać przypisane, jako wyższej rangi niż niepowodzenie zabezpieczenia o mniejszym znaczeniu dla zdolności.

Ostatecznie decyzje autoryzacyjne (tj. decyzje dotyczące akceptacji ryzyka) są podejmowane w oparciu o stopień, w jakim pożądane zdolności w zakresie bezpieczeństwa i ochrony prywatności zostały skutecznie osiągnięte i spełniają wymogi bezpieczeństwa i prywatności określone przez organizację. Te oparte na ryzyku decyzje są bezpośrednio związane z tolerancją ryzyka organizacji, która jest zdefiniowana, jako część strategii zarządzania ryzykiem organizacji.

OCENY OPARTE NA ZDOLNOŚCIACH

Grupowanie zabezpieczeń z uwagi na możliwości w zakresie bezpieczeństwa i ochrony prywatności wymaga przeprowadzenia analizy przyczyn źródłowych w celu ustalenia, czy niepowodzenie danej zdolności w zakresie bezpieczeństwa lub ochrony prywatności można przypisać niepowodzeniu jednego lub większej liczby środków bezpieczeństwa lub ochrony prywatności w oparciu o ustalone relacje między zabezpieczeniami. Struktura procedur oceny zawartej w niniejszej publikacji, wraz z dekompozycją na poziomie symbolicznym i oznaczeniem celów oceny związanych z konkretną treścią środka bezpieczeństwa i ochrony prywatności, wspiera analizę głównych przyczyn niepowodzeń. Dlatego też oceny środków bezpieczeństwa i ochrony prywatności (określone jako część zdolności) mogą być dostosowane w oparciu o wytyczne zawarte w sekcji 3.2.3 standardu NIST SP 800 137 w celu określenia nakładów na zasoby (np. częstotliwość i poziom wysiłku) związanych z takimi ocenami. Ta dodatkowa precyzja w ocenach ma zasadnicze znaczenie dla wsparcia strategii ciągłego monitorowania opracowanych przez organizacje i bieżących decyzji zatwierdzających podejmowanych przez kadrę kierowniczą.

Rysunek 1 podsumowuje proces środków bezpieczeństwa i ochrony prywatności, w tym działania prowadzone podczas oceny wstępnej, oceny bieżącej i oceny końcowej.



Rysunek 1. Przegląd procesu oceny środków bezpieczeństwa i ochrony prywatności.

ZAŁĄCZNIK A - REFERENCJE

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[42]	
NSC 199	Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199
NSC 200	Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych – na podstawie FIPS 200
NSC 500-292	Architektura referencyjna chmury obliczeniowej - rekomendacje
NSC 800-18	Przewodnik do opracowywania planów bezpieczeństwa systemów informacyjnych 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 informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu – na podstawie NIST SP 800-37
NSC 800-39	Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego – na podstawie NIST SP 800-39

[42] Narodowe Standardy Cyberbezpieczeństwa - Baza wiedzy - Portal Gov.pl (www.gov.pl)

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[42]	
NSC 800-53	Zabezpieczenia i ochrona prywatności w systemach informacyjnych oraz organizacjach – na podstawie NIST SP 800-53
NSC 800-53B	Zabezpieczenia bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B
NSC 800-53 MAP	Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 Patrz: SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)
NSC 800-60	Wytyczne w zakresie określania kategorii bezpieczeństwa informacji I kategorii bezpieczeństwa systemu informacyjnego – na podstawie NIST SP 800-60
NSC 800-61	Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego – na podstawie NIST SP 800-61

PUBLIKACJE ANGLOJĘZYCZNE[43]

Dokumenty legislacyjne

1. E-Government Act [includes FISMA] (P.L. 107-347), December 2002. http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf (accessed 12/4/14).
2. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002. http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf (accessed 12/4/14).
3. Privacy Act of 1974 (P.L. 93-579), December 1974. http://www.justice.gov/opcl/privacy-act-1974 (accessed 12/4/14).

Zarządzenia, dyrektywy, rekomendacje

1. Committee on National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, April 2010. https://www.cnss.gov/CNSS/issuances/Instructions.cfm (accessed 12/4/14).
2. Committee on National Security Systems (CNSS) Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, March 2014. https://www.cnss.gov/CNSS/issuances/Instructions.cfm (accessed 12/4/14).
3. Office of Management and Budget, Circular A-130, Appendix I, Transmittal Memorandum #4, *Federal Agency Responsibilities for Maintaining Records About Individual*, November 2000. http://www.whitehouse.gov/omb/circulars_a130_a130appendix_i (accessed 12/4/14).

[43] Publikacje anglojęzyczne zostały podane w celach uzupełniających dla osób zainteresowanych.

4. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.

   http://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii (accessed 12/4/14).

5. Office of Management and Budget Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 2001.

   http://www.whitehouse.gov/omb/memoranda_m02-01 (accessed 12/4/14).

Standardy

1. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

   http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf (accessed 12/4/14).

2. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

   http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf (accessed 12/4/14).

3. ISO/IEC 15408, *Common Criteria for Information Technology Security Evaluation*, (as amended).

Przewodniki

1. National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

   http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf (accessed 12/4/14).

2. National Institute of Standards and Technology Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*, September 2012.

   http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf (accessed 12/4/14).

3. National Institute of Standards and Technology Special Publication 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010.

   http://dx.doi.org/10.6028/NIST.SP.800-37r1.

4. National Institute of Standards and Technology Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011.

   http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf (accessed 12/4/14).

5. National Institute of Standards and Technology Special Publication 800-40, Revision 3, Guide to Enterprise Patch Management Technologies, July 2013.

   http://dx.doi.org/10.6028/NIST.SP.800-40r3.

6. National Institute of Standards and Technology Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

http://dx.doi.org/10.6028/NIST.SP.800-53r4.

7. National Institute of Standards and Technology Special Publication 800-59, Guideline for Identifying an Information System as a National Security System, August 2003.

http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf (accessed 12/4/14).

8. National Institute of Standards and Technology Special Publication 800-60, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008.

http://csrc.nist.gov/publications/PubsSPs.html#800-60 (accessed 12/4/14).

9. National Institute of Standards and Technology Special Publication 800-64, Revision 2, Security Considerations in the System Development Life Cycle, October 2008.

http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf (accessed 12/4/14).

10. National Institute of Standards and Technology Special Publication 800-115, Technical Guide to Information Security Testing and Assessment, September 2008.

http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf (accessed 12/4/14).

11. National Institute of Standards and Technology Special Publication 800-126, Revision 2, The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2, September 2011.

http://csrc.nist.gov/publications/nistpubs/800-126-rev2/SP800-126r2.pdf

12. National Institute of Standards and Technology Special Publication 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations, September 2011.

http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf (accessed 12/4/14).

ZAŁĄCZNIK B - SŁOWNIK

PATRZ: NSC 7298, *SŁOWNIK KLUCZOWYCH POJĘĆ Z ZASIĘGU CYBERBEZPIECZEŃSTWA*

ZAŁĄCZNIK C - AKRONIMY

PATRZ: NSC 7298, *SŁOWNIK KLUCZOWYCH POJĘĆ Z ZASIĘGU CYBERBEZPIECZEŃSTWA*

ZAŁĄCZNIK D - OPIS METOD OCENY

DEFINICJE METOD OCENY, OBIEKTÓW I ATRYBUTÓW

Niniejszy załącznik określa trzy metody oceny, które mogą być stosowane przez osoby oceniające podczas oceny środków bezpieczeństwa i ochrony prywatności: (I) badanie; (II) rozmowa kwalifikacyjna/wywiad; oraz (III) test. Definicja każdej metody oceny obejmuje rodzaje obiektów, do których można zastosować daną metodę. Zastosowanie każdej metody oceny jest opisane pod względem *atrybutów szczegółowości* i *zasięgu*, od *podstawowego* poprzez *szczegółowy* do *kompleksowego*. Wartości tych atrybutów korelują z wymaganiami dotyczącymi wiarygodności/gwarancji określonymi przez organizację[44].

Atrybut szczegółowości odnosi się do rygoru i poziomu dokładności oceny. W przypadku atrybutu szczegółowości, *szczegółowa* wartość atrybutu obejmuje i opiera się na rygorze oceny i poziomie szczegółowości zdefiniowanym dla podstawowej wartości atrybutu; *kompleksowa* wartość atrybutu obejmuje i opiera się na rygorze oceny i poziomie szczegółowości zdefiniowanym dla *ukierunkowanej* wartości atrybutu.

Atrybut zasięgu odnosi się do zasięgu lub zakresu stosowania oceny. W przypadku *atrybutu zasięgu*, wartość atrybutu *szczegółowego* obejmuje i opiera się na liczbie i rodzajach obiektów oceny określonych dla wartości atrybutu *podstawowego*; wartość atrybutu *kompleksowego* obejmuje i opiera się na liczbie i rodzaju obiektów oceny określonych dla wartości atrybutu *szczegółowego*.

Zastosowanie pogrubionego tekstu w opisie metody oceny wskazuje na treść dodaną i pojawiającą się po raz pierwszy; wskazuje na większy rygor i poziom szczegółowości dla danej wartości atrybutu.

[44] W przypadku innych niż krajowe systemy bezpieczeństwa, organizacje powinny spełniać minimalne wymagania w zakresie zapewnienia bezpieczeństwa określone w publikacji specjalnej NIST SP 800-53 rev. 4, Appendix E.

METODA OCENY: Badanie

OBIEKTY OCENY: Specyfikacje (np. polityki, plany, procedury, wymagania systemowe, projekty).

Mechanizmy (np. funkcjonalność zaimplementowana w sprzęcie, oprogramowaniu, oprogramowaniu sprzętowym).

Działania (np. eksploatacja systemu, administracja, zarządzanie, ćwiczenia).

DEFINICJA: Proces sprawdzania, inspekcji, przeglądu, obserwacji, badania lub analizy jednego lub więcej obiektów oceny w celu ułatwienia zrozumienia, osiągnięcia wyjaśnienia lub uzyskania dowodów, których wyniki są wykorzystywane do określenia istnienia środków bezpieczeństwa i ochrony prywatności, funkcjonalności, poprawności, kompletności i zdolności poprawy w czasie.

WYTYCZNE UZUPEŁNIAJĄCE: Typowe działania oceniające mogą obejmować na przykład: przegląd polityki, planów i procedur w zakresie bezpieczeństwa informacji; analizę dokumentacji projektowej systemu i specyfikacji interfejsów; obserwację operacji tworzenia kopii zapasowych systemu, przegląd wyników ćwiczeń z planu awaryjnego; obserwację działań w zakresie reagowania na incydenty; badanie dokumentacji technicznej i instrukcji dla użytkowników/administratorów; sprawdzanie, badanie lub obserwację działania mechanizmu informatycznego w sprzęcie/oprogramowaniu systemu informacyjnego; lub sprawdzanie, badanie lub obserwację środków bezpieczeństwa fizycznego związanych z działaniem systemu informacyjnego.

Narzędzia oceny SCAP wspierające specyfikację komponentów OCIL, mogą być wykorzystywane do automatyzacji zbierania obiektów oceny od konkretnych, odpowiedzialnych osób w organizacji. Uzyskane w ten sposób informacje mogą być następnie sprawdzane przez osoby oceniające podczas oceny bezpieczeństwa i ochrony prywatności.

ATRYBUTY: Szczegółowość, Zasięg (zakres stosowania)

- *Atrybut szczegółowości odnosi się do rygoru i poziomu szczegółowości w procesie badania. Istnieją trzy możliwe wartości dla atrybutu szczegółowości badania: (I) podstawowe; (II) szczegółowe; oraz (III) kompleksowe.*

  ✓ Badanie podstawowe: Badanie składające się z przeglądów, badań kontrolnych, obserwacji lub inspekcji obiektu oceny przeprowadzanych na wysokim poziomie. Ten rodzaj badania przeprowadzany jest z wykorzystaniem ograniczonego materiału dowodowego lub dokumentacji (np. opisy mechanizmów na poziomie funkcjonalnym; opisy procesów na wysokim poziomie działań; aktualne dokumenty ze specyfikacjami). Badania podstawowe zapewniają poziom zrozumienia środków bezpieczeństwa i ochrony prywatności niezbędny do określenia, czy zabezpieczenia te są realizowane i wolne od oczywistych błędów.

  ✓ Badanie szczegółowe: Badanie składające się z wysokiego poziomu przeglądów, badań kontrolnych, obserwacji lub inspekcji oraz **bardziej szczegółowych badań/analiz** przedmiotu oceny. Ten rodzaj badania jest przeprowadzany z wykorzystaniem istotnego materiału dowodowego lub dokumentacji (np. opisy na poziomie funkcjonalnym oraz, w **stosownych przypadkach i jeżeli są one dostępne, informacje na temat projektowania mechanizmów wysokiego poziomu; wysokiego poziomu opisy procesów i procedury wdrażania działań**; aktualne dokumenty i dokumenty **związane ze specyfikacjami**). Badania szczegółowe zapewniają poziom zrozumienia środków bezpieczeństwa i ochrony prywatności niezbędny do określenia, czy zabezpieczenia są realizowane i nie posiadają oczywistych błędów **oraz czy istnieją zwiększone podstawy zaufania do prawidłowo realizowanych i działających zgodnie z założeniami zabezpieczeń**.

  ✓ Badanie kompleksowe: Badanie, na które składają się wysokiego poziomu przeglądy, badania kontrolne, obserwacje lub inspekcje oraz bardziej szczegółowe, **gruntowe** i **dogłębne** badania/analizy przedmiotu oceny. Ten

rodzaj badania jest przeprowadzany z wykorzystaniem **szczegółowego** materiału dowodowego lub dokumentacji (np. opisy na poziomie funkcjonalnym oraz, w stosownych przypadkach i jeżeli są dostępne, informacje na temat projektu wysokiego poziomu, informacje na temat projektu **niskiego poziomu oraz informacje dotyczące wdrażania** mechanizmów; opisy procesów wysokiego poziomu i szczegółowe procedury wdrażania działań; faktyczne dokumenty i związane z nimi dokumenty dotyczące specyfikacji[45]). Badania kompleksowe zapewniają poziom zrozumienia środków bezpieczeństwa i ochrony prywatności niezbędny do określenia, czy zabezpieczenia są przeprowadzane i wolne od oczywistych błędów, oraz czy istnieją **dalsze** zwiększone podstawy zaufania, że zabezpieczenia są zaimplementowane prawidłowo i działają zgodnie z **założeniami na bieżąco i spójnie oraz, że istnieje wsparcie dla ciągłej poprawy skuteczności zabezpieczeń**.

- *Atrybut zasięgu (zakresu stosowania) odnosi się do zasięgu lub rozległości stosowania procesu badania i obejmuje rodzaje przedmiotów oceny, które mają zostać zbadane, liczbę przedmiotów, które mają zostać zbadane (według rodzaju) oraz konkretne przedmioty, które mają zostać zbadane[46]. Istnieją trzy możliwe wartości dla atrybutu zasięgu: (I) podstawowy; (II) szczegółowy; oraz (III) kompleksowy.*

  ✓ Badanie podstawowe: Badanie, które wykorzystuje reprezentatywną próbkę obiektów oceny (według typu i liczby w ramach typu) w celu zapewnienia poziomu zasięgu stosowania niezbędnego do określenia, czy środki

[45] Podczas gdy dodatkowa dokumentacja jest wymagana w przypadku mechanizmów przejścia od badań podstawowych, poprzez szczegółowe, do kompleksowych, dokumentacja dotycząca specyfikacji i działań może być taka sama lub podobna w przypadku badań szczegółowych i kompleksowych, przy czym rygor badań tych dokumentów wzrasta na poziomie kompleksowym.

[46] Organizacja, biorąc pod uwagę różne czynniki (np. dostępne zasoby, znaczenie oceny, ogólne cele i zadania oceny organizacji), uzgadnia z oceniającym i nadaje kierunek rodzajowi, liczbie i określonym obiektom, które mają być zbadane pod kątem wartości konkretnego atrybutu.

bezpieczeństwa i ochrony prywatności są zaimplementowane i wolne od oczywistych błędów.

- ✓ Badanie szczegółowe: Badanie, w którym wykorzystuje się reprezentatywną próbę ocenianych przedmiotów (według rodzaju i liczby w ramach rodzaju) **oraz innych ocenianych przedmiotów uznanych za szczególnie ważne dla osiągnięcia celu oceny**, w celu zapewnienia poziomu zakresu stosowania niezbędnego do ustalenia, czy środki w zakresie bezpieczeństwa i ochrony prywatności są wdrożone i wolne od oczywistych błędów **oraz czy istnieją zwiększone podstawy pewności, że zabezpieczenia są wdrożone prawidłowo i działają zgodnie z założeniami**.
- ✓ Badanie kompleksowe: Badanie, w którym wykorzystuje się **wystarczająco dużą** próbkę przedmiotów oceny (według rodzaju i liczby w ramach rodzaju) oraz innych przedmiotów oceny szczegółowej uznanych za szczególnie ważne dla osiągnięcia celu oceny, w celu zapewnienia poziomu zakresu stosowania niezbędnego do ustalenia, czy środki w zakresie bezpieczeństwa i ochrony prywatności są wdrożone i wolne od oczywistych błędów oraz czy istnieją **dalsze** zwiększone podstawy pewności, że zabezpieczenia są przeprowadzane prawidłowo i działają zgodnie z założeniami w **sposób ciągły i spójny, a także czy istnieje wsparcie w zakresie ciągłego zwiększania skuteczności zabezpieczeń**.

METODA OCENY: Rozmowa kwalifikacyjna/wywiad

OBIEKTY OCENY: Osoby indywidualne lub grupy osób

DEFINICJA: Proces prowadzenia dyskusji z osobami lub grupami w ramach organizacji w celu ułatwienia zrozumienia, osiągnięcia wyjaśnienia lub doprowadzenia do umiejscowienia dowodów, których wyniki są wykorzystywane do wspierania istniejących środków bezpieczeństwa i ochrony prywatności, funkcjonalności, poprawności, kompletności i zdolności poprawy w czasie.

WYTYCZNE UZUPEŁNIAJĄCE: Typowe działania oceniające mogą obejmować na przykład, przeprowadzanie wywiadów z kierownikiem jednostki organizacyjnej, CIO, SAISO, osobą autoryzującą, właścicielami informacji, właścicielami systemów informacyjnych i misji, ISSO, menadżerami ds. bezpieczeństwa systemów, kierownikami ds. zasobów ludzkich, kierownikami obiektów, personelem ds. szkoleń, operatorami systemów informacyjnych, administratorami sieci i systemów, personelem ds. bezpieczeństwa fizycznego i użytkownikami.

Narzędzia zatwierdzone przez SCAP, które obsługują specyfikację komponentów OCIL, mogą być wykorzystywane do zautomatyzowania procesu wywiadu dla konkretnych osób lub grup osób. Uzyskane w ten sposób informacje mogą być następnie sprawdzane przez osoby oceniające podczas oceny bezpieczeństwa i ochrony prywatności.

ATRYBUTY: Szczegółowość, Zasięg (zakres stosowania)

- *Atrybut szczegółowości odnosi się do rygoru i poziomu szczegółowości w procesie wywiadu. Istnieją trzy możliwe wartości atrybutu szczegółowości wywiadu: (I) podstawowy; (II) szczegółowy; oraz (III) kompleksowy.*
  - ✓ Wywiad podstawowy: Wywiad z osobami lub grupami osób, polegający na szeroko zakrojonych rozmowach na poziomie ogólnym. Ten rodzaj wywiadu jest prowadzony z wykorzystaniem zestawu uogólnionych pytań wysokiego poziomu. Wywiady podstawowe zapewniają poziom zrozumienia środków

bezpieczeństwa i ochrony prywatności niezbędny do ustalenia, czy zabezpieczenia te są wdrożone i wolne od oczywistych błędów.

- ✓ Wywiad szczegółowy: Wywiad z osobami lub grupami osób, który składa się z szeroko zakrojonych dyskusji na poziomie ogólnym oraz **bardziej dogłębnych dyskusji w określonych obszarach**. Ten rodzaj wywiadu jest prowadzony z wykorzystaniem zestawu uogólnionych pytań **oraz bardziej dogłębnych pytań w określonych obszarach, w przypadku których odpowiedzi wskazują na potrzebę bardziej dogłębnego zbadania sprawy**. Wywiady szczegółowe zapewniają poziom zrozumienia środków bezpieczeństwa i ochrony prywatności niezbędny do ustalenia, czy zabezpieczenia są przeprowadzane i wolne od oczywistych błędów **oraz czy istnieją większe podstawy do pewności, że zabezpieczenia są przeprowadzane prawidłowo i działają zgodnie z założeniami**.
- ✓ Wywiad kompleksowy: Wywiad z osobami lub grupami osób, który składa się z szeroko zakrojonych dyskusji na poziomie ogólnym oraz bardziej dogłębnych, **sondażowych** dyskusji w określonych obszarach. Ten rodzaj wywiadu jest prowadzony z wykorzystaniem zestawu uogólnionych pytań oraz bardziej dogłębnych, **sondażowych** pytań w określonych obszarach, w których odpowiedzi wskazują na potrzebę bardziej dogłębnego zbadania. Wywiady kompleksowe zapewniają poziom zrozumienia środków bezpieczeństwa i ochrony prywatności niezbędny do określenia, czy zabezpieczenia są przeprowadzane i wolne od oczywistych błędów, oraz czy istnieją **dodatkowe** podstawy do przekonania, że zabezpieczenia są przeprowadzane prawidłowo i działają zgodnie z założeniami **na bieżąco i konsekwentnie oraz że istnieje wsparcie dla ciągłej poprawy skuteczności zabezpieczeń.**

- *Atrybut zasięgu (zakresu stosowania) odnosi się do zasięgu lub rozległości stosowania procesu przeprowadzania rozmów i obejmuje kategorie osób, z którymi przeprowadza się rozmowy (według roli organizacyjnej i związanej z nią odpowiedzialności), liczbę osób, z którymi przeprowadza się rozmowy (według rodzaju) oraz konkretne osoby,*

z którymi przeprowadza się rozmowy[47]*. Istnieją trzy możliwe wartości dla atrybutu zasięgu: (I) podstawowa; (II) szczegółowa; oraz (III) kompleksowa.*

- ✓ Wywiad podstawowy: Wywiad, w którym wykorzystuje się reprezentatywną próbkę osób pełniących kluczowe funkcje organizacyjne, aby zapewnić poziom zakresu stosowania niezbędny do ustalenia, czy środki bezpieczeństwa i ochrony prywatności są wdrożone i wolne od oczywistych błędów.
- ✓ Wywiad szczegółowy: Wywiad, w którym wykorzystuje się reprezentatywną próbkę osób pełniących kluczowe role w organizacji **oraz innych konkretnych osób uważanych za szczególnie ważne dla osiągnięcia celu oceny, w celu zapewnienia odpowiedniego zasięgu niezbędnego do ustalenia**, czy zabezpieczenia w zakresie bezpieczeństwa i ochrony prywatności są wdrożone i wolne od oczywistych błędów **oraz czy istnieją zwiększone podstawy pewności, że zabezpieczenia są wdrożone prawidłowo i działają zgodnie z założeniami**.
- ✓ Wywiad kompleksowy: Wywiad, w którym wykorzystuje się **dostatecznie dużą próbkę** osób pełniących kluczowe funkcje w organizacji oraz innych konkretnych osób uznanych za szczególnie ważne dla osiągnięcia celu oceny, aby zapewnić zakres niezbędny do ustalenia, czy zabezpieczenia w zakresie bezpieczeństwa i ochrony prywatności są wdrożone i wolne od oczywistych błędów oraz czy istnieją **dodatkowe** podstawy do uzyskania pewności, że zabezpieczenia są przeprowadzane prawidłowo i działają zgodnie z założeniami w **sposób ciągły i spójny oraz, że istnieje wsparcie dla ciągłej poprawy skuteczności zabezpieczeń**.

[47] Organizacja, biorąc pod uwagę różne czynniki (np. dostępne zasoby, znaczenie oceny, ogólne cele i zadania organizacji w zakresie oceny), uzgadnia z oceniającymi i ukierunkowuje ich na status, liczbę i konkretne osoby, z którymi należy przeprowadzić rozmowę w odniesieniu do danej wartości opisywanego atrybutu.

METODA OCENY: Test

OBIEKTY OCENY: Mechanizmy (np. sprzęt, aplikacje, oprogramowanie układowe)

Działania (np. eksploatacja systemu; administracja; zarządzanie; ćwiczenia).

DEFINICJA: Proces wykonywania jednej lub większej liczby oceny obiektów w określonych warunkach w celu porównania zachowań rzeczywistych z oczekiwanymi, których wyniki są wykorzystywane do określenia istnienia środków bezpieczeństwa i ochrony prywatności, funkcjonalności, poprawności, kompletności i zdolności poprawy w czasie[48].

WYTYCZNE UZUPEŁNIAJĄCE: Typowe działania osoby oceniającej mogą obejmować na przykład: testowanie kontroli dostępu, identyfikacji i uwierzytelniania oraz mechanizmów audytu; testowanie bezpieczeństwa konfiguracji ustawień; testowanie fizycznych urządzeń kontroli dostępu; przeprowadzanie testów penetracyjnych kluczowych komponentów systemu informacyjnego; testowanie działania tworzenia kopii zapasowej systemu informacyjnego; testowanie zdolności do reagowania na incydenty; oraz ćwiczenia wydajności planowania awaryjnego. Narzędzia zatwierdzone przez SCAP mogą być wykorzystywane do automatyzacji zbierania obiektów oceny i oceny tych obiektów pod kątem oczekiwanego zachowania. Wykorzystanie SCAP jest szczególnie istotne w przypadku testowania mechanizmów, które wiążą się z oceną rzeczywistego stanu urządzenia.

[48] Testowanie jest zazwyczaj stosowane w celu określenia, czy mechanizmy lub działania spełniają zestaw uprzednio zdefiniowanych specyfikacji. Testy mogą być również przeprowadzane w celu określenia właściwości środków bezpieczeństwa lub ochrony prywatności, które nie są powszechnie kojarzone z wcześniej zdefiniowanymi specyfikacjami, przy czym przykładem takich testów są testy penetracyjne. Rekomendacje dotyczące przeprowadzania badań penetracyjnych znajdują się w załączniku E.

National Checklist Program[49] kataloguje szereg list kontrolnych z obsługą SCAP, które są odpowiednie do oceny postawy konfiguracyjnej określonych systemów operacyjnych i aplikacji. Ocenione przez SCAP narzędzia mogą wykorzystywać te listy kontrolne w celu określenia ogólnej zgodności systemu ze wszystkimi ustawieniami konfiguracji w liście kontrolnej (np. zabezpieczenie CM-6) lub określonymi konfiguracjami, które są istotne dla środków bezpieczeństwa lub ochrony prywatności, które odnoszą się do jednego lub większej liczby ustawień konfiguracyjnych. Narzędzia zatwierdzone przez SCAP mogą również określać brak poprawki lub obecność stanu zagrożenia. Wyniki uzyskane za pomocą narzędzi SCAP mogą być następnie badane przez osoby oceniające w ramach oceny środków bezpieczeństwa i ochrony prywatności.

ATRYBUTY: Szczegółowość, Zasięg (zakres stosowania)

- *Atrybut szczegółowości odnosi się do typu testu, który ma zostać przeprowadzony. Istnieją trzy możliwe wartości atrybutu szczegółowości testu: (I) podstawowy; (II) szczegółowy; oraz (III) kompleksowy.*

  ✓ Testowanie podstawowe: Metodologia testów {znana jako testowanie „czarnej skrzynki" (*ang. black box testing*)}, która zakłada brak znajomości wewnętrznej struktury i szczegółów realizacji przedmiotu oceny. Ten rodzaj testowania jest przeprowadzany z wykorzystaniem specyfikacji funkcjonalnej mechanizmów i opisu procesu na wysokim poziomie działań[50]. Testowanie podstawowe zapewnia poziom zrozumienia środków bezpieczeństwa i ochrony prywatności niezbędny do określenia, czy zabezpieczenia te są wdrożone i wolne od oczywistych błędów.

[49] Patrz: National Checklist Program | CSRC (nist.gov)

[50] Ogólny poziom funkcjonowania.

- ✓ Testowanie szczegółowe: Metodologia testowania {znana jako testowanie „szarej skrzynki" (*ang. gray box testing*)}, która zakłada **pewną** wiedzę na temat wewnętrznej struktury i szczegółów wdrożenia obiektu oceny. Ten rodzaj testowania jest przeprowadzany z wykorzystaniem specyfikacji funkcjonalnej i **ograniczonej informacji o architekturze systemu (np. projekt wysokiego poziomu)** dla mechanizmów oraz opisu procesu wysokiego poziomu i **wysokiego poziomu opisu integracji ze środowiskiem operacyjnym** działań. Testy szczegółowe zapewniają poziom zrozumienia środków bezpieczeństwa i ochrony prywatności niezbędny do określenia, czy zabezpieczenia są wdrożone i wolne od oczywistych błędów **oraz czy istnieją zwiększone podstawy zaufania, że zabezpieczenia są wdrożone prawidłowo i działają zgodnie z założeniami**.
- ✓ Testowanie kompleksowe: Metodologia testów {znana jako testowanie „białej skrzynki" (*ang. white box testing*)}, która zakłada **wyraźną i istotną** wiedzę na temat wewnętrznej struktury i szczegółów wdrożenia przedmiotu oceny. Ten rodzaj testowania przeprowadzany jest z wykorzystaniem specyfikacji funkcjonalnej, **obszernej** informacji o architekturze systemu (np. projekt wysokiego poziomu, **projekt niskiego poziomu) i reprezentacji wdrożenia** (np. **kod źródłowy, schematy**) mechanizmów oraz opisu procesu wysokiego poziomu i **szczegółowego** opisu integracji ze środowiskiem operacyjnym działań. Kompleksowe testowanie zapewnia poziom zrozumienia środków bezpieczeństwa i ochrony prywatności niezbędny do określenia, czy zabezpieczenia są wdrażane i wolne od oczywistych błędów oraz czy istnieją **dalsze** zwiększone podstawy pewności, że zabezpieczenia są wdrażane prawidłowo i działają zgodnie z założeniami w **sposób ciągły i spójny oraz że istnieje wsparcie dla ciągłego zwiększania skuteczności zabezpieczeń**.

- *Atrybut zasięgu (zakresu stosowania) odnosi się do zasięgu lub rozległości stosowania procesu badania i obejmuje typy obiektów oceny, które mają być badane, liczbę*

obiektów, które mają być badane (według typu) oraz konkretne obiekty, które mają być badane[51].

Istnieją trzy możliwe wartości atrybutu zasięgu testowania: (I) podstawowy; (II) szczegółowy; oraz (III) kompleksowy.

- ✓ Testowanie podstawowe: Testowanie wykorzystujące reprezentatywną próbkę obiektów oceny (według typu i liczby w ramach typu) w celu zapewnienia poziomu zakresu stosowania niezbędnego do określenia, czy środek bezpieczeństwa i ochrony prywatności jest realizowany i wolny od oczywistych błędów.
- ✓ Testowanie szczegółowe: Testowanie wykorzystujące reprezentatywną próbkę obiektów oceny (według rodzaju i liczby w ramach rodzaju) **oraz innych ocenianych przedmiotów uważanych za szczególnie ważne dla osiągnięcia celu oceny**, z zamiarem zapewnienia zasięgu niezbędnego do ustalenia, czy zabezpieczenia w zakresie bezpieczeństwa i ochrony prywatności są wdrożone i wolne od oczywistych błędów **oraz czy istnieją zwiększone podstawy pewności, że zabezpieczenia są wdrożone prawidłowo i działają zgodnie z założeniami**.
- ✓ Testowanie kompleksowe: Testowanie wykorzystujące **wystarczająco dużą** próbkę przedmiotów oceny (według rodzaju i liczby w ramach rodzaju oraz innych ocenianych przedmiotów uważanych za szczególnie ważne dla osiągnięcia celu oceny, w celu zapewnienia poziomu zasięgu stosowania niezbędnego do ustalenia, czy środki w zakresie bezpieczeństwa i ochrony

[51] Organizacja, biorąc pod uwagę różne czynniki (np. dostępne zasoby, znaczenie oceny, ogólne cele i zadania oceny organizacji), ustala i ukierunkowuje osoby oceniające na rodzaj, liczbę i konkretne obiekty, które mają być badane pod kątem opisywanej wartości konkretnego atrybutu. W przypadku testowania związanego z mechanizmami, atrybut *zasięgu* odnosi się również do zakresu przeprowadzanych testów (np. w przypadku oprogramowania, liczby testowanych przypadków i modułów; w przypadku sprzętu, zakresu nakładów, liczby testowanych komponentów i zakresu czynników środowiskowych, w odniesieniu do których przeprowadzane są testy).

prywatności są przeprowadzane i wolne od oczywistych błędów oraz czy istnieją **dalsze** zwiększone podstawy pewności, że zabezpieczenia są przeprowadzane prawidłowo i działają zgodnie z założeniami w **sposób ciągły i spójny,** a **także czy istnieje poparcie dla ciągłej poprawy skuteczności zabezpieczeń**.

ZAŁĄCZNIK E - TESTY PENETRACYJNE

NARZĘDZIA I TECHNIKI OCENY DO IDENTYFIKOWANIA PODATNOŚCI SYSTEMU INFORMACYJNEGO

Organizacje mogą rozważyć dodanie kontrolowanych technik penetracyjnych do swojego zbioru narzędzi wykorzystywanych do oceny środków bezpieczeństwa i ochrony prywatności w systemach informacyjnych organizacji. Testy penetracyjne to specyficzny rodzaj oceny, w której osoby oceniające symulują działania danej klasy napastników za pomocą określonego zestawu dokumentacji (tj. dokumentacji reprezentatywnej dla tego, co dana klasa napastników prawdopodobnie posiada) oraz pracując w innych specyficznych warunkach, w celu próby obejścia zabezpieczeń lub ochrony prywatności w systemie informacyjnym. Testy penetracyjne, prowadzone jako kontrolowana próba naruszenia środków bezpieczeństwa i ochrony prywatności, stosowane są w systemie informacyjnym przy użyciu technik i odpowiednich narzędzi sprzętowych i programowych atakującego. Testy penetracyjne reprezentują wyniki konkretnej osoby oceniającej lub grupy oceniającej w określonym czasie, przy zastosowaniu uzgodnionych zasad zaangażowania. Biorąc pod uwagę złożoność technologii informatycznych powszechnie stosowanych obecnie przez organizacje, testy penetracyjne mogą być postrzegane nie jako sposób na weryfikację bezpieczeństwa lub ochrony prywatności w systemie informacyjnym, ale raczej jako środek w celu: (I) poprawy zrozumienia systemu przez organizację; (II) wykrycia słabych punktów lub niedociągnięć systemu; oraz (III) wskazania poziomu wysiłku wymaganego od przeciwników w celu naruszenia zabezpieczeń systemu.

Testy penetracyjne mogą być zaplanowane i/lub przypadkowe, zgodnie z przyjętą polityką organizacyjną i oceną ryzyka. Można rozważyć przeprowadzenie testów penetracyjnych: (I) w każdym nowo opracowanym systemie informacyjnym (lub starszym systemie przechodzącym poważną modernizację) przed zatwierdzeniem systemu do eksploatacji; (II) po dokonaniu istotnych zmian w środowisku, w którym działa system informacyjny; oraz (III) w przypadku wykrycia nowego rodzaju ataku,

który może mieć wpływ na system. Organizacje aktywnie monitorują środowisko systemów informacyjnych i poziom zagrożeń (np. nowe słabe punkty, techniki ataku, wdrażanie nowych technologii, świadomość i szkolenie w zakresie bezpieczeństwa użytkowników i ochrony prywatności) w celu zidentyfikowania zmian, które wymagają nieplanowanego testowania penetracyjnego.

Organizacje określają, które elementy systemu informacyjnego podlegają testowaniu penetracyjnemu oraz profil napastnika, który ma być przyjęty w trakcie ćwiczeń penetracyjnych. Organizacje szkolą wybrany personel w zakresie stosowania i obsługi narzędzi i technik stosowanych w testach penetracyjnych. Skuteczne narzędzia do testów penetracyjnych mają możliwość łatwego aktualizowania listy technik i podatności eksploatacyjnych wykorzystywanych podczas ćwiczeń. Organizacje aktualizują listę technik i użytecznych podatności stosowanych w testach penetracyjnych na podstawie oceny ryzyka organizacji lub w przypadku zidentyfikowania i zgłoszenia istotnych nowych podatności lub zagrożeń. Gdy tylko jest to możliwe, organizacje stosują zautomatyzowane narzędzia i techniki ataku, które obejmują możliwość wykonywania w systemach informacyjnych ćwiczeń z zakresu testów penetracyjnych środków bezpieczeństwa i ochrony prywatności[52].

Informacje uzyskane w ramach procesu testowania penetracyjnego mogą być udostępniane upoważnionemu personelowi w całej organizacji, aby pomóc w ustaleniu priorytetów dotyczących słabych punktów systemu informacyjnego, które w sposób oczywisty podlegają ujawnieniu przez napastników o profilu odpowiadającym profilowi wykorzystanemu w ćwiczeniach testów penetracyjnych. Ustalenie priorytetów pomaga w określeniu skutecznych strategii eliminowania zidentyfikowanych słabych punktów

[52] Pomimo, że narzędzia do zautomatyzowanego testowania penetracyjnego zapewniają powtarzalne wyniki i zmniejszają wykorzystywane zasoby, organizacje dokładnie rozważają potencjalny szkodliwy wpływ zautomatyzowanego wykorzystania na dostępność systemu podczas stosowania narzędzi do testowania penetracyjnego. Dodatkowo, testy penetracyjne oparte wyłącznie na narzędziach automatycznych mogą nie zapewniać poziomu prób naruszenia zasad ochrony, którego organizacje mogą doświadczyć od rzeczywistego atakującego.

i ograniczania związanych z nimi zagrożeń działalności i aktywów organizacji, osób fizycznych, innych organizacji oraz społeczeństwa, wynikających z działania i korzystania z systemu informacyjnego. Testy penetracyjne mogą być zintegrowane z procesem testowania bezpieczeństwa sieci oraz z procesem zarządzania łatami i podatnościami. Standard NIST SP 800-40 zawiera wskazówki dotyczące zarządzania łatami i podatnościami. Standard NIST SP 800-115 zawiera wskazówki na temat testowania bezpieczeństwa informacji i sieci.

Metody testowania penetracyjnego

Organizacje biorą pod uwagę następujące kryteria przy opracowywaniu i wdrażaniu kontrolowanego programu testowania penetracyjnego. Skuteczny test penetracyjny:

- *Wykracza poza skanowanie podatności, dostarczając wyraźnego i często mocnego dowodu na ryzyko związane z misją oraz wskaźnika poziomu wysiłku, jaki przeciwnik musiałby ponieść, aby zaszkodzić działalności i zasobom organizacji, osobom, innym organizacjom lub społeczeństwu.*
- *Podchodzi do systemu informacyjnego jak do przeciwnika, biorąc pod uwagę słabe punkty, nieprawidłowe konfiguracje systemu, relacje zaufania między organizacjami oraz słabości architektoniczne badanego środowiska.*
- *Ma jasno określony zakres i zawiera, jako minimum, definicje:*
  - ✓ środowiska podlegającego testowaniu (np. obiektów, użytkowników, grup organizacyjnych);
  - ✓ testowanej powierzchni ataku (np. serwery, systemy stacjonarne, sieci bezprzewodowe, aplikacje internetowe, systemy wykrywania i zapobiegania włamaniom, zapory ogniowe, konta pocztowe, świadomość bezpieczeństwa użytkowników i postawa szkoleniowa, postawa reagowania na incydenty);
  - ✓ źródeł zagrożeń, które mają być symulowane (np. wyliczenie profili napastników, które mają być wykorzystane: napastnik wewnętrzny, napastnik

zwykły, pojedynczy lub grupa zewnętrznych napastników, organizacja przestępcza);

- ✓ celów symulowanego napastnika (np. uzyskanie dostępu administratora domeny w strukturze LDAP (*ang. Lightweight Directory Access Protocol*) organizacji, dostęp i modyfikacja informacji w systemie finansowym organizacji);
- ✓ poziomu nakładu pracy (czasu i zasobów), który należy poświęcić; oraz
- ✓ zasad zaangażowania.

- *Dokładnie dokumentuje wszystkie czynności wykonane podczas testu, w tym wszystkie wykorzystane luki w zabezpieczeniach oraz sposób, w jaki podatności te zostały wykorzystane do ataków.*
- *Uzyskuje wyniki wskazujące na prawdopodobieństwo wystąpienia ataku, poprzez wykorzystanie poziomu wysiłku, jaki zespół musiał poświęcić na penetrację systemu informacyjnego, jako wskaźnika odporności systemu na penetrację.*
- *Zatwierdza istniejące mechanizmy środków bezpieczeństwa i ochrony prywatności (w tym mechanizmy ograniczania ryzyka, takie jak zapory ogniowe, systemy wykrywania i zapobiegania włamaniom).*
- *Dostarcza możliwy do zweryfikowania i powtarzalny rejestr wszystkich czynności wykonywanych podczas testu, oraz*
- *Dostarcza informacji o możliwych środkach zaradczych w przypadku udanych ataków.*

ZAŁĄCZNIK F - PROCEDURY OCENY BEZPIECZEŃSTWA

CELE, METODY I OBIEKTY DO OCENY ZABEZPIECZEŃ

Patrz: Załącznik F - Procedury oceny bezpieczeństwa

ZAŁĄCZNIK G - SPRAWOZDANIA Z OCENY

DOKUMENTOWANIE USTALEŃ Z OCENY ŚRODKÓW BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Podstawowym celem *raportów z oceny bezpieczeństwa i ochrony prywatności* jest przekazanie wyników oceny środków bezpieczeństwa i ochrony prywatności odpowiedniemu personelowi organizacyjnemu. Raport z oceny bezpieczeństwa zawarty jest w pakiecie autoryzacji bezpieczeństwa wraz z planem bezpieczeństwa (w tym zaktualizowaną oceną ryzyka) oraz planem i etapami działania, w celu dostarczenia upoważnionym osobom informacji niezbędnych do podjęcia, w oparciu o ryzyko, decyzji o uruchomieniu lub kontynuacji działania systemu informacyjnego. Organizacje mogą zdecydować o włączeniu podobnych artefaktów związanych z ochroną prywatności do pakietu autoryzującego do przekazywania upoważnionym osobom istotnych informacji. Wszystkie kwestie związane z przestrzeganiem przepisów, dyrektyw, rozporządzeń lub zasad dotyczących ochrony prywatności są koordynowane z osobą odpowiedzialną za ochronę prywatności (SAOP/CPO)[53]. W miarę, jak proces oceny i autoryzacji staje się coraz bardziej dynamiczny, opierając się w większym stopniu na ciągłości monitorowania aspektów procesu, jako zintegrowanej i ściśle powiązanej części cyklu życia systemu, możliwość aktualizacji raportów oceny bezpieczeństwa i ochrony prywatności staje się często krytycznym aspektem programów bezpieczeństwa informacji i ochrony prywatności.

Należy podkreślić związek, opisany w standardzie NSC 800-37, pomiędzy trzema kluczowymi dokumentami pakietu autoryzacyjnego (tj. planem bezpieczeństwa, raportem oceny bezpieczeństwa oraz planem i etapami działania). To właśnie te

[53] Ocena zgodności z obowiązującym Załącznikiem J dotyczącym ochrony prywatności, musi zostać przeprowadzona przez SAOP/CPO. Zatwierdzenie przez SAOP/CPO jest wymagane, jako warunek wstępny wydania upoważnienia do działania (*ang. authorization into operate*). Organizacje mają swobodę w określaniu odpowiedniego procesu zatwierdzania przez SAOP.

dokumenty dostarczają najbardziej wiarygodnych informacji na temat ogólnego stanu bezpieczeństwa systemu informacyjnego i zdolności systemu do ochrony w niezbędnym stopniu działalności i aktywów organizacji, osób, innych organizacji i społeczeństwa. Aktualizacje tych kluczowych dokumentów są dostarczane na bieżąco, zgodnie z ustanowionym przez organizację programem ciągłości monitorowania. Aktualizacje podobnych dokumentów związanych z ochroną prywatności odbywają się z częstotliwością i formatem określonym przez SAOP/CPO we współpracy z upoważnionymi osobami.

Sprawozdania z oceny bezpieczeństwa i ochrony prywatności zapewniają zdyscyplinowane i ustrukturyzowane podejście do dokumentowania ustaleń osoby oceniającej oraz zalecenia dotyczące skorygowania wszelkich słabych punktów lub niedociągnięć w zakresie środków bezpieczeństwa i ochrony prywatności. Niniejszy załącznik stanowi wzór do raportowania wyników ocen środków bezpieczeństwa i ochrony prywatności. Organizacje nie są ograniczone do określonego formatu szablonu; przewiduje się jednak, że ogólny raport z oceny będzie zawierał informacje podobne do tych wyszczególnionych we wzorze dla każdego ocenianego środka bezpieczeństwa i ochrony prywatności, poprzedzone podsumowaniem zawierającym wykaz wszystkich ocenionych środków bezpieczeństwa i ochrony prywatności oraz ogólny status każdego zabezpieczenia.

Kluczowe elementy sprawozdawczości z oceny

Poniższe elementy powinny być zawarte w sprawozdaniach z oceny bezpieczeństwa i ochrony prywatności[54]:

- *nazwa systemu informacyjnego;*

[54] Informacje dostępne w innych kluczowych dokumentach organizacyjnych (np. planach bezpieczeństwa lub ochrony prywatności, ocenach ryzyka, planach i etapach działań lub planach oceny bezpieczeństwa lub ochrony prywatności) nie muszą być powielane w raportach z oceny bezpieczeństwa i ochrony prywatności.

- *kategoryzacja bezpieczeństwa;*
- *strona(y) poddana(e) ocenie i data(y) oceny;*
- *nazwa/identyfikacja osoby oceniającej;*
- *poprzednie wyniki oceny (w przypadku ponownego wykorzystania);*
- *planowane do oceny środki bezpieczeństwa/ochrony prywatności lub zabezpieczenia rozszerzone;*
- *wybrane metody i obiekty oceny;*
- *wartości atrybutów szczegółowości i zasięgu;*
- *podsumowanie wyników oceny (wskazujące na satysfakcjonujące (S) lub niesatysfakcjonujące (N);*
- *komentarze oceniającego (stwierdzone słabe punkty lub braki); oraz*
- *zalecenia oceniającego (priorytety, korekty, działania naprawcze lub ulepszenia).*

Ustalenia z oceny

Każdy zestaw instrukcji wykonywany przez osobę oceniającą prowadzi do jednego z poniższych wniosków: (I) *satysfakcjonujące* (S); lub (II) *niesatysfakcjonujące* (N). Jako przykład, weźmy pod uwagę następujące środki bezpieczeństwa CP-2(3). Oceniający przeprowadza procedurę oceny dla CP-2(3) i formułuje następujące ustalenia: (I) spełnia wymagania (S); lub (II) nie spełnia wymagań (N):

CP-3 SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA	
	CEL OCENY: *Ustalenie, czy organizacja zapewnia użytkownikom systemów informacyjnych szkolenie w zakresie sytuacji awaryjnych zgodnie z przydzielonymi rolami i obowiązkami:*

CP-3 SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA			
	CP-3(a)	**CP-3(a)[1]**	*w określonym przez organizację okresie czasu, w którym przejmują role lub odpowiedzialność w sytuacjach awaryjnych; (**S**)*
		CP-3(a)[2]	*określa okres czasu, w którym należy przeprowadzić szkolenie z zakresu sytuacji awaryjnych dla użytkowników systemu informacyjnego, którzy przejmują na siebie role lub odpowiedzialność w sytuacjach awaryjnych; (**S**)*
	CP-3(b)	*gdy jest to wymagane przez zmiany w systemie informacyjnym; (N)*	
	CP-3(c)	**CP-3(c)[1]**	*następnie, zgodnie z częstotliwością określoną przez organizację; (**S**)*
		CP-3(c)[2]	*określa częstotliwość szkolenia w sytuacjach awaryjnych. (**S**)*
	Komentarze i zalecenia: CP-3(b) jest oznaczony jako niesatysfakcjonujący, ponieważ osoby oceniające nie mogły znaleźć dowodów na to, że organizacja w przypadku istotnych zmian w systemie, zapewniła użytkownikom systemu informacyjnego szkolenie w sytuacjach awaryjnych zgodnie z przydzielonymi im rolami i obowiązkami.		

Podczas faktycznej oceny środków bezpieczeństwa i ochrony prywatności, wyniki oceny, oraz uwagi i zalecenia są dokumentowane na odpowiednich formularzach sprawozdawczych zdefiniowanych przez organizację. Zachęca się organizacje do opracowania standardowych szablonów raportów, które zawierają kluczowe elementy raportowania oceny opisane powyżej. Tam, gdzie to możliwe, stosuje się automatyzację, aby gromadzenie danych z oceny i raportowanie było efektywne kosztowo, terminowe i skuteczne.

ZAŁĄCZNIK H - PRZYPADKI OCEN[55]

RZECZYWISTE PRZYKŁADY DZIAŁAŃ OCENIAJĄCEGO WYNIKAJĄCE Z PROCEDUR OCENY

Zaprzestanie realizacji projektu dotyczącego przypadków oceny

NIST zainicjował projekt rozwoju przypadków oceny w październiku 2007 r. we współpracy z Departamentami Sprawiedliwości, Energii, Transportu oraz Wspólnotą Wywiadowczą. Międzyagencyjna grupa zadaniowa opracowała pełen zestaw przypadków oceny w oparciu o procedury oceny zawarte w publikacji specjalnej NIST SP 800-53A, rev. 1.

Nie będzie dalszego rozwoju przypadków oceny, począwszy od Publikacji Specjalnej NIST SP 800-53A, rev. 4. Wszystkie wcześniej opracowane przypadki oceny będą nadal dostępne i mogą być pobierane ze strony internetowej NIST pod adresem http://csrc.nist.gov/sec-cert.

Materiały zawarte w Dodatku H, w tym przykładowe szablony do opracowywania przypadków oceny, będą również nadal dostępne w archiwalnych wersjach Publikacji Specjalnej NIST SP 800-53A, rev. 1.

[55] Załącznik H zawiera dane informacyjne do ewentualnego wykorzystania.

ZAŁĄCZNIK I - BIEŻĄCA OCENA I AUTOMATYZACJA OCEN

WYKORZYSTANIE ZAUTOMATYZOWANYCH TECHNIK W CELU OSIĄGNIĘCIA BARDZIEJ EFEKTYWNYCH OCEN

Bieżąca ocena bezpieczeństwa to ciągła ocena skuteczności wdrażania środków bezpieczeństwa[56]. Stanowi ona istotny podzbiór działań ciągłości monitorowania bezpieczeństwa informacji (*ang. Information Security Continuous Monitoring - ISCM*)[57]. Bieżąca ocena obejmuje Kroki 3 i 4 ciągłości monitorowania bezpieczeństwa informacji i rozpoczyna się w ramach Kroku 3 ciągłości monitorowania bezpieczeństwa informacji, po rozpoczęciu zbierania informacji związanych z bezpieczeństwem zgodnie z ustalonymi przez organizację częstotliwościami. Ocena bieżąca jest kontynuowana, gdy informacje dotyczące bezpieczeństwa wygenerowane w ramach Kroku 3 ISCM są skorelowane, analizowane i raportowane kadrze kierowniczej w ramach Kroku 4 ISCM. Jak podano w NIST SP 800-137, informacje związane z bezpieczeństwem są generowane, korygowane, analizowane i raportowane przy użyciu zautomatyzowanych narzędzi w zakresie, w jakim jest to możliwe i praktyczne. Jeżeli nie jest możliwe i praktyczne wykorzystanie narzędzi automatycznych, informacje związane z bezpieczeństwem są generowane, korygowane, analizowane i raportowane przy użyciu metod ręcznych lub proceduralnych. W ten sposób kierownicy wyższego szczebla otrzymują informacje związane z bezpieczeństwem, niezbędne do podejmowania wiarygodnych, opartych na ryzyku decyzji dotyczących zagrożenia bezpieczeństwa informacji dla misji/biznesu[58].

---

[56] Koncepcje i techniki stosowane przez organizacje do bieżącej oceny środków bezpieczeństwa mogą być również skutecznie wykorzystywane do bieżącej oceny ochrony prywatności.

[57] Publikacja NIST SP 800-137 zawiera wytyczne dotyczące ciągłości monitorowania bezpieczeństwa informacji.

[58] Ciągłe monitorowanie może być skutecznie stosowane do zabezpieczeń prywatności zgodnej z koncepcjami, technikami i zasadami opisanymi w NIST SP 800-137. SAOP / CPO udzielają wskazówek w zakresie bieżącego monitorowania zabezpieczeń prywatności.

Automatyzacja ocen jest podstawowym elementem pomagającym organizacjom w zarządzaniu ryzykiem związanym z bezpieczeństwem informacji. Ewoluujące zagrożenia stanowią wyzwanie dla organizacji, które projektują, wdrażają i obsługują złożone systemy informacyjne, zawierające wiele komponentów sprzętowych, oprogramowanie układowe i aplikacje. Zdolność do oceny wszystkich wdrożonych środków bezpieczeństwa tak często, jak to konieczne, przy użyciu metod manualnych lub proceduralnych stała się niepraktyczna dla większości organizacji ze względu na rozmiar, złożoność i zakres ich infrastruktury informatycznej.

Jedna ze strategii zwiększania liczby środków bezpieczeństwa, dla których ocena/monitorowanie może być zautomatyzowane, zależy od zdefiniowania specyfikacji stanu pożądanego i wyrażenia pożądanego stanu w formie, która może być automatycznie porównywana ze stanem rzeczywistym. Pożądanym stanem jest zdefiniowana wartość lub specyfikacja, do której wartość stanu rzeczywistego może być porównywana. Niedopasowanie tych dwóch wartości wskazuje na występowanie wady w skuteczności jednego lub kilku środków bezpieczeństwa. Na przykład, polityka organizacyjna może stanowić, że konta użytkowników zostaną zablokowane po trzech nieudanych próbach logowania. Pożądanym stanem jest skonfigurowanie odpowiednich mechanizmów do blokowania kont po trzech nieudanych próbach logowania. Jeżeli podczas automatycznej oceny zebrane informacje dotyczące bezpieczeństwa wskazują, że określone urządzenie jest skonfigurowane w taki sposób, że konta zostaną zablokowane dopiero po pięciu nieudanych próbach logowania, identyfikowana jest rozbieżność pomiędzy żądanym stanem (trzy próby dozwolone przed zablokowaniem), a stanem rzeczywistym (pięć prób dozwolonych przed zablokowaniem). Niedopasowanie to może odzwierciedlać problem ze skutecznością środków bezpieczeństwa z publikacji NSC 800-53, zabezpieczenie AC-7, Nieudane próby logowania, AC-2, Zarządzanie kontami, oraz CM-2, Konfiguracja podstawowa. W przypadku zastosowania takiej strategii, informacje dotyczące bezpieczeństwa generowane w wyniku działalności ISCM są równoważne z wynikami oceny środków bezpieczeństwa.

W celu efektywnego zautomatyzowania oceny środków bezpieczeństwa z wykorzystaniem specyfikacji pożądanej strategii, ważne jest spełnienie następujących warunków wstępnych:

- *zautomatyzowane specyfikacje stanu rzeczywistego/zachowania są zdefiniowane;*
- *zdefiniowane są specyfikacje stanu pożądanego oparte na danych (porównywalne ze stanem rzeczywistym); oraz*
- *określona jest metoda obliczania/identyfikacji wad (różnice pomiędzy stanem pożądanym, a rzeczywistym/zachowaniem).*

Jeżeli satysfakcjonujące są warunki wstępne, system oceny może automatycznie obliczyć, gdzie występują różnice pomiędzy stanem pożądanym, a rzeczywistym (usterki) i wykorzystać te informacje do stworzenia raportów oceny bezpieczeństwa, dostarczając te raporty do wyznaczonego personelu za pomocą konsoli zarządzania bezpieczeństwem (pulpit menadżerski).

W przypadku korzystania z narzędzi automatycznych do przeprowadzania ocen, stosuje się metodę oceny testów[59]. Organizacja określa i dokumentuje: (I) konkretne zdolności lub środki bezpieczeństwa, które są oceniane przez zautomatyzowane narzędzie[60]; (II) częstotliwość, z jaką narzędzie będzie oceniać zdolności lub środki bezpieczeństwa; oraz (III) wymagania dotyczące analizy i sprawozdawczości w zakresie zdolności lub środków bezpieczeństwa.

[59] Jeżeli do uzyskania dodatkowej pewności potrzebna jest większa szczegółowość i zakres, zautomatyzowana metoda badania może być uzupełniona przez zastosowanie ręcznych / proceduralnych metod oceny (tj. rozmowa kwalifikacyjna, badanie lub test).

[60] W przypadku zdefiniowania zdolności w zakresie bezpieczeństwa, dokumentuje się macierz wszystkich indywidualnych zabezpieczeń, które wspierają tę zdolność. Jeżeli organizacja definiuje wieloraki potencjał, należy oczekiwać, że pomiędzy środkami bezpieczeństwa, a potencjałem będzie istniała relacja "kilka-do-kilku". Dodatkowe informacje dotyczące oceny zdolności w zakresie ochrony można znaleźć w sekcji 3.5.

Przejście od ocen ręcznych do zautomatyzowanych wymaga czasu na wdrożenie systemu zbierania danych do obsługi ocen automatycznych oraz konsoli zarządzania bezpieczeństwem do prezentacji wyników oceny. Wymaga to również czasu i wysiłku, aby zmodyfikować i zaktualizować proces oceny.

Więcej informacji na temat wsparcia zautomatyzowanego przeprowadzania ocen bieżących oraz tego, jak ułatwić przeprowadzanie ocen bieżących, znajduje się w publikacji NIST SP 8011, *Wsparcie automatyzacji w zakresie oceny środków bezpieczeństwa*.

ZAŁĄCZNIK J - PROCEDURY CENY PRYWATNOŚCI[61]

CELE, METODY I OBIEKTY OCENY ZABEZPIECZEŃ PRYWATNOŚCI

Przyszłościowe procedury oceny ochrony prywatności

Procedury oceny ochrony prywatności zawarte są w standardzie NIST SP 800-53 rev. 4, Appendix J. Format procedur oceny prywatności jest podobny do formatu procedur oceny bezpieczeństwa zawartych w Załączniku F publikacji.

Procedury oceny i materiały uzupełniające, które mają być włączone do niniejszego załącznika, zostaną poddane szerokiemu przeglądowi publicznemu w taki sam sposób, jak zabezpieczenia prywatności w NIST SP 800-53 rev. 4 zostały zweryfikowane przed włączeniem ich do ostatecznej publikacji .

Organizacje powinny konsultować się ze swoimi SAOP/CPO, w celu uzyskania wskazówek dotyczących oceny zabezpieczeń prywatności zawartych w NIST SP 800-53 rev. 4, Załącznik J, do czasu zakończenia procedur oceny dla Załącznika J.

[61] Załącznik J zawiera dane informacyjne do ewentualnego wykorzystania.