NSC NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA

Narodowy Standard Cyberbezpieczeństwa

Nazwa standardu	Symbol	Wersja	Data wydania
ZABEZPIECZENIA BAZOWE SYSTEMÓW INFORMATYCZNYCH ORAZ ORGANIZACJI	NSC 800-53B	1.0	01/07/2021

Zabezpieczenia bazowe systemów informatycznych oraz organizacji

PEŁNOMOCNIK RZĄDU DS. CYBERBEZPIECZEŃSTWA
Warszawa 2021

Szanowni Państwo,

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

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

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

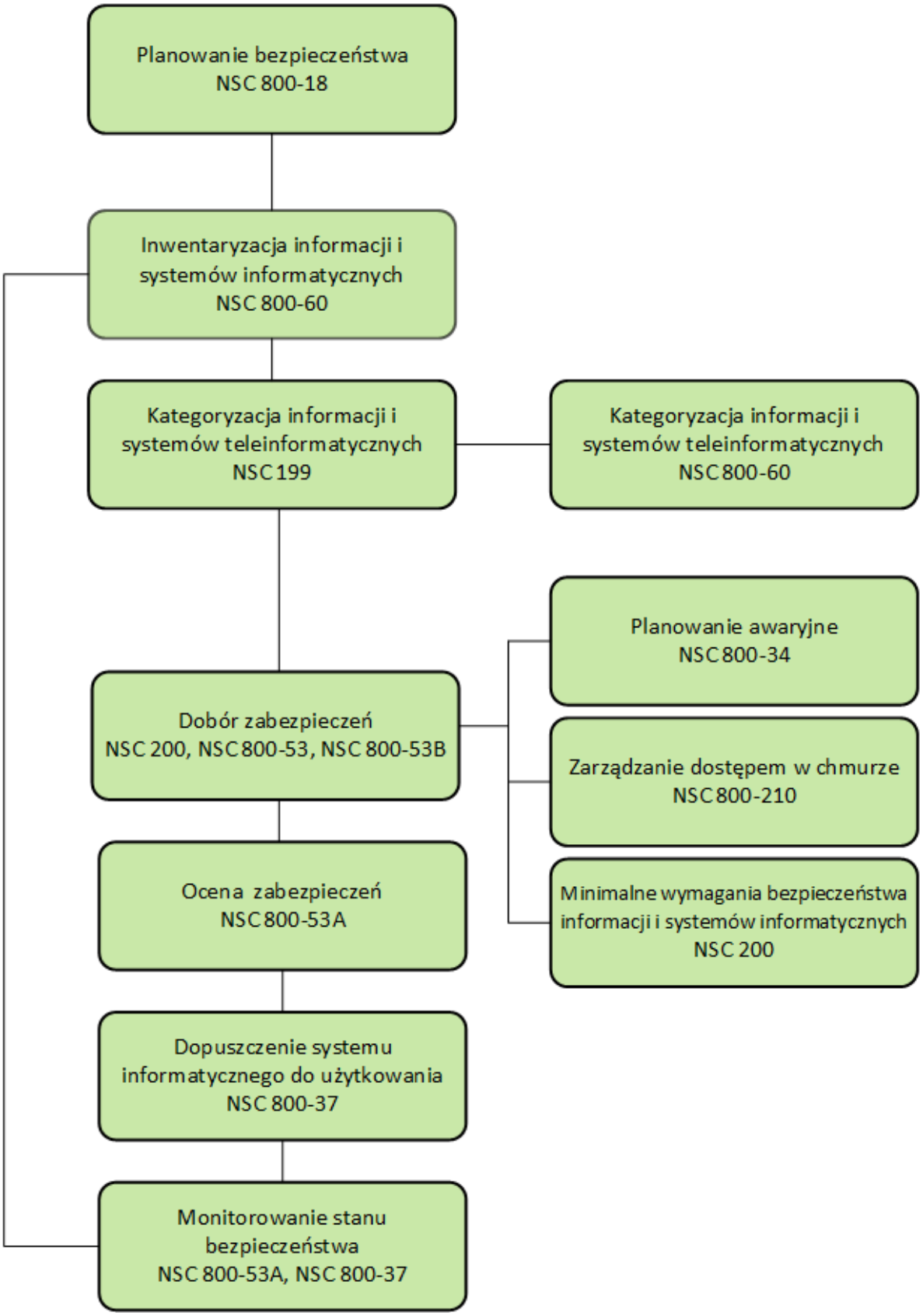
- NSC[2] 199, *Standardy kategoryzacji bezpieczeństwa* – na podstawie FIPS 199;
- NSC 200, *Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych* – na podstawie FIPS 200;
- NSC 500-92, *Architektura referencyjna chmury obliczeniowej – rekomendacje* – na podstawie NIST SP 500-292;
- NSC 800-18, *Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych* – na podstawie NIST SP 800- 18;

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

- NSC 800-30, *Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne* – na podstawie NIST SP 800-30;
- NSC 800-34, *Poradnik planowania awaryjnego* – na podstawie NIST SP 800-34;
- NSC 800-37, *Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu* – na podstawie NIST SP 800-37;
- NSC 800-53, *Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji* – na podstawie NIST SP 800-53;
- NSC 800-53A, *Ocena środków bezpieczeństwa i ochrony prywatności systemów informatycznych oraz organizacji. Tworzenie skutecznych planów oceny* – na podstawie NIST SP 800-53A;
- NSC 800-53B, *Zabezpieczenia bazowe systemów informatycznych oraz organizacji* – na podstawie NIST SP 800-53B;
- NSC 800-60, *Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego* – na podstawie NIST SP 800-60;
- NSC 800-61, *Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego* – na podstawie NIST SP 800-61;
- NSC 800-210, *Ogólne wytyczne dotyczące kontroli dostępu do systemów chmury obliczeniowej* – na podstawie NIST SP 800-210.

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

Cykl zarządzania bezpieczeństwem bazujący na publikacjach NIST wykorzystuje następujące dokumenty:


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

WSPÓLNE FUNDAMENTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

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

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

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

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

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

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

Niniejsza publikacja, ***Zabezpieczenia bazowe systemów informatycznych oraz organizacji***, opracowana została za zgodą National Institute of Science and Technology (NIST) na podstawie specjalnej publikacji NIST SP 800-53B.

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.***

PODSUMOWANIE

Niniejsza publikacja przedstawia zestaw zabezpieczeń bazowych (*ang. control baselines*)[3] w zakresie bezpieczeństwa i ochrony prywatności. Istnieją trzy poziomy bazowe środków bezpieczeństwa (jeden dla każdego poziomu wpływu na system - niski wpływ, umiarkowany wpływ i wysoki wpływ), a także poziom bazowy zabezpieczeń prywatności, który jest stosowany do systemów niezależnie od poziomu wpływu na system. Poza poziomami bazowymi zabezpieczeń, niniejsza publikacja zawiera wskazówki dostosowawcze i zestaw założeń roboczych, które pomagają w prowadzeniu i informowaniu o procesie wyboru zabezpieczeń. Zawarte są także wskazówki dotyczące rozwoju nakładek zabezpieczających ułatwiających dostosowanie poziomu bazowych środków bezpieczeństwa do potrzeb konkretnych społeczności, technologii i środowiska działania.

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

ZARZĄDZANIE RYZYKIEM

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

KORZYSTANIE Z PRZYKŁADÓW W NINIEJSZEJ PUBLIAKCJI

W niniejszej publikacji podano przykłady ilustrujące, wyjaśniające lub objaśniające niektóre pozycje w sekcjach rozdziałów, zabezpieczeniach podstawowych i zabezpieczeniach rozszerzonych.

Przykłady te mają charakter ilustracyjny i nie mają na celu ograniczenia lub narzucania stosowania przez organizacje prezentowanych w publikacji zabezpieczeń podstawowych i rozszerzonych.

SPIS TREŚCI

STRESZCZENIE

Istnieje pilna potrzeba ciągłego wzmacniania systemów informatycznych, produktów i usług, i zapewnienia, że te systemy, komponenty i usługi są wystarczająco wiarygodne i zapewniają niezbędną odporność, aby wspierać interesy gospodarcze i bezpieczeństwo narodowe Państwa.

NSC 800-53B przedstawia proaktywne i systemowe podejście do opracowania i udostępniania podmiotom publicznym oraz prywatnym organizacjom sektorowym kompleksowego zestawu bazowych środków bezpieczeństwa i ochrony prywatności dla wszystkich rodzajów platform obliczeniowych, w tym systemów obliczeniowych ogólnego przeznaczenia, systemów cyberfizycznych, systemów opartych na chmurze, urządzeń mobilnych oraz przemysłowych systemów i procesów sterowania. Zabezpieczenia bazowe stanowią punkt wyjścia dla organizacji w procesie selekcji środków bezpieczeństwa i ochrony prywatności. Korzystając z dostarczonych wytycznych i założeń dotyczących doboru zabezpieczeń, organizacje mogą dostosować swoje bazowe środki bezpieczeństwa i ochrony prywatności, zapewniając sobie zdolność do ochrony swoich krytycznych i istotnych operacji i aktywów.

ROZDZIAŁ PIERWSZY

WPROWADZENIE

POTRZEBA STOSOWANIA BAZOWYCH ŚRODKÓW BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Środki bezpieczeństwa to środki zarządcze, organizacyjne lub technologiczne wybrane i wdrożone w ramach systemu informatycznego lub organizacji, stosowane w celu zapewnienia poufności, integralności i dostępności informacji i/lub dostępności systemu informatycznego oraz zarządzania ryzykiem w zakresie bezpieczeństwa informacji.

Zabezpieczenia prywatności to administracyjne, techniczne i fizyczne zabezpieczenia stosowane w organizacji w celu zapewnienia zgodności z obowiązującymi wymogami w zakresie ochrony prywatności i zarządzania zagrożeniami dla prywatności.

Środki bezpieczeństwa i prywatności są wybierane i wdrażane w celu spełnienia wymagań w zakresie bezpieczeństwa i prywatności nakładanych na system informatyczny i/lub organizację. Wymogi te wynikają z obowiązujących przepisów prawa, regulacji wewnętrznych, polityk, standardów, które mają na celu zapewnienie poufności, integralności i dostępności przetwarzanych informacji oraz zarządzanie zagrożeniami dla prywatności osób. Wybór, opracowanie i skuteczne wdrożenie zabezpieczeń to ważne zadania, które mają istotny wpływ na działalność i majątek organizacji, jak również na dobro osób i Państwa.

NSC 800-37 definiuje dwa podejścia do wyboru środków bezpieczeństwa i ochrony prywatności: podejście wyboru *bazowych (ang. baseline)*[4] zabezpieczeń oraz podejście wyboru zabezpieczeń *generowanych przez organizację.* Podejście wyboru zabezpieczeń bazowych wykorzystuje zestawy minimalnych zabezpieczeń, które są predefiniowanymi zestawami środków bezpieczeństwa specjalnie przygotowanymi w celu zaspokojenia potrzeb ochrony grupy, organizacji lub wspólnoty interesów. Zabezpieczenia bazowe służą jako punkt

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

wyjścia do ochrony prywatności osób, oraz zapewnienia bezpieczeństwa informacji i systemów informatycznych. Podejście do wyboru zabezpieczeń generowanych przez organizację nie zostało uwzględnione w niniejszej publikacji.

1.1. CEL I ZASTOSOWANIE

Niniejsza publikacja ustanawia bazowe środki bezpieczeństwa i ochrony prywatności dla systemów informatycznych i organizacji oraz zawiera wskazówki dotyczące dostosowania tych środków do potrzeb organizacji. Zabezpieczenia bazowe mogą być wdrażane przez każdą organizację przetwarzającą informacje. Wdrożenie minimalnego zestawu zabezpieczeń wybranych z NSC SP 800-53 jest obowiązkowe w celu ochrony informacji i systemów informatycznych podmiotów publicznych. Pomimo, że stosowanie bazowych zabezpieczeń prywatności nie jest obligatoryjne, NSC 800-53B - wraz z innymi wspierającymi publikacjami NSC - ma na celu pomóc organizacjom w określeniu środków bezpieczeństwa i ochrony prywatności niezbędnych do zarządzania ryzykiem oraz spełnienia wymogów bezpieczeństwa i ochrony prywatności zawartych w przepisach o ochronie danych osobowych.

Niniejsza publikacja spełnia wymogi bezpieczeństwa i ochrony prywatności poprzez zastosowanie założeń, które stanowią podstawę do opracowania bazowych środków bezpieczeństwa i ochrony prywatności, jak opisano w sekcji 2.3. Zabezpieczenia bazowe służą jako punkt wyjścia do zaspokojenia potrzeb organizacji w zakresie ochrony. Zabezpieczenia zawarte w ramach zabezpieczeniach bazowych są dostosowywane do wymagań bezpieczeństwa podmiotu zgodnie z procesem opisanym w sekcji 2.4, w celu dalszego ułatwienia zarządzania ryzykiem w zakresie bezpieczeństwa i prywatności właściwym dla danej organizacji. Proces dostosowywania może być prowadzony i wspierany przez wiele czynników, w tym misję i potrzeby biznesowe organizacji, potrzeby ochrony interesariuszy oraz ocenę ryzyka. Połączenie procesów selekcji zabezpieczeń bazowych i dostosowywania zabezpieczeń może pomóc organizacjom w spełnieniu określonych wymagań w zakresie bezpieczeństwa i ochrony prywatności.

1.2. ODBIORCY DOCELOWI

Niniejsza publikacja jest przeznaczona dla zróżnicowanej publiczności. Zachęca się, aby z niniejszej publikacji korzystały:

- Osoby odpowiedzialne za system, bezpieczeństwo informacji, prywatność lub zarządzanie ryzykiem i nadzór, w tym osoby autoryzujące, CIO, SAISO, SAOP.[5]
- Osoby odpowiedzialne za rozwój systemów, w tym właściciele misji, programiści, inżynierowie systemów, inżynierowie bezpieczeństwa systemów, inżynierowie ochrony prywatności, twórcy sprzętu i oprogramowania, integratorzy systemów oraz osoby zajmujące się zakupami lub zamówieniami.
- Osoby odpowiedzialne za logistykę, w tym programiści, personel ds. zamówień publicznych, integratorzy systemów i zarządcy nieruchomości.
- Osoby odpowiedzialne za bezpieczeństwo i prywatność oraz za realizację operacji, w tym właściciele misji lub firm, właściciele systemów, właściciele lub władający informacją, administratorzy systemów oraz SSO I SPO.[6]
- Osoby odpowiedzialne za ocenę bezpieczeństwa i prywatności oraz monitorowanie, w tym audytorzy, osoby oceniające system, osoby oceniające zabezpieczenia, niezależni weryfikatorzy i zatwierdzający oraz analitycy.
- Podmioty komercyjne, w tym partnerzy przemysłowi, którzy wytwarzają komponenty i systemy oraz opracowują technologie bezpieczeństwa i ochrony prywatności.

[5] Patrz – NSC 800-37 oraz NSC 7298.

[6] j.w.

1.3. OBOWIĄZKI ORGANIZACYJNE

Organizacje są odpowiedzialne za wybór zabezpieczeń zgodnie z NSC 800-37[7]. W przypadku wyboru podejścia opartego na zabezpieczeniach bazowych, organizacje wybierają bazowy zestaw środków bezpieczeństwa i zabezpieczeń prywatności, jak opisano w rozdziale trzecim. Po wybraniu zabezpieczeń bazowych, organizacje stosują wytyczne dotyczące dostosowywania środków bezpieczeństwa zawarte w rozdziale drugim, aby upewnić się, że wynikające z nich zabezpieczenia są niezbędne i wystarczające do zarządzania ryzykiem bezpieczeństwa[8] i ryzykiem utraty prywatności[9].

1.4. ZWIĄZEK Z INNYMI PUBLIKACJAMI

Niniejsza publikacja ustanawia bazowe środki bezpieczeństwa i ochrony prywatności, które wynikają z zabezpieczeń przedstawionych w NSC 800-53. Zabezpieczenia bazowe zawarte w niniejszej publikacji są zgodne z wymaganiami dotyczącymi systemów informatycznych zawartych w NSC 199, oraz NSC 200. Publikacja NSC 800-37 zawiera wytyczne dotyczące metod selekcji zabezpieczeń.

1.5. WERSJE I ROZSZERZENIA

Bazowe środki bezpieczeństwa i ochrony prywatności reprezentują stan zabezpieczenia osób, systemów informatycznych i organizacji. Zabezpieczenia bazowe są okresowo przeglądane i zmieniane w celu odzwierciedlenia doświadczeń zdobytych podczas ich stosowania; nowych lub zmienionych przepisów prawa powszechnego, regulacji wewnętrznych, polityk I standardów; zmieniających się wymagań dotyczących bezpieczeństwa i ochrony prywatności; pojawiających się zagrożeń, podatności, ataków i metod przetwarzania informacji; oraz dostępności nowych technologii. W związku z tym

[7] W ramach podejścia wyboru zabezpieczeń bazowych oraz podejścia wyboru zabezpieczeń generowanych przez organizacje, organizacje opracowują odpowiednio zdefiniowany zestaw wymagań dotyczących bezpieczeństwa i ochrony prywatności, wykorzystując proces inżynierii systemów oparty na cyklu życia, zgodnie z opisem zawartym w NSC 800-37 (Etap: przygotowania zadań - *poziom systemu*, Zadanie P-15, *Definicja wymagań).* Proces definiowania wymagań generuje zestaw wymagań, które mogą być wykorzystane do wyboru i informowania o wyborze zabezpieczeń spełniających te wymagania.

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

[9] [IR8062] wprowadza pojęcia oceny ryzyka dla prywatności.

oczekuje się, że środki bezpieczeństwa I ochrony prywatności określone w zabezpieczeniach bazowych również z czasem ulegną zmianie, zostaną wycofane, skorygowane i uzupełnione. Oprócz konieczności wprowadzenia zmian, została uwzględniona potrzeba stabilności. Osiągane jest to poprzez wprowadzenie wymogu, aby proponowane zmiany poziomu bazowego zostały poddane rygorystycznemu i przejrzystemu procesowi przeglądu publicznego w celu uzyskania informacji zwrotnych od sektora publicznego i prywatnego oraz stworzenia konsensusu dotyczącego zmian poziomu bazowego. Publiczny proces przeglądu zapewnia opracowanie stabilnych elastycznie i solidnych technicznie zestawów bazowych środków bezpieczeństwa i ochrony prywatności.

1.6. STRUKTURA PUBLIKACJI

Pozostała część tej publikacji jest zorganizowana w następujący sposób:

- W **rozdziale drugim** opisano podstawowe pojęcia związane z zabezpieczeniami bazowymi, wybór odpowiednich poziomów bazowych, założeń bazowych, dostosowywanie poziomów bazowych, nakładek i ich możliwości.
- W **rozdziale trzecim** zamieszczono zestaw tabel uporządkowanych według kategorii zabezpieczeń, które zawierają informacje o zabezpieczeniach o niskim, umiarkowanym i wysokim wpływie na bezpieczeństwo i ochronę prywatności.
- Lista informacyjnych **referencji**[10] zamieszczona jest po rozdziale trzecim.
- Załączniki pomocnicze obejmują:
  - **Załącznik A:** Słownik
  - **Załącznik B:** Akronimy
  - **Załącznik C:** Wskazówki dotyczące nakładek.

[10] O ile nie podano inaczej, wszystkie odniesienia do publikacji NIST odnoszą się do najnowszej wersji tych publikacji.

BAZOWE ŚRODKI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Bazowe środki bezpieczeństwa i ochrony prywatności są zdefiniowanymi zestawami zabezpieczeń, zebranymi w celu zaspokojenia potrzeb ochrony grup, organizacji lub wspólnot interesów. Zabezpieczenia bazowe służą, jako punkt wyjścia do ochrony prywatności osób fizycznych, informacji i systemów informatycznych i mogą być dostosowywane (tzn. dopasowywane do indywidualnych potrzeb) odpowiednio do misji organizacji i funkcji biznesowych; konkretnych i wiarygodnych informacji o zagrożeniach; środowiska, w którym działa organizacja; oraz interesów ochrony prywatności osób.

ROZDZIAŁ DRUGI

PODSTAWY

ZABEZPIECZENIA BAZOWE, DOSTOSOWYWANIE, NAKŁADKI I WYMAGANIA

W niniejszym rozdziale przedstawiono podstawowe pojęcia związane z bazowymi środkami bezpieczeństwa i ochrony prywatności, w tym cel stosowania zabezpieczeń bazowych, sposób wyboru, uwarunkowania związane z zabezpieczeniami bazowymi, sposób, w jaki proces dostosowywania jest wykorzystywany do dopasowywania bazowych środków bezpieczeństwa, cel stosowania nakładek (*ang. overlays*) i sposób, w jaki są one wykorzystywane do zaspokajania potrzeb w zakresie bezpieczeństwa i ochrony prywatności społeczności będących przedmiotem zainteresowania oraz sposób, w jaki koncepcja rozwijania wydajności może ułatwić grupowanie wzajemnie wzmacniających się zabezpieczeń.

2.1. ZABEZPIECZENIA BAZOWE

Istotnym wyzwaniem dla organizacji jest wybór stosownego zestawu środków bezpieczeństwa i ochrony prywatności, które mogą zabezpieczać ich misję i funkcje biznesowe oraz zapewnić możliwość zarządzania ryzykiem w zakresie bezpieczeństwa i prywatności. Wybrane mechanizmy bezpieczeństwa, jeśli są prawidłowo wdrożone i uznane za skuteczne, spełniają wymagania dotyczące bezpieczeństwa i ochrony prywatności określone w obowiązujących przepisach prawa, dyrektywach, politykach i regulacjach wewnętrznych. Nie ma jednego zestawu środków bezpieczeństwa, który uwzględniałby wszystkie kwestie bezpieczeństwa i ochrony prywatności w każdej sytuacji. Jednak wybór najodpowiedniejszych zabezpieczeń dla konkretnej sytuacji lub systemu, dokonywany w celu odpowiedniej reakcji na ryzyko, wymaga fundamentalnego zrozumienia misji i priorytetów biznesowych organizacji, misji i funkcji biznesowych, które będą wspierane przez systemy, oraz środowisk, w których systemy będą działać. Wymaga to również ścisłej współpracy z kluczowymi interesariuszami organizacji. Przy takim podejściu, organizacja musi wykazać, w jaki sposób skutecznie i efektywnie kosztowo zapewnić poufność, integralność, dostępność informacji i systemów organizacyjnych, a także prywatność osób fizycznych w kontekście wspierania misji i funkcji biznesowych organizacji.

Wprowadzenie koncepcji *bazowych (podstawowych / minimalnych) zabezpieczeń (mechanizmów / środków bezpieczeństwa),* może pomóc organizacjom w wyborze zestawu zabezpieczeń dla ich systemów, który jest współmierny do zagrożenia bezpieczeństwa i prywatności. Zabezpieczenia bazowe są zbiorem zabezpieczeń ustanawianym na podstawie środków bezpieczeństwa prezentowanych w publikacji NSC 800-53, zebranych w celu zaspokojenia potrzeb ochrony grupy, organizacji lub wspólnoty interesów. Dostarcza on uogólniony zestaw zabezpieczeń, który stanowi punkt wyjścia dla kolejnych działań dostosowawczych, które są wykorzystywane w celu stworzenia bazowych środków bezpieczeństwa (ukierunkowanych lub zindywidualizowanych rozwiązań w zakresie bezpieczeństwa i ochrony prywatności dla podmiotu, któremu zabezpieczenia bazowe mają służyć). Zabezpieczenia bazowe są dostosowane do różnych czynników, w tym informacji o zagrożeniach, misji lub wymagań biznesowych, rodzajów systemów, wymagań sektorowych, konkretnych technologii, środowisk operacyjnych, założeń organizacyjnych i ograniczeń, interesów związanych z ochroną prywatności osób fizycznych, przepisów, rozporządzeń, zasad, dyrektyw, standardów lub najlepszych praktykach branżowych. Działania związane z dostosowywaniem zabezpieczeń do potrzeb organizacji zostały opisane bardziej szczegółowo w sekcji 2.4.

2.2. WYBÓR ZABEZPIECZEŃ BAZOWYCH

Programy bezpieczeństwa informacji są odpowiedzialne za ochronę informacji i systemów informatycznych przed nieautoryzowanym dostępem, użyciem, ujawnieniem, zakłóceniem, modyfikacją lub zniszczeniem (tj. nieautoryzowaną działalnością lub nieprawidłowym zachowaniem systemu) w celu zapewnienia poufności, integralności i dostępności. Programy ochrony prywatności są odpowiedzialne za zarządzanie ryzykiem odnoszącym się do osób fizycznych, związanym z tworzeniem, gromadzeniem, wykorzystywaniem, przetwarzaniem, rozpowszechnianiem, przechowywaniem, konserwacją, ujawnianiem lub usuwaniem (zwanych łącznie *przetwarzaniem*) danych osobowych (*ang. personal identification information - PII*) oraz za zapewnienie zgodności z obowiązującymi wymogami dotyczącymi

prywatności.[11] Jeżeli system przetwarza dane osobowe, programy bezpieczeństwa informacji i programy ochrony prywatności są współodpowiedzialne za zarządzanie wpływem zagrożeń na osoby fizyczne wynikającym z tych zagrożeń oraz współpracują w celu określenia kategorii bezpieczeństwa oraz wyboru i dostosowania stosownych zabezpieczeń na podstawie bazowych środków bezpieczeństwa.

2.2.1. Zabezpieczenia bazowe

Przygotowując się do wyboru i dostosowania odpowiednich bazowych środków bezpieczeństwa dla systemów organizacji i ich środowisk działania, organizacje najpierw określają krytyczność i wrażliwość informacji, które mają być przetwarzane, przechowywane lub przekazywane przez te systemy. Proces określania krytyczności i wrażliwości informacji jest znany jako *kategoryzacja bezpieczeństwa* i opisany jest w NSC 199. Wyniki kategoryzacji bezpieczeństwa są pomocne przy wyborze bazowych środków bezpieczeństwa w celu ochrony systemów i informacji. Zabezpieczenia bazowe wybrane dla systemów są współmierne do potencjalnego negatywnego wpływu na działalność organizacji, zasoby organizacyjne, osoby fizyczne, inne organizacje lub Państwo w przypadku utraty poufności, integralności lub dostępności. NSC 199 wymaga, aby organizacje kategoryzowały systemy jako mające niski, umiarkowany lub wysoki poziom wpływu zagrożenia na określone atrybuty bezpieczeństwa, takie jak poufność, integralność i dostępność.[12]

Ponieważ potencjalne wartości wpływu w zakresie poufności, integralności i dostępności nie zawsze mogą być takie same dla danego systemu, wprowadzona w NSC 199 koncepcja

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

[12] NSC 800-60 (część 1 i 2) zawiera wytyczne dotyczące przypisywania kategorii bezpieczeństwa do systemów informatycznych. NSC 800-37 zawiera wytyczne dotyczące poszczególnych zadań w ramach kroków kategoryzacji ram zarządzania ryzykiem (RMF).

najwyższej wartości[13] (*ang. high water mark*) jest stosowana w NSC 200 w celu określenia poziomu wpływu na system. Poziom wpływu na system jest z kolei wykorzystywany w celu wyboru, mającego w danej sytuacji zastosowanie, jednego z trzech zabezpieczeń bazowych określonych w rozdziale trzecim. Zatem system o *niskim poziomie wpływu* definiuje się, jako system, w którym wszystkim trzem atrybutom bezpieczeństwa (tj. poufności, integralności i dostępności) przypisuje się niską wartość potencjalnego wpływu określonego w NSC 199. System o *umiarkowanym wpływie* to system, w którym przynajmniej jednemu atrybutowi bezpieczeństwa przypisuje się umiarkowaną wartość potencjalnego wpływu, a żadnemu z atrybutów bezpieczeństwa nie przypisuje się wysokiej wartości potencjalnego wpływu. Wreszcie, system o *wysokim wpływie* to system, w którym co najmniej jednemu z trzech atrybutów bezpieczeństwa przypisuje się wysoką wartość potencjalnego wpływu.

Po określeniu poziomu wpływu na system, organizacje wybierają odpowiednie zabezpieczenia bazowe.[14] Wyboru zabezpieczeń bazowych dokonuje się na podstawie poziomu wpływu na system, określanego w opisanym powyżej procesie kategoryzacji bezpieczeństwa.[15] Organizacja wybiera jeden z trzech zestawów zabezpieczeń bazowych z rozdziału trzeciego, odpowiadający kategorii niskiego, umiarkowanego lub wysokiego poziomu wpływu na system. Należy zauważyć, że nie wszystkie zabezpieczenia podstawowe lub zabezpieczenia rozszerzone zidentyfikowane w publikacji NSC 800-53 są przypisane do zabezpieczeń bazowych, jak to wskazano w tabelach w rozdziale trzecim. Zabezpieczenia podstawowe i zabezpieczenia rozszerzone, które są przypisane do zabezpieczeń bazowych, są zaznaczone w tabelach 3-1 do 3-20 znakiem "X" w kolumnach "Niski, Umiarkowany lub Wysoki". Użycie terminu "zabezpieczenie bazowe" jest celowe. Zabezpieczenia podstawowe

[13] Stosowana jest koncepcja najwyższej wartości, ponieważ istnieją znaczące zależności pomiędzy atrybutami bezpieczeństwa, takimi jak poufność, integralność i dostępność. W większości przypadków naruszenie jednego z atrybutów bezpieczeństwa ostatecznie wpływa również na pozostałe atrybuty bezpieczeństwa. W związku z tym środki bezpieczeństwa nie są kategoryzowane według atrybutów bezpieczeństwa. Natomiast są grupowane w zabezpieczenia bazowe mające na celu zapewnienia ogólnej zdolności ochrony poszczególnych klas systemów w oparciu o poziom wpływu na te systemy.

[14] Ogólny proces wyboru zabezpieczeń bazowych może zostać rozszerzony lub uszczegółowiony o dodatkowe wytyczne dla poszczególnych sektorów, np. dla społeczności mającej wspólne cele w zakresie zarządzania ryzykiem lub dla podsektora przemysłowego, jak opisano w załączniku *Nakładki.*

[15] Patrz – NSC 200.

i zabezpieczenia rozszerzone ujęte w zabezpieczeniach bazowych są punktem wyjścia, z którego środki bezpieczeństwa lub rozszerzenia środków bezpieczeństwa mogą zostać usunięte, dodane lub ukierunkowane w oparciu o wskazówki dotyczące dostosowywania zawarte w sekcji 2.4.[16]

2.2.2. Zabezpieczenia bazowe prywatności

Poza trzema poziomami bazowych środków bezpieczeństwa, w rozdziale trzecim przedstawiono wstępne zabezpieczenia bazowe prywatności w organizacji w celu uwzględnienia wymogów dotyczących prywatności i zarządzania ryzykiem w zakresie prywatności wynikającym z przetwarzania danych osobowych. Zabezpieczenia podstawowe I zabezpieczenia rozszerzone, które są przypisane do bazowych zabezpieczeń prywatności, są oznaczone znakiem "X.".[17] Nie wszystkie zabezpieczenia podstawowe i zabezpieczenia rozszerzone, które dotyczą obszarów zagrożenia prywatności są przypisane do zabezpieczeń bazowych prywatności. To podejście stanowi punkt wyjścia, z którego można usunąć, dodać lub ukierunkować zabezpieczenia podstawowe lub zabezpieczenia rozszerzone w oparciu o dostosowywanie opisane w sekcji 2.4.

Organizacje przeprowadzają oceny ryzyka w zakresie ochrony prywatności, które uwzględniają charakter przetwarzania danych osobowych i jego wpływ na osoby fizyczne, aby ukierunkować dostosowanie zabezpieczeń bazowych prywatności do swoich programów i systemów. Oceny ryzyka w zakresie ochrony prywatności obejmują ocenę możliwości zastosowania wymogów prawnych i zasad do ich programów. Na przykład, organizacje mogą

[16] Ukierunkowanie odnosi się do modyfikacji zabezpieczeń podstawowych lub zabezpieczeń rozszerzonych (w tym parametrów zdefiniowanych przez organizację), lub dodatkowych wytycznych umożliwiających organizacji dalsze doskonalenie zabezpieczeń bazowych w celu uwzględnienia specyficznych wymagań, technologii, misji, funkcji biznesowych lub środowisk działania organizacji. W celu zaspokojenia zapotrzebowania na specjalistyczne zestawy zabezpieczeń dla grup społeczności, systemów i organizacji, wprowadza się koncepcję *nakładek*. Więcej informacji na temat nakładek znajduje się w załączniku *Nakładki*.

[17] Rozszerzenia zabezpieczeń prywatności w tabelach 3-1 do 3-20 w rozdziale trzecim nie mogą być wybrane i wdrożone bez wybrania i wdrożenia powiązanych zabezpieczeń podstawowych. Takie działania mogą wymagać współpracy z programami bezpieczeństwa w przypadkach, gdy program bezpieczeństwa jest odpowiedzialny za zabezpieczenia podstawowe. Organizacje zapewniają, że odpowiedzialność za wybór i wdrożenie zabezpieczeń jest jasno określona pomiędzy programami bezpieczeństwa informacji i ochrony prywatności.

usunąć zabezpieczenia rozszerzone związane z wymogami prawnymi lub politykami, które nie mają zastosowania do przetwarzanych przez nich danych osobowych, chyba, że w oparciu o ocenę ryzyka związanego z ochroną prywatności ustalą, że zabezpieczenia podstawowe i zabezpieczenia rozszerzone byłyby pomocne w ograniczeniu zidentyfikowanych zagrożeń prywatności. Ponadto organizacje mogą dodać nieprzypisane zabezpieczenia podstawowe i zabezpieczenia rozszerzone w celu ograniczenia zagrożeń dla prywatności charakterystycznych dla ich systemów informatycznych, określone na podstawie własnej oceny ryzyka dla prywatności.

2.3. ZAŁOŻENIA ZABEZPIECZEŃ BAZOWYCH

Zabezpieczenia bazowe przedstawione w rozdziale trzecim odnoszą się do potrzeb w zakresie ochrony zróżnicowanych grup odbiorców, w tym użytkowników indywidualnych i organizacji. W związku z tym, niektóre hipotezy robocze stanowią na ogół zabezpieczenia bazowe określone w rozdziale trzecim. Założenia te, przyjęte przy określaniu poziomów bazowych w rozdziale trzecim, uwzględniają środowiska, w których funkcjonują systemy informatyczne organizacji, w tym obowiązki legislacyjne, regulacje lub polityki; charakter działalności organizacji; specyficzną funkcjonalność wykorzystywaną w ramach systemów; rodzaje zagrożeń, z którymi borykają się organizacje, misje i procesy biznesowe; interesy ochrony prywatności osób fizycznych; oraz rodzaje informacji przetwarzanych, przechowywanych lub przekazywanych przez systemy.[18] Wyrażenie podstawowych założeń jest kluczowym elementem etapu opracowywania schematów ryzyka (*ang. Risk Framing)* procesu zarządzania ryzykiem opisanego w [NIST SP 800-39] i wzmocnionego w etapie *Przygotowanie* przedstawionego w publikacji NSC 800-37. Szczegółowe hipotezy, które leżą u podstaw zabezpieczeń bazowych opisanych w rozdziale trzecim zakładają, że:

[18] Zabezpieczenia bazowe uwzględniają charakter zagrożeń w zakresie, w jakim jest to możliwe ze względu na dynamiczny charakter zagrożeń.

- Informacje w systemach organizacyjnych są relatywnie trwałe.[19]
- Systemy organizacyjne są eksploatowane przez wielu użytkowników (pracujących zarówno pojedynczo jak i jednocześnie).
- Niektóre informacje w systemach organizacyjnych nie są udostępniane innym użytkownikom, którzy mają autoryzowany dostęp do tych samych systemów.
- Systemy organizacyjne istnieją w środowiskach sieciowych i są ogólnego przeznaczenia.
- Organizacje posiadają niezbędną strukturę, zasoby i infrastrukturę do realizacji zabezpieczeń.[20]

Jeżeli którekolwiek z powyższych założeń jest niewłaściwe, wówczas niektóre środki bezpieczeństwa przypisane do zabezpieczeń bazowych w rozdziale trzecim, mogą nie mieć zastosowania - jest to sytuacja, którą można rozwiązać stosując wytyczne dotyczące dostosowywania oraz wyniki oceny ryzyka na poziomie organizacji i systemu z sekcji 2.4. Dodatkowe założenia, które **nie są** uwzględnione w zabezpieczeniach bazowych obejmują:

- Zagrożenia wewnętrzne istniejące wewnątrz organizacji.
- Informacje niejawne przetwarzane, przechowywane lub przekazywane przez systemy organizacyjne.[21]
- Zaawansowane trwałe zagrożenia (*ang. advanced persistent threats - APT*) istniejące wewnątrz organizacji.
- Informacje wymagające specjalistycznej ochrony w oparciu o ustawodawstwo, dyrektywy, rozporządzenia, oraz polityki.
- Systemy organizacyjne komunikujące się z innymi systemami w różnych domenach bezpieczeństwa.

[19] Trwałe dane/informacja odnoszą się do danych/informacji mających użyteczność przez stosunkowo długi czas (np. dni, tygodnie).

[20] Ogólnie rzecz biorąc, organizacje spełniają to założenie. Założenie to może jednak stać się problemem dla niektórych podmiotów. Podmioty takie mogą nie być wystarczająco duże lub nie posiadać wystarczających zasobów, aby dysponować elementami dedykowanymi do zapewnienia bezpieczeństwa systemów lub ochrony prywatności, które są zakładane przez zabezpieczenia bazowe. Organizacje uwzględniają takie czynniki w swoich decyzjach opartych na ryzyku.

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

Jeżeli którekolwiek z tych założeń ma zastosowanie, prawdopodobnie konieczne będzie zastosowanie dodatkowych zabezpieczeń z NSC 800-53 w celu zapewnienia odpowiedniej ochrony - sytuacja, której można również skutecznie zaradzić, stosując wytyczne dotyczące dostosowywania w sekcji 2.4 (w szczególności uzupełnienie środków bezpieczeństwa) oraz wyniki oceny ryzyka na poziomie organizacji i systemu.

2.4. DOSTOSOWYWANIE ZABEZPIECZEŃ BAZOWYCH

Po wybraniu odpowiednich zabezpieczeń bazowych, organizacje inicjują proces dostosowywania zabezpieczeń do konkretnych wymogów bezpieczeństwa i ochrony prywatności określonych przez organizację. Proces dostosowywania jest częścią procesu zarządzania ryzykiem w całej organizacji, który obejmuje ustanawianie struktury, ocenę, reagowanie i monitorowanie zagrożeń w zakresie bezpieczeństwa i prywatności informacji. Decyzje dotyczące dostosowywania zależą od czynników organizacyjnych lub systemowych. Podczas, gdy decyzje o dostosowaniu koncentrują się na kwestiach bezpieczeństwa i ochrony prywatności, są one zazwyczaj powiązane z innymi kwestiami związanymi z ryzykiem, które organizacje muszą rutynowo podejmować. Kwestie związane z ryzykiem, takie jak koszty, harmonogram i wydajność, są brane pod uwagę przy ustalaniu, jakie środki bezpieczeństwa należy zastosować i jak wdrożyć je w systemach organizacyjnych i środowiskach działania. Proces dostosowywania może obejmować, ale nie ogranicza się do następujących działań:[22]

- Określanie i wyznaczanie zabezpieczeń wspólnych;
- Stosowanie rozważań dotyczących zakresu stosowania i wdrażania;
- Wybór zabezpieczeń kompensacyjnych;
- Przypisywanie wartości do zdefiniowanych przez organizację parametrów zabezpieczeń poprzez jednoznaczne operacje przyporządkowania i wyboru;
- Uzupełnianie zabezpieczeń bazowych o dodatkowe zabezpieczenia podstawowe i rozszerzone;
- Dostarczanie informacji dotyczących specyfikacji w celu implementacji zabezpieczeń.

[22] Dodatkowe wskazówki dotyczące dostosowywania zabezpieczeń prywatności znajdują się w sekcji 2.2.2, *Zabezpieczenia bazowe prywatności.*

Organizacje korzystają z wytycznych dotyczących zarządzania ryzykiem w celu ułatwienia podejmowania decyzji opartych na szacowaniu ryzyka w odniesieniu do możliwości zastosowania zabezpieczeń na poziomie bazowym. Ostatecznie, organizacje stosują proces dostosowywania w celu uzyskania efektywnych kosztowo rozwiązań, które wspierają misję i potrzeby biznesowe organizacji oraz zapewniają bezpieczeństwo i ochronę prywatności współmierną do ryzyka. Organizacje mają możliwość elastycznego dostosowania na poziomie organizacji dla systemów wspierających linię biznesową, misję lub proces biznesowy, na poziomie pojedynczego systemu lub poprzez zastosowanie kombinacji tych dwóch rozwiązań. [23] Organizacje nie usuwają jednak arbitralnie środków bezpieczeństwa i ochrony prywatności z zabezpieczeń bazowych. Oczekuje się, że decyzje związane z dostosowywaniem będą możliwe do podjęcia w oparciu o misję i potrzeby biznesowe, solidne uzasadnienie i wyraźne ustalenia oparte na ryzyku.[24]

Decyzje korygujące, w tym uzasadnienie decyzji oparte na ryzyku, są udokumentowane w planach bezpieczeństwa i ochrony prywatności systemów organizacyjnych. [25] Każde zabezpieczenie wybrane spośród zabezpieczeń bazowych, jest ewidencjonowane przez organizację. Jeżeli niektóre zabezpieczenia są dostosowywane, uzasadnienie jest rejestrowane w planach bezpieczeństwa i ochrony prywatności systemu, a następnie zatwierdzane przez uprawniony personel organizacji w ramach procesu zatwierdzania planów. Udokumentowanie decyzji dotyczących zarządzania ryzykiem przeprowadzanych podczas procesu dostosowywania zabezpieczeń bazowych jest niezbędne, aby upoważniony personel organizacji dysponował niezbędnymi informacjami w celu podejmowania

[23] Patrz NSC 800-37, Zadanie P-4, *Ustanowienie, udokumentowanie i opublikowanie dostosowanych przez organizację zestawu minimalnych zabezpieczeń i/lub Profili Ram Cyberbezpieczeństwa*, w celu uzyskania dodatkowych wskazówek na temat dostosowania zabezpieczeń bazowych do użytku w całej organizacji.
Patrz NSC 800-37, Zadanie S-2, *Dostosowanie zabezpieczeń,* w celu zapewnienia dodatkowych wytycznych dotyczących dostosowywania zabezpieczeń bazowych do systemów i środowisk operacyjnych.

[24] Decyzje dotyczące dostosowywania mogą być podejmowane w oparciu o czas i możliwość zastosowania wybranych zabezpieczeń pod pewnymi warunkami. To znaczy, że środki bezpieczeństwa i ochrony prywatności mogą nie mieć zastosowania w każdej sytuacji, lub wartości parametrów dla operacji dostosowywania mogą ulec zmianie w pewnych okolicznościach.

[25] NSC 800-18 zawiera wskazówki dotyczące opracowywania planów bezpieczeństwa systemu. Wytyczne dotyczące opracowywania planów zarządzania ryzykiem w zakresie ochrony prywatności i łańcucha dostaw będę upublicznione w przyszłości.

wiarygodnych, opartych na ryzyku decyzji dotyczących bezpieczeństwa i ochrony prywatności oraz aby czynił to w sposób w pełni wspierający przejrzystość, identyfikowalność i odpowiedzialność.

2.4.1. Określanie i wyznaczanie zabezpieczeń wspólnych

Zabezpieczenia wspólne to środki bezpieczeństwa, które mogą być dziedziczone przez jeden lub więcej systemów organizacyjnych. Jeżeli system dziedziczy zabezpieczenie wspólne zapewnione przez inny podmiot (wewnętrzny lub zewnętrzny), nie ma możliwości wdrożenia tego zabezpieczenia w ramach tego systemu. Decyzje organizacyjne, w odniesieniu do których zabezpieczenia są wyznaczone jako zabezpieczenia wspólne, mogą mieć wpływ na obowiązki poszczególnych właścicieli systemów w odniesieniu do realizacji zabezpieczeń w ramach systemu podstawowego.[26] Dostawcy zabezpieczeń wspólnych zapewniają dostępność aktualnych informacji dotyczących wdrożenia oraz wyników oceny, co ułatwia właścicielom systemu oraz osobom autoryzującym podejmowanie decyzji. Właściciele systemów i osoby autoryzujące ustalają, czy zabezpieczenia wspólne dostępne w przypadku dziedziczenia, faktycznie zapewniają ochronę proporcjonalną do ryzyka związanego z dziedziczeniem systemów.[27]

Wyznaczanie i wdrażanie zabezpieczeń wspólnych może mieć wpływ na wydatki finansowe organizacji przeznaczone na zasoby. Ogólnie rzecz biorąc, im większa jest liczba wdrożonych zabezpieczeń wspólnych, tym większe są potencjalne oszczędności kosztów, ponieważ wspólne środki ochronne są amortyzowane przez wiele systemów. Dodatkowo, wdrożenie zabezpieczenia, jako zabezpieczenia wspólnego często zapewnia bardziej znormalizowane, stabilne, skalowalne i bezpieczne wdrożenie w całej organizacji, w przeciwieństwie do tego samego zabezpieczenia wdrażanego oddzielnie w wielu pojedynczych systemach.

[26] Więcej informacji na temat decyzji organizacyjnych dotyczących wyznaczania zabezpieczeń wspólnych można znaleźć w dokumencie NSC 800-37, Krok: *Przygotowanie zadań – poziom organizacyjny*, Zadanie P-5, *Identyfikacja zabezpieczeń wspólnych*. Więcej informacji na temat zabezpieczeń wspólnych, jako podejścia do wdrażania zabezpieczeń, można znaleźć w sekcji 2.3 publikacji NSC 800-53.

[27] Organizacje mogą również korzystać z zabezpieczeń hybrydowych. Zabezpieczenia hybrydowe są częściowo wdrażane przez jednego lub więcej dostawców zabezpieczeń wspólnych, a częściowo przez system.

2.4.2. Stosowanie rozważań dotyczących zakresu stosowania i wdrażania

Stosowanie rozważań dotyczących zakresu stosowania i wdrażania, w połączeniu z wytycznymi dotyczącymi zarządzania ryzykiem, zapewniają organizacjom bardziej szczegółowe podstawy do podejmowania decyzji opartych na ryzyku.[28] Zastosowanie rozważań dotyczących zakresu stosowania i wdrażania, może wyeliminować zbędne zabezpieczenia z początkowych zabezpieczeń bazowych i zapewnić, że organizacje wybiorą ***tylko*** te zabezpieczenia, które są potrzebne, a ponadto zapewnią poziom ochrony proporcjonalny do ryzyka. Organizacje mogą stosować opisane poniżej rozważania dotyczące zakresu stosowania i wdrażania, które mogą pomóc im w podejmowaniu decyzji opartych na ryzyku odnoszącym się do wyboru i specyfikacji zabezpieczeń.

- ***Wdrażanie, zastosowanie oraz zasady przydzielania zabezpieczeń***

Rosnąca złożoność systemów wymaga dokładnej analizy w zakresie wdrażania środków bezpieczeństwa i ochrony prywatności. Wstępne zabezpieczenia bazowe mogą nie mieć zastosowania do każdego elementu systemu. Środki bezpieczeństwa mają zastosowanie tylko do tych komponentów systemu, które zapewniają lub wspierają funkcje lub możliwości w zakresie bezpieczeństwa lub ochrony prywatności objęte tymi zabezpieczeniami.[29] Organizacje podejmują decyzje w oparciu o ryzyko dotyczące tego, gdzie w systemach organizacji należy zastosować lub przydzielić konkretne środki bezpieczeństwa, umożliwiające osiągnięcie wymaganej funkcji lub możliwości w zakresie bezpieczeństwa lub prywatności oraz spełnienie wymogów bezpieczeństwa i ochrony prywatności.

- ***Względy operacyjne i środowiskowe***

Niektóre środki bezpieczeństwa z zabezpieczeń bazowych zakładają istnienie czynników operacyjnych lub środowiskowych. W przypadku, gdy czynniki operacyjne lub środowiskowe

[28] Wymienione w tej części rozważania dotyczące zakresu stosowania i wdrażania są przykładami i ***nie*** mają na celu ograniczania organizacji w podejmowaniu decyzji dotyczących świadczenia usług w oparciu o inne, określone przez organizację rozważania wraz z odpowiednim uzasadnieniem lub przesłaniem organizacyjnym.

[29] Na przykład, zabezpieczenia audytowe są zazwyczaj stosowane do komponentów systemu, które zapewniają możliwości audytowe i nie muszą być stosowane do każdego komponentu na poziomie użytkownika w organizacji.

nie występują lub znacznie odbiegają od założeń bazowych opisanych w sekcji 2.3, uzasadnione jest dostosowanie zabezpieczeń bazowych. Wspólne czynniki operacyjne i środowiskowe obejmują urządzenia i operacje mobilne; systemy i operacje wykonywane przez jednego użytkownika; dostępność i przepustowość danych; systemy o bardzo ograniczonej lub sporadycznej przepustowości, takie jak systemy taktyczne wspierające misje wojskowe lub organów ścigania; systemy cyberfizyczne, czujniki i urządzenia wykorzystujące Internet rzeczy (IoT); systemy o limitowanej funkcjonalności, takie jak faksy, drukarki i aparaty cyfrowe; systemy, które przetwarzają, przechowują lub przesyłają nietrwałe informacje lub które wykorzystują technikę wirtualizacji, tworząc nietrwałe instancje systemów operacyjnych i aplikacji; oraz systemy, które wymagają publicznego dostępu.

- ***Rozważania dotyczące technologii***

Zabezpieczenia, które odnoszą się do konkretnych technologii - takich jak technologie bezprzewodowe, kryptograficzne lub infrastruktury klucza publicznego - mają zastosowanie tylko wtedy, gdy technologie te są wdrożone lub wymagane do stosowania w systemach organizacyjnych. Środki bezpieczeństwa, które mogą być skutecznie wspierane przez zautomatyzowane mechanizmy, nie wymagają opracowywania takich mechanizmów, jeżeli mechanizmy te jeszcze nie istnieją lub nie są łatwo dostępne w gotowych produktach komercyjnych lub rządowych. Jeżeli mechanizmy automatyczne są nie dostępne, opłacalne lub technicznie wykonalne, w celu spełnienia określonych wymogów zabezpieczeń podstawowych lub zabezpieczeń rozszerzonych można wdrożyć zabezpieczenia kompensacyjne za pomocą procedur lub mechanizmów nieautomatycznych.

- ***Misja i rozważania biznesowe***

Niektóre środki bezpieczeństwa mogą nie być odpowiednie, jeżeli ich wdrożenie może mieć potencjalnie negatywny wpływ na jakość, osłabić lub zakłócić misję organizacyjną lub funkcje biznesowe, w tym narażać na niebezpieczeństwo lub szkodzić osobom fizycznym. Jednakże decyzje dotyczące stosowności wdrażania zabezpieczeń zawsze powinny uwzględniać wymogi prawne, regulacyjne i ustanawianych polityk.

- ***Rozważania dotyczące atrybutów bezpieczeństwa***

Środki bezpieczeństwa, które zabezpieczają tylko jeden lub dwa z atrybutów bezpieczeństwa (tj. poufności, integralności, dostępności) mogą zostać obniżone do odpowiedniego zabezpieczenia niższego poziomu zabezpieczeń bazowych (lub zmodyfikowane, lub wyeliminowane, o ile nie są zdefiniowane na poziomie niższym zabezpieczenia bazowego) i tylko wtedy, gdy działanie obniżające ocenę: odzwierciedla kategoria bezpieczeństwa (zgodnie z NSC 199) obsługiwanych atrybutów bezpieczeństwa przed rozważeniem (zgodnie z NSC 200) poziomu wpływu (koncepcja najwyższej wartości - *high water mark*), jest poparte oceną ryzyka na poziomie organizacji i nie wpływa niekorzystnie na poziom ochrony informacji istotnych dla bezpieczeństwa w systemie. Na przykład, jeżeli system zostanie skategoryzowany za pomocą koncepcji najwyższej wartości, jako system o umiarkowanym poziomie wpływu, ponieważ potencjalny wpływ na poufność i/lub integralność jest umiarkowany, ale potencjalny wpływ na dostępność jest skategoryzowany jako niski, istnieją oddzielne zabezpieczenia, które wspierają jedynie atrybut dostępności i które potencjalnie mogą zostać zakwalifikowane jako zabezpieczenia o niskim poziomie wyjściowym. W tym scenariuszu właściwe może być powstrzymanie się od wdrożenia zabezpieczenia CP-2(1), ponieważ zabezpieczenie rozszerzone wspiera jedynie dostępność i jest wybierane w umiarkowanym poziomie bazowym, a nie w niskim poziomie bazowym.

Poniższe środki bezpieczeństwa i zabezpieczenia rozszerzone mogą zostać obniżone dla każdej z kategorii bezpieczeństwa:

- *Wspieranie tylko poufności:* AC-21, MA-3(3), MP-3, MP-4, MP-5, MP-6(1), MP-6(2), PE-4,PE-5, SC-4.
- *Wspieranie tylko integralności:* CM-5, CM-5(1), CM-5(3), SI-7, SI-7(1), SI-7(5), SI-10.
- *Wspieranie tylko dostępności:* CP-2(1), CP-2(2), CP-2(3), CP-2(5), CP-2(8), CP-3(1), CP-4(1), CP-4(2), CP-6, CP-6(1), CP-6(2), CP-6(3), CP-7, CP-7(1), CP-7(2), CP-7(3), CP-7(4), CP-7(6), CP-8,CP-8(1), CP-8(2), CP-8(3), CP-8(4), CP-8(5), CP-9(2), CP-9(3), CP-9(5), CP-9(6), CP-10(2), CP-10(4), CP-11, MA-6, PE-9, PE-10, PE-11, PE-11(1), PE-13(1), PE-13(2), PE-15(1).

- ***Względy prawne i dotyczące polityk***

Chociaż zabezpieczenia, które są stosowane w celu spełnienia wymogów prawnych, regulacyjnych lub dotyczących polityk, nie są dopasowane do zabezpieczeń bazowych, niektóre wymogi prawne, regulacyjne lub dotyczące polityk mogą mieć zastosowanie w określonych okolicznościach. Uzasadnione jest dostosowanie poziomu bazowego, jeżeli okoliczności nie mają zastosowania do organizacji lub niektórych systemów.[30]

2.4.3. Wybór zabezpieczeń kompensacyjnych

Zabezpieczenia kompensacyjne są stosowane przez organizacje zamiast specyficznych środków bezpieczeństwa z zabezpieczeń bazowych. Stosowanie zabezpieczeń kompensacyjnych jest właściwe, gdy środki bezpieczeństwa są z konieczności stosowane spoza zestawów zabezpieczeń bazowych, ale ochrona zapewniona przez te środki bezpieczeństwa pozwala zmniejszyć ryzyko do akceptowalnego poziomu. Zabezpieczenia kompensacyjne są często wybierane, gdy wdrożenie zabezpieczeń bazowych jest technicznie niewykonalne, nieefektywne kosztowo lub gdy wdrożenie zabezpieczeń ma negatywny wpływ na misję organizacyjną lub funkcje biznesowe.[31] W przypadku zastosowania rozważań dotyczących zakresu stosowania i wdrażania zabezpieczeń opartych na technologii, zabezpieczenia kompensacyjna mogą być tymczasowe i stosowane tylko do czasu, gdy system nie zostanie wdrożony do eksploatacji.

Zabezpieczenia kompensacyjne mają na celu zapewnienie równoważnej lub porównywalnej ochrony[32] systemów, organizacji i osób fizycznych.[33] Zabezpieczenia kompensacyjne są

[30] Chodzi tu o sytuację, gdy przepisy prawa narzucają określone zabezpieczenia, nawet wtedy, gdy nie wynika to z szacowania ryzyka.

[31] Na przykład, w niektórych aplikacjach biznesowych lub misjach czasu rzeczywistego w miejsce blokady urządzenia można zastosować dodatkowe środki bezpieczeństwa fizycznego. W małej organizacji zamiast rozdzielania obowiązków można wdrożyć częstsze audyty, ukierunkowane szkolenia w zakresie ról lub bardziej rygorystyczne kontrolowanie personelu. Zamiast mechanizmów automatycznych można wdrożyć dobrze określone procedury, ukierunkowane szkolenia w oparciu o role oraz częstsze audyty.

[32] Zabezpieczenia kompensacyjne nie są stosowane w celu uniknięcia konieczności spełnienia wymagań bezpieczeństwa. Stosowanie takich zabezpieczeń zapewnia raczej alternatywne i odpowiednie zabezpieczenia i ochronę prywatności w celu ułatwienia zarządzania ryzykiem.

[33] Może być wymagane więcej niż jedno zabezpieczenie kompensacyjne w celu zapewnienia równoważnego środka bezpieczeństwa, który został dostosowany do poziomu zabezpieczenia bazowego.

wybierane po uwzględnieniu rozważań dotyczących procesu dostosowywania. W celu użycia zabezpieczeń kompensacyjnych, organizacje:

- Wybierają zabezpieczenia kompensacyjne z katalogu zabezpieczeń NSC 800-53.
- Uzasadniają, w jaki sposób zabezpieczenia kompensacyjne spełniają wymogi bezpieczeństwa lub ochrony prywatności oraz dlaczego nie można było wdrożyć zabezpieczeń bazowych.
- W przypadku, gdy odpowiednie zabezpieczenia kompensacyjne nie są dostępne w publikacji NSC 800-53, przyjmują odpowiednie zabezpieczenia kompensacyjne z innych źródeł.[34]
- Oceniają i akceptują zagrożenia bezpieczeństwa i prywatności związane z wdrożeniem zabezpieczeń kompensacyjnych.

2.4.4. Przypisywanie wartości parametrów zabezpieczeń

Zabezpieczenia podstawowe i zabezpieczenia rozszerzone zawierające wbudowane parametry (tj. *oświadczenie o przydzieleniu* oraz *deklaracja wyboru)* dają organizacjom elastyczność w określaniu wartości dla niektórych zabezpieczeń podstawowych i zabezpieczeń rozszerzonych, w celu wsparcia określonych wymagań organizacyjnych. Po przeprowadzeniu rozważań dotyczących zakresu stosowania i wdrażania zabezpieczeń kompensacyjnych, organizacje dokonują przeglądu zabezpieczeń podstawowych i zabezpieczeń rozszerzonych dla operacji przypisania lub wyboru i określają odpowiednie wartości zdefiniowane przez organizację dla zidentyfikowanych parametrów. Wartości parametrów mogą wynikać z misji lub wymagań biznesowych lub wartości te mogą być określone przez przepisy prawa, regulacje wewnętrzne, polityki, standardy, wytyczne lub najlepsze praktyki biznesowe.

[34] Organizacje dokładają wszelkich starań, aby wybrać zabezpieczenia kompensacyjne ze skonsolidowanego katalogu zabezpieczeń przedstawionego w publikacji NSC 800-53. Zdefiniowane przez organizację zabezpieczenia kompensacyjne są stosowane ***tylko*** wtedy, gdy organizacje stwierdzą, że katalog zabezpieczeń nie zawiera odpowiednich zabezpieczeń kompensacyjnych.

Po określeniu przez organizacje wartości parametrów dla zabezpieczeń podstawowych i zabezpieczeń rozszerzonych, określone wartości zakresu stosowania i wdrażania stają się stałą częścią zabezpieczeń podstawowych i zabezpieczeń rozszerzonych. Jako takie, są one dokumentowane w planach programów bezpieczeństwa i ochrony prywatności lub planach bezpieczeństwa i ochrony prywatności systemów, w zależności od potrzeb. Organizacje mogą określić wartości parametrów przed wyborem zabezpieczeń kompensacyjnych, ponieważ specyfikacja parametrów uzupełnia definicje środków bezpieczeństwa i może mieć wpływ na potrzebę stosowania zabezpieczeń kompensacyjnych. Współpraca przy opracowywaniu wartości parametrów zabezpieczeń może przynieść znaczące korzyści. W przypadku organizacji, które współpracują ze sobą często lub regularnie przeprowadzają wymianę informacji, przydatne może być opracowanie wzajemnie uzgodnionego zestawu wartości parametrów zabezpieczeń.

2.4.5. Uzupełnianie zabezpieczeń bazowych

W pewnych sytuacjach mogą być wymagane dodatkowe zabezpieczenia podstawowe i zabezpieczenia rozszerzone wykraczające poza zabezpieczenia podstawowe i zabezpieczenia rozszerzone zawarte w zabezpieczeniach bazowych w rozdziale trzecim, aby przeciwdziałać konkretnym zagrożeniom dla organizacji, misji i procesów biznesowych oraz systemów, w celu uwzględnienia szczególnych rodzajów danych osobowych i związanych z tym zagrożeń dla prywatności oraz aby spełnić wymagania dotyczące aspektów prawnych, polityk, regulacji wewnętrznych, standardów i wytycznych. Organizacyjne oceny ryzyka dostarczają informacji do określenia konieczności i wystarczalności zabezpieczeń podstawowych i zabezpieczeń rozszerzonych w zakresie zabezpieczeń bazowych. Zachęca się organizacje do maksymalnego wykorzystania katalogu zabezpieczeń przedstawionych w publikacji NSC 800-53, celem uzupełnienia zabezpieczeń bazowych o dodatkowe zabezpieczenia podstawowe i zabezpieczenia rozszerzone.

2.4.6. Dostarczanie dodatkowych specyfikacji w celu wdrożenia zabezpieczeń

Ponieważ zabezpieczenia podstawowe i zabezpieczenia rozszerzone są oświadczeniami o funkcjach i właściwościach bezpieczeństwa lub ochrony prywatności, które są

przekazywane na wyższych poziomach abstrakcji, zabezpieczenia mogą nie posiadać wystarczających informacji wdrożeniowych. W związku z tym konieczne może okazać się podanie dodatkowych szczegółów w celu pełnego określenia przeznaczenia danego zabezpieczenia do celów wdrożenia oraz zapewnienia, że wymogi bezpieczeństwa i ochrony prywatności związane z tym zabezpieczeniem są spełnione. Na przykład, dodatkowe informacje mogą być dostarczone, jako część procesu przechodzenia od zabezpieczenia do wymogów specyfikacji i mogą obejmować dopracowanie szczegółów wykonania, dopracowanie zakresu lub iterację, która ma być stosowana w celu zastosowania tego samego zabezpieczenia w inny sposób do różnych zakresów. Potrzeba zapewnienia informacji o specyfikacji zabezpieczenia pojawia się rutynowo, gdy zabezpieczenie jest stosowane w procesie inżynierii systemowej w ramach wymagań tej inżynierii. Organizacje zapewniają, że jeśli istniejące informacje dotyczące środków bezpieczeństwa nie są wystarczające do określenia zamierzonych szczegółów realizacji zabezpieczeń, informacje takie są dostarczane właścicielom systemów i dostawcom zabezpieczeń wspólnych. Organizacje mają możliwość elastycznego określania, czy informacje dotyczące specyfikacji zabezpieczeń są zawarte w deklaracji zgodności lub w osobnej sekcji dodatku zgodności. Przy podawaniu dodatkowych szczegółów, organizacje są pouczane, aby nie zmieniać intencji zabezpieczeń bazowych, ani nie modyfikować oryginalnego języka w zabezpieczeniu. Informacje dotyczące wdrożenia są udokumentowane w planach bezpieczeństwa i ochrony prywatności systemu.

2.5. ZESTAW MOŻLIWOŚCI ZABEZPIECZEŃ

Organizacje rozważają zdefiniowanie zestawu możliwości, jako wstępnego elementu procesu wyboru zabezpieczeń. Koncepcja *możliwości* uznaje, że spełnienie wymogów bezpieczeństwa lub prywatności rzadko wynika z pojedynczego zabezpieczenia, ale raczej z zestawu wzajemnie wzmacniających się środków bezpieczeństwa. Na przykład, organizacje mogą chcieć zdefiniować zdolność do bezpiecznego zdalnego uwierzytelniania. Ta zdolność może być osiągnięta poprzez wybór i implementację zestawu zabezpieczeń z publikacji NSC 800-53, takich jak IA-2 (1), IA-2 (2), IA-2 (8), IA-2 (9) i SC-8 (1). Ponadto możliwości mogą dotyczyć różnych obszarów, które mogą obejmować środki techniczne, środki fizyczne,

środki proceduralne lub dowolną ich kombinację. Oprócz wyżej wymienionych możliwości bezpiecznego zdalnego dostępu, organizacje mogą również wymagać posiadania zapewniania bezpieczeństwa środków fizycznych, takich jak wykrywanie naruszeń modułu kryptograficznego lub wykrywanie/analizowanie anomalii.

W miarę jak liczba zabezpieczeń zawartych w NSC 800-53 rośnie w odpowiedzi na coraz bardziej wyrafinowaną przestrzeń zagrożenia, ważne jest, aby organizacje miały możliwość opisania kluczowych zdolności potrzebnych do ochrony misji organizacji i funkcji biznesowych, a następnie wybrania zabezpieczeń, które - jeśli są odpowiednio zaprojektowane, opracowane i wdrożone - zapewniają takie zdolności. Wykorzystanie różnych możliwości zabezpieczeń upraszcza koncepcyjne postrzeganie problemu ochrony. Wykorzystanie konstrukcji zdolności zapewnia metodę grupowania zabezpieczeń, które są wykorzystywane do wspólnego celu lub do osiągnięcia wspólnego zamierzonego efektu. Na przykład, grupowanie środków bezpieczeństwa jest ważnym aspektem przy ocenie zabezpieczeń pod kątem skuteczności.[35]

Tradycyjnie oceny przeprowadzano na zasadzie "zabezpieczenie po zabezpieczeniu", uzyskują wyniki określane jako pozytywne (tzn. zabezpieczenie zapewnione) lub negatywne (tzn. zabezpieczenie niezapewnione). Jednak niepowodzenie pojedynczego zabezpieczenia lub w niektórych przypadkach wielu zabezpieczeń, może nie mieć wpływu na ogólną zdolność organizacji. Ponadto zastosowanie szerszej koncepcji posiadanych przez zabezpieczenie możliwości, pozwala organizacji na ocenę powagi słabych punktów w jej systemach i określenie, czy niepowodzenie określonego środka bezpieczeństwa lub decyzja o niestosowaniu danego zabezpieczenia, wpływa na zdolność potrzebną do ochrony misji i działalności. Ułatwia to również przeprowadzenie analizy *przyczyn źródłowych w* celu ustalenia, czy niepowodzenie jednego środka bezpieczeństwa można prześledzić na podstawie ustalonych relacji tego zabezpieczenia z innymi środkami bezpieczeństwa. Ostatecznie, decyzje autoryzacyjne (tj. decyzje o akceptacji ryzyka) są podejmowane na

[35] NIST Interagency Report 8011, Vol. 1 [IR8011v1], opisuje grupowanie środków bezpieczeństwa według celu ułatwienia automatycznej oceny zabezpieczeń.

podstawie stopnia, w jakim pożądane zdolności zostały osiągnięte i spełniają wymogi bezpieczeństwa i ochrony prywatności określone przez organizację. Te oparte na ryzyku decyzje są bezpośrednio związane z organizacyjną tolerancją ryzyka, która jest zdefiniowana w ramach strategii zarządzania ryzykiem w organizacji.

ROZDZIAŁ TRZECI

ZABEZPIECZENIA BAZOWE

BAZOWE ŚRODKI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

W tabelach od 3-1 do 3-20 przedstawiono wykaz zabezpieczeń podstawowych i zabezpieczeń rozszerzonych przypisanych do kategorii zabezpieczeń zawartych w standardzie NSC 800-53. Dokonano odpowiedniego przydziału zabezpieczeń z NSC 800-53 do bazowych zabezpieczeń prywatności oraz do bazowych środków bezpieczeństwa o niskim, umiarkowanym i wysokim poziomie wpływu na bezpieczeństwo. W sekcji 2.2 przedstawiono dodatkowe informacje na temat kryteriów wyboru zabezpieczeń prywatności.

PODSTAWOWE RELACJE W ZAKRESIE BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Zabezpieczenia podstawowe i zabezpieczenia rozszerzone, które są przypisane do bazowych środków bezpieczeństwa, są wykorzystywane do zarządzania ryzykiem wynikającym z utraty poufności, integralności i dostępności (systemów lub informacji organizacyjnych).

SAOP są odpowiedzialni za zarządzanie ryzykiem związanym z prywatnością, a ponieważ ryzyko związane z prywatnością wynika zarówno z przetwarzania danych osobowych, jak i utraty poufności, integralności i dostępności danych osobowych, ważne jest, aby organizacje uwzględniły sposób współpracy programów ochrony prywatności i bezpieczeństwa w zakresie działań związanych z tymi zabezpieczeniami, tj. działań takich jak kategoryzacja, dostosowywanie, wdrażanie i ocena.

1. Zabezpieczenia podstawowe i zabezpieczenia rozszerzone, które są przypisane (**zaznaczone w tabelach 3-1 do 3-20 znakiem "X"**) tylko do zabezpieczeń bazowych prywatności, a nie do bazowych środków bezpieczeństwa, są istotne dla zarządzania programem ochrony prywatności, ale generalnie nie wspierają zarządzania ryzykiem wynikającym z utraty poufności, integralności i dostępności.
2. Zabezpieczenia podstawowe i zabezpieczenia rozszerzone, które są przypisane (**zaznaczone w tabelach 3-1 do 3-20 znakiem "X"**) zarówno do zabezpieczeń bazowych prywatności, jaki i bazowych środków bezpieczeństwa, są wykorzystywane do zarządzania programem ochrony prywatności oraz ryzykiem wynikającym z utraty poufności, integralności i dostępności (w tym danych osobowych).
3. Niektóre zabezpieczenia podstawowe i zabezpieczenia rozszerzone nie są przypisane (**puste miejsca w tabelach 3-1 do 3-20**) do żadnych zabezpieczeń bazowych. Poprzez dostosowywanie, ***organizacje dokonują własnych ustaleń***, co do tego, czy zabezpieczenia te są niezbędne do spełnienia odpowiednich wymagań, lub mogą być wykorzystywane w ramach zarządzania ryzykiem wynikającym z utraty poufności, integralności, dostępności lub przetwarzania danych osobowych.

3.1. KATEGORIA AC - KONTROLA DOSTĘPU

Tabela 3-1 zawiera podsumowanie zabezpieczeń podstawowych i zabezpieczeń rozszerzonych przypisanych do *kategorii AC - Kontrola dostępu*. Zabezpieczenia są przypisane do bazowych zabezpieczeń prywatności oraz do bazowych środków bezpieczeństwa o niskim, umiarkowanym i wysokim poziomie wpływu, w zależności od potrzeb. Zabezpieczenie podstawowe lub zabezpieczenie rozszerzone, które zostało wycofane z katalogu zabezpieczeń lub przeniesione do innej kategorii zabezpieczeń, jest oznaczone symbolem "W" z objaśnieniem dokonanym czcionką kursywa w jasnoszarym kolorze, z podaniem miejsca umieszczenia wycofanego / przeniesionego zabezpieczenia podstawowego lub zabezpieczenia rozszerzonego.

TABELA 3-1: KATEGORIA AC - KONTROLA DOSTĘPU

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
AC-1	**POLITYKA I PROCEDURY**	X[36]	X[37]	X	X
AC-2	**ZARZĄDZANIE KONTAMI**	[38]	X	X	X
AC-2(1)	AUTOMATYCZNE ZARZĄDZANIE KONTEM SYSTEMU			X	X

[36] Patrz: *Podstawowe relacje w zakresie bezpieczeństwa i ochrony prywatności – pkt. 2*. Dotyczy to tabel 3.1. do 3.20.
[37] Patrz: *Podstawowe relacje w zakresie bezpieczeństwa i ochrony prywatności – pkt. 1*. Dotyczy to tabel 3.1. do 3.20.
[38] Patrz: *Podstawowe relacje w zakresie bezpieczeństwa i ochrony prywatności – pkt. 3*. Dotyczy to tabel 3.1. do 3.20.

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
AC-2(2)	AUTOMATYCZNE ZARZĄDZANIE KONTEM CZASOWYM | AWARYJNYM			X	X
AC-2(3)	WYŁĄCZANIE KONT			X	X
AC-2(4)	AUTOMATYCZNE DZIAŁANIA AUDYTOWE			X	X
AC-2(5)	WYLOGOWANIE PRZEZ UŻYTKOWNIKA PO OKREŚLONYM OKRESIE NIEAKTYWNOŚCI			X	X
AC-2(6)	DYNAMICZNE ZARZĄDZANIE UPRAWNIENIAMI				
AC-2(7)	UPRZYWILEJOWANE KONTA UŻYTKOWNIKÓW				
AC-2(8)	DYNAMICZNE ZARZĄDZANIE KONTEM				
AC-2(9)	OGRANICZENIA W KORZYSTANIU Z KONT WSPÓLNYCH I GRUPOWYCH				
AC-2(10)	*ZMIANA POŚWIADCZANIA UPRAWNIEŃ KONTA WSPÓLNEGO I GRUPOWEGO*	*W: włączone do AC-2k.*			
AC-2(11)	WARUNKI UŻYTKOWANIA				X
AC-2(12)	MONITOROWANIE KONTA POD WZGLĘDEM NIETYPOWYCH ZASTOSOWAŃ				X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
AC-2(13)	WYŁĄCZANIE KONT DOSTĘPOWYCH UŻYTKOWNIKOM WYSOKIEGO RYZYKA			X	X
AC-3	**EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU**		X	X	X
AC-3(1)	*OGRANICZONY DOSTĘP DO FUNKCJI UPRZYWILEJOWANYCH*	*W: włączone do AC-6.*			
AC-3(2)	PODWÓJNA AUTORYZACJA				
AC-3(3)	OBOWIĄZKOWA KONTROLA DOSTĘPU				
AC-3(4)	UZNANIOWA KONTROLA DOSTĘPU				
AC-3(5)	INFORMACJE DOTYCZĄCE BEZPIECZEŃSTWA				
AC-3(6)	*OCHRONA INFORMACJI UŻYTKOWNIKA I SYSTEMU*	*W: włączone do MP-4 i SC-28.*			
AC-3(7)	KONTROLA DOSTĘPU OPARTA NA ROLI				
AC-3(8)	COFNIĘCIE ZEZWOLEŃ NA DOSTĘP				
AC-3(9)	KONTROLOWANE UDOSTĘPNIENIE INFORMACJI				
AC-3(10)	NADZOROWANE OBEJŚCIE MECHANIZMÓW KONTROLI DOSTĘPU				
AC-3(11)	OGRANICZENIE DOSTĘPU DO OKREŚLONYCH RODZAJÓW INFORMACJI				
AC-3(12)	ZAPEWNIENIE I EGZEKWOWANIE DOSTĘPU DO APLIKACJI				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
AC-3(13)	KONTROLA DOSTĘPU NA PODSTAWIE ATRYBUTÓW				
AC-3(14)	DOSTĘP INDYWIDUALNY	X			
AC-3(15)	UZNANIOWA I OBOWIĄZKOWA KONTROLA DOSTĘPU				
AC-4	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI**			X	X
AC-4(1)	BEZPIECZEŃSTWO OBIEKTÓW I ATRYBUTY PRYWATNOŚCI				
AC-4(2)	PRZETWARZANIE DOMEN				
AC-4(3)	DYNAMICZNA KONTROLA PRZEPŁYWU INFORMACJI				
AC-4(4)	KONTROLA PRZEPŁYWU ZASZYFROWANYCH INFORMACJI				X
AC-4(5)	WBUDOWANE RODZAJE DANYCH				
AC-4(6)	METADANE				
AC-4(7)	MECHANIZMY PRZEPŁYWU JEDNOKIERUNKOWEGO				
AC-4(8)	FILTRY POLITYKI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI				
AC-4(9)	OCENA PRZEZ UPRAWNIONĄ OSOBĘ				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
AC-4(10)	WŁĄCZANIE I WYŁĄCZANIE FILTRÓW BEZPIECZEŃSTWA LUB POLITYKI PRYWATNOŚCI				
AC-4(11)	KONFIGURACJA FILTRÓW BEZPIECZEŃSTWA LUB POLITYKI PRYWATNOŚCI				
AC-4(12)	IDENTYFIKATORY TYPÓW DANYCH				
AC-4(13)	DEKOMPOZYCJA INFORMACJI NA ODPOWIEDNIE PODSKŁADNIKI				
AC-4(14)	POLITYKA STOSOWANIA FILTRÓW BEZPIECZEŃSTWA LUB OCHRONY PRYWATNOŚCI				
AC-4(15)	WYKRYWANIE INFORMACJI NIEAKCEPTOWANYCH				
AC-4(16)	*PRZEKAZYWANIE INFORMACJI POMIĘDZY SYSTEMAMI*	*W: włączone do AC-4.*			
AC-4(17)	UWIERZYTELNIANIE DOMEN				
AC-4(18)	*POWIĄZANIE ATRYBUTÓW BEZPIECZEŃSTWA*	*W: włączone do AC-16.*			
AC-4(19)	UWIERZYTELNIANIE METADANYCH				
AC-4(20)	ZATWIERDZONE ROZWIĄZANIA BEZPIECZEŃSTWA				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
AC-4(21)	FIZYCZNA LUB LOGICZNA SEPARACJA PRZEPŁYWÓW INFORMACJI				
AC-4(22)	TYLKO DOSTĘP				
AC-4(23)	MODYFIKACJA INFORMACJI, KTÓRYCH NIE MOŻNA UDOSTĘPNIAĆ				
AC-4(24)	WEWNĘTRZNY ZNORMALIZOWANY FORMAT				
AC-4(25)	SANITYZACJA DANYCH				
AC-4(26)	AUDYT DZIAŁAŃ FILTRUJĄCYCH				
AC-4(27)	REDUNDANTNE / NIEZALEŻNE MECHANIZMY FILTRACJI				
AC-4(28)	KASKADOWY FILTR TREŚCI				
AC-4(29)	SILNIKI ARANŻACJI FILTROWANIA				
AC-4(30)	MECHANIZMY FILTRUJĄCE WYKORZYSTUJĄCE PROCESY WIELOKROTNE				
AC-4(31)	ZAPOBIEGANIE PRZENOSZENIU NIEWŁAŚCIWYCH TREŚCI				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
AC-4(32)	WYMAGANIA DOTYCZĄCE PROCESU PRZEKAZYWANIA INFORMACJI				
AC-5	**ROZDZIAŁ OBOWIĄZKÓW**			X	X
AC-6	**ZASADA WIEDZY KONIECZNEJ**			X	X
AC-6(1)	UPOWAŻNIONY DOSTĘPU DO FUNKCJI BEZPIECZEŃSTWA			X	X
AC-6(2)	NIEUPRZYWILEJOWANY DOSTĘP DLA FUNKCJI NIEZWIĄZANYCH Z BEZPIECZEŃSTWEM			X	X
AC-6(3)	DOSTĘP SIECIOWY DO UPRZYWILEJOWANYCH POLECEŃ				X
AC-6(4)	ODDZIELNE DOMENY PRZETWARZANIA				
AC-6(5)	UPRZYWILEJOWANE KONTA			X	X
AC-6(6)	UPRZYWILEJOWANY DOSTĘP PRZEZ UŻYTKOWNIKÓW NIEORGANIZACYJNYCH				
AC-6(7)	PRZEGLĄD UPRAWNIEŃ UŻYTKOWNIKA			X	X
AC-6(8)	POZIOMY UPRAWNIEŃ DO WYKONYWANIA KODU				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
AC-6(9)	KONTROLA WYKORZYSTANIA UPRZYWILEJOWANYCH FUNKCJI			X	X
AC-6(10)	ODMOWA WYKONYWANIA PRZEZ NIEUPRZYWILEJOWANYCH UŻYTKOWNIKÓW UPRZYWILEJOWANYCH FUNKCJI			X	X
AC-7	**NIEUDANE PRÓBY LOGOWANIA**		X	X	X
AC-7(1)	*AUTOMATYCZNE ZAMKNIĘCIE KONTA*	*W: włączone do AC-7.*			
AC-7(2)	USUWANIE INFORMACJI Z URZĄDZEŃ PRZENOŚNYCH				
AC-7(3)	OGRANICZENIE PRÓB LOGOWANIA BIOMETRYCZNEGO				
AC-7(4)	UŻYCIE ALTERNATYWNEGO CZYNNIKA UWIERZYTELNIANIA				
AC-8	**POWIADOMIENIE O ZASADACH UŻYCIA SYSTEMU**		X	X	X
AC-9	**POWIADOMIENIE O POPRZEDNIM ZALOGOWANIU**				
AC-9(1)	NIEUDANE LOGOWANIE				
AC-9(2)	UDANE I NIEUDANE LOGOWANIE				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
AC-9(3)	POWIADAMIANIE O ZMIANACH W KONCIE				
AC-9(4)	DODATKOWE INFORMACJE DOTYCZĄCE LOGOWANIA				
AC-10	**KONTROLA ILOŚCI RÓWNOCZESNYCH SESJI**				X
AC-11	**BLOKADA URZĄDZENIA**			X	X
AC-11(1)	WYGASZACZ EKRANU			X	X
AC-12	**ZAKOŃCZENIE SESJI**			X	X
AC-12(1)	WYLOGOWANIE INICJOWANE PRZEZ UŻYTKOWNIKA				
AC-12(2)	KOMUNIKAT O ZAKOŃCZENIU SESJI (WYLOGOWANIU)				
AC-12(3)	KOMUNIKAT OSTRZEGAWCZY O PRZEKROCZENIU LIMITU CZASU				
AC-13	***NADZÓR I PRZEGLĄD KONTROLI DOSTĘPU***	*W: włączone do AC-2 i AU-6.*			
AC-14	**DZIAŁANIA DOZWOLONE BEZ IDENTYFIKACJI LUB UWIERZYTELNIENIA**		X	X	X
AC-14(1)	*NIEZBĘDNE ZASTOSOWANIA*	*W: włączone do AC-2 i AU-6.*			

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
AC-15	*ZNAKOWANIE AUTOMATYCZNE*	*W: włączone do AC-2 i AU-6.*			
AC-16	**ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI**				
AC-16(1)	DYNAMICZNE KOJARZENIE ATRYBUTÓW				
AC-16(2)	ZMIANY WARTOŚCI ATRYBUTÓW PRZEZ UPOWAŻNIONE OSOBY				
AC-16(3)	UTRZYMANIE KOJARZENIA ATRYBUTÓW PRZEZ SYSTEM INFORMATYCZNY				
AC-16(4)	KOJARZENIE ATRYBUTÓW PRZEZ AUTORYZOWANY PERSONEL				
AC-16(5)	ATRYBUTY BEZPIECZEŃSTWA PREZENTOWANE NA WYŚWIETLACZACH URZĄDZEŃ WYJŚCIOWYCH				
AC-16(6)	ZARZĄDZANIE POWIĄZANYMI ATRYBUTAMI				
AC-16(7)	INTERPRETACJA WSPÓLNYCH ATRYBUTÓW				
AC-16(8)	TECHNIKI I TECHNOLOGIE WIĄZANIA				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
AC-16(9)	PONOWNY PRZYDZIAŁ ATRYBUTÓW - MECHANIZMY ZMIANY KLASYFIKACJI				
AC-16(10)	KONFIGURACJA ATRYBUTÓW PRZEZ UPOWAŻNIONE OSOBY				
AC-17	**DOSTĘP ZDALNY**		X	X	X
AC-17(1)	AUTOMATYCZNE MONITOROWANIE I KONTROLA			X	X
AC-17(2)	OCHRONA POUFNOŚCI I INTEGRALNOŚCI Z WYKORZYSTANIEM SZYFROWANIA			X	X
AC-17(3)	ZARZĄDZANE PUNKTY KONTROLI DOSTĘPU			X	X
AC-17(4)	POLECENIA UPRZYWILEJOWANE I DOSTĘP			X	X
AC-17(5)	*MONITOROWANIE NIEAUTORYZOWANYCH POŁĄCZEŃ*	*W: włączone do SI-4.*			
AC-17(6)	OCHRONA MECHANIZMÓW DOSTĘPU ZDALNEGO				
AC-17(7)	*DODATKOWA OCHRONA DOSTĘPU DO FUNKCJI BEZPIECZEŃSTWA*	*W: włączone do AC-3(10).*			
AC-17(8)	*WYŁĄCZANIE NIEZABEZPIECZONYCH PROTOKOŁÓW SIECIOWYCH*	*W: włączone do CM-7.*			

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
AC-17(9)	ODŁĄCZENIE LUB WYŁĄCZENIE DOSTĘP				
AC-17(10)	UWIERZYTELNIANIE ZDALNYCH POLECEŃ				
AC-18	**DOSTĘP BEZPRZEWODOWY**		X	X	X
AC-18(1)	UWIERZYTELNIANIE ORAZ SZYFROWANIE			X	X
AC-18(2)	*MONITOROWANIE POŁĄCZEŃ NIEAUTORYZOWANYCH*	*W: włączone do SI-4.*			
AC-18(3)	DEZAKTYWACJA SIECI BEZPRZEWODOWEJ			X	X
AC-18(4)	OGRANICZENIE DOKONYWANIE KONFIGURACJI PRZEZ UŻYTKOWNIKÓW				X
AC-18(5)	POZIOMY MOCY ANTEN / TRANSMISJI				X
AC-19	**KONTROLA DOSTĘPU DO URZĄDZEŃ PRZENOŚNYCH**		X	X	X
AC-19(1)	*KORZYSTANIE Z ZAPISYWALNYCH I PRZENOŚNYCH URZĄDZEŃ MAGAZYNUJĄCYCH*	*W: włączone do MP-7.*			
AC-19(2)	*KORZYSTANIE Z OSOBISTYCH PRZENOŚNYCH URZĄDZEŃ MAGAZYNUJĄCYCH*	*W: włączone do MP-7.*			

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
AC-19(3)	*KORZYSTANIE Z OGÓLNODOSTĘPNYCH PRZENOŚNYCH URZĄDZEŃ MAGAZYNUJĄCYCH*	*W: włączone do MP-7.*			
AC-19(4)	OGRANICZENIA DOTYCZĄCE INFORMACJI NIEJAWNYCH				
AC-19(5)	SZYFROWANIE ZAWARTOŚCI CAŁEGO URZĄDZENIA / WYBRANYCH ZASOBÓW URZĄDZENIA			X	X
AC-20	**WYKORZYSTANIE SYSTEMÓW ZEWNĘTRZNYCH**		X	X	X
AC-20(1)	OGRANICZENIA AUTORYZOWANEGO DOSTĘPU			X	X
AC-20(2)	PRZENOŚNE URZĄDZENIA MAGAZYNUJĄCE - OGRANICZONE ZASTOSOWANIE			X	X
AC-20(3)	SYSTEMY NIE NALEŻĄCE ORGANIZACJI - OGRANICZONE ZASTOSOWANIE				
AC-20(4)	SIECIOWE URZĄDZENIA MAGAZYNUJĄCE - ZAKAZ UŻYWANIA				
AC-20(5)	PRZENOŚNE URZĄDZENIA MAGAZYNUJĄCE - ZAKAZ UŻYWANIA				
AC-21	**UDOSTĘPNIANIE INFORMACJI**			X	X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
AC-21(1)	AUTOMATYCZNE WSPARCIE DECYZJI				
AC-21(2)	WYSZUKIWANIE I ODZYSKIWANIE INFORMACJI				
AC-22	**TREŚCI PUBLICZNIE DOSTĘPNE**		X	X	X
AC-23	**OCHRONA PRZED PRZESZUKIWANIEM DANYCH**				
AC-24	**PRZYZNAWANIE PRAW DOSTĘPU**				
AC-24(1)	PRZESYŁANIE INFORMACJI O AUTORYZACJI DOSTĘPU				
AC-24(2)	BRAK TOŻSAMOŚCI UŻYTKOWNIKA LUB PROCESU				
AC-25	**MONITOR REFERENCYJNY**				

3.2. KATEGORIA AT - UŚWIADAMIANIE I SZKOLENIA

Tabela 3-2 zawiera podsumowanie zabezpieczeń podstawowych i zabezpieczeń rozszerzonych przypisanych do Kategorii AT - Uświadamianie i szkolenia. Zabezpieczenia są przypisane do bazowych zabezpieczeń prywatności oraz do bazowych środków bezpieczeństwa o niskim, umiarkowanym i wysokim poziomie wpływu, w zależności od potrzeb. Zabezpieczenie podstawowe lub zabezpieczenie rozszerzone, które zostało wycofane z katalogu zabezpieczeń lub przeniesione do innej kategorii zabezpieczeń, jest oznaczone symbolem "W" z objaśnieniem dokonanym czcionką kursywa w jasnoszarym kolorze, z podaniem miejsca umieszczenia wycofanego / przeniesionego zabezpieczenia podstawowego lub zabezpieczenia rozszerzonego.

TABELA 3-2: KATEGORIA AT - UŚWIADAMIANIE I SZKOLENIA

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
AT-1	**POLITYKA I PROCEDURY**	X	X	X	X
AT-2	**SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA**	X	X	X	X
AT-2(1)	ĆWICZENIA PRAKTYCZNE				
AT-2(2)	ZAGROŻENIE WEWNĘTRZNE		X	X	X
AT-2(3)	INŻYNIERIA SPOŁECZNA I POZYSKIWANIE DANYCH			X	X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
AT-2(4)	PODEJRZANA TRANSMISJA I ANOMALIE ZACHOWANIA SYSTEMU				
AT-2(5)	ZAAWANSOWANE TRWAŁE ZAGROŻENIA (TYPU APT)				
AT-2(6)	ŚRODOWISKA CYBERZAGROŻEŃ				
AT-3	**SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH**	X	X	X	X
AT-3(1)	ZABEZPIECZENIA ŚRODOWISKOWE				
AT-3(2)	ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO				
AT-3(3)	ĆWICZENIA PRAKTYCZNE				
AT-3(4)	*PODEJRZANE TRANSMISJE I ANOMALIE ZACHOWANIA SYSTEMU*	*W: włączone do AT-2(4).*			
AT-3(5)	PRZETWARZANIE DANYCH OSOBOWYCH	X			
AT-4	**DOKUMENTACJA SZKOLENIOWA**	X	X	X	X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
AT-5	*UTRZYMYWANIE KONTAKTÓW Z ZESPOŁAMI I STOWARZYSZENIAMI SPECJALIZUJĄCYMI SIĘ W CYBERBEZPIECZEŃSTWIE*	*W: włączone do PM-15.*			
AT-6	**INFORMACJE ZWROTNE O SZKOLENIACH**				

3.3. KATEGORIA AU – AUDYT I ROZLICZALNOŚĆ

Tabela 3- zawiera podsumowanie zabezpieczeń podstawowych i zabezpieczeń rozszerzonych przypisanych do *Kategorii AU - Audyt i rozliczalność*. Zabezpieczenia są przypisane do bazowych zabezpieczeń prywatności oraz do bazowych środków bezpieczeństwa o niskim, umiarkowanym i wysokim poziomie wpływu, w zależności od potrzeb. Zabezpieczenie podstawowe lub zabezpieczenie rozszerzone, które zostało wycofane z katalogu zabezpieczeń lub przeniesione do innej kategorii zabezpieczeń, jest oznaczone symbolem "W" z objaśnieniem dokonanym czcionką kursywa w jasnoszarym kolorze, z podaniem miejsca umieszczenia wycofanego / przeniesionego zabezpieczenia podstawowego lub zabezpieczenia rozszerzonego.

TABELA 3-3: KATEGORIA AU - AUDYT I ROZLICZALNOŚĆ

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
AU-1	**POLITYKA I PROCEDURY**	X	X	X	X
AU-2	**AUDYT ZDARZEŃ**	X	X	X	X
AU-2(1)	*KOMPILACJA ZAPISÓW AUDYTU Z WIELU ŹRÓDEŁ*	*W: włączone do AU-12.*			
AU-2(2)	*WYBÓR ZDARZEŃ AUDYTOWYCH WEDŁUG KOMPONENTÓW*	*W: włączone do AU-12.*			
AU-2(3)	*OPINIE I AKTUALIZACJE*	*W: włączone do AU-2.*			

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
AU-2(4)	*UPRZYWILEJOWANE FUNKCJE*	*W: włączone do AC-6(9).*			
AU-3	**ZAWARTOŚĆ REJESTRÓW AUDYTU**		X	X	X
AU-3(1)	DODATKOWE INFORMACJE KONTROLNE			X	X
AU-3(2)	*CENTRALNE ZARZĄDZANIE TREŚCIĄ PLANOWANEGO REJESTRU AUDYTU*	*W: włączone do PL-9.*			
AU-3(3)	OGRANICZENIE INFORMACJI UMOŻLIWIAJĄCYCH IDENTYFIKACJĘ OSÓB	X			
AU-4	**POJEMNOŚĆ PAMIĘCI ZAPISÓW AUDYTU**		X	X	X
AU-4(1)	TRANSFER REKORDÓW DO ALTERNATYWNYCH URZĄDZEŃ MAGAZYNUJĄCYCH				
AU-5	**REAKCJA NA BŁĘDY PROCESÓW AUDYTU**		X	X	X
AU-5(1)	OSTRZEŻENIA DOTYCZĄCE LIMITU PAMIĘCI PRZECHOWYWANIA REKORDÓW AUDYTU				X
AU-5(2)	ALERTY CZASU RZECZYWISTEGO				X
AU-5(3)	KONFIGUROWALNE PROGI NATĘŻENIA RUCHU				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
AU-5(4)	WYŁĄCZENIE W PRZYPADKU AWARII				
AU-5(5)	ZDOLNOŚĆ ALTERNATYWNEGO PROWADZENIA REJESTRU AUDYTÓW				
AU-6	**PRZEGLĄD ZAPISÓW AUDYTU, ANALIZA I RAPORTOWANIE**		X	X	X
AU-6(1)	ZAUTOMATYZOWANA INTEGRACJA PROCESÓW			X	X
AU-6(2)	*AUTOMATYCZNE ALARMY BEZPIECZEŃSTWA*	*W: włączone do SI-4.*			
AU-6(3)	KORELACJA ZBIORÓW AUDYTU			X	X
AU-6(4)	CENTRALNE PRZEGLĄDANIE I ANALIZY				
AU-6(5)	ZINTEGROWANA ANALIZA ZAPISÓW Z AUDYTU				X
AU-6(6)	KORELACJA AUDYTU Z MONITOROWANIEM FIZYCZNYM				X
AU-6(7)	DOPUSZCZALNE DZIAŁANIA				
AU-6(8)	PEŁNA ANALIZA TEKSTU UPRZYWILEJOWANYCH POLECEŃ				
AU-6(9)	KORELACJA Z INFORMACJAMI UZYSKANYMI ZE ŹRÓDEŁ NIETECHNICZNYCH				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
AU-6(10)	*KORYGOWANIE POZIOMU AUDYTU*	*W: włączone do AU-6.*			
AU-7	**REDUKCJA TREŚCI ZAPISÓW Z AUDYTU I GENEROWANIE RAPORTÓW**			X	X
AU-7(1)	AUTOMATYZACJA PROCESU			X	X
AU-7(2)	*AUTOMATYCZNE SORTOWANIE I WYSZUKIWANIE*	*W: włączone do AU-7(1)*			
AU-8	**ZNACZNIKI CZASU**		X	X	X
AU-8(1)	*SYNCHRONIZACJA Z AUTORYZOWANYM ŹRÓDŁEM CZASU ODNIESIENIA*	*W: włączone do SC-45(1).*			
AU-8(2)	*WTÓRNE ŹRÓDŁO CZASU ODNIESIENIA*	*W: włączone do SC-45(2).*			
AU-9	**OCHRONA INFORMACJI AUDYTOWYCH**		X	X	X
AU-9(1)	NOŚNIKI JEDNOKROTNEGO ZAPISU				
AU-9(2)	BACKUP AUDYTU W ODSEPAROWANYM FIZYCZNIE SYSTEMIE / KOMPONENCIE				X
AU-9(3)	OCHRONA KRYPTOGRAFICZNA				X
AU-9(4)	DOSTĘP DO PODZBIORU UPRZYWILEJOWANYCH			X	X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
	UŻYTKOWNIKÓW				
AU-9(5)	PODWÓJNA AUTORYZACJA				
AU-9(6)	DOSTĘP TYLKO DO ODCZYTU				
AU-9(7)	PRZECHOWYWANIE INFORMACJI NA KOMPONENTACH Z RÓŻNYMI SYSTEMAMI OPERACYJNYMI				
AU-10	**NIEZAPRZECZALNOŚĆ**				X
AU-10(1)	POŁĄCZENIE TOŻSAMOŚCI				
AU-10(2)	POWIĄZANIE INFORMACJI Z TOŻSAMOŚCIĄ TWÓRCY				
AU-10(3)	ŁAŃCUCH NADZORU				
AU-10(4)	POTWIERDZANIE TOŻSAMOŚCI PRZEGLĄDAJĄCEGO INFORMACJE				
AU-10(5)	*PODPISY CYFROWE*	*W: włączone do SI-7.*			
AU-11	**RETENCJA ZAPISÓW AUDYTU**	X	X	X	X
AU-11(1)	DŁUGOTERMINOWA ZDOLNOŚĆ DO ODZYSKU				
AU-12	**TWORZENIE ZAPISÓW AUDYTU**		X	X	X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
AU-12(1)	OGÓLNOSYSTEMOWE / SKORELOWANE W CZASIE ŚCIEŻKI AUDYTU				X
AU-12(2)	UJEDNOLICONE FORMATY				
AU-12(3)	ZMIANY DOKONYWANE PRZEZ UPRAWNIONE OSOBY				X
AU-12(4)	AUDYT PARAMETRÓW ZAPYTAŃ O DANE OSOBOWE				
AU-13	**MONITOROWANIE UJAWNIANIA INFORMACJI**				
AU-13(1)	WYKORZYSTANIE ZAUTOMATYZOWANYCH NARZĘDZI				
AU-13(2)	PRZEGLĄD MONITOROWANYCH STRON				
AU-13(3)	NIEAUTORYZOWANE POWIELANIE INFORMACJI				
AU-14	**AUDYT SESJI**				
AU-14(1)	URUCHAMIANIE SYSTEMU				
AU-14(2)	*PRZECHWYTY / NAGRYWANIE I ZAWARTOŚĆ DZIENNIKÓW LOGOWANIA*	*W: włączone do AU-14.*			
AU-14(3)	ZDALNE WYŚWIETLANIE I ODSŁUCHIWANIE				
AU-15	*ZDOLNOŚĆ DO ALTERNATYWNEGO AUDYTU*	*W: włączone do AU-5(5).*			

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
AU-16	**AUDYT MIĘDZYORGANIZACYJNY**				
AU-16(1)	OCHRONA TOŻSAMOŚCI				
AU-16(2)	UDOSTĘPNIANIE INFORMACJI AUDYTOWYCH				
AU-16(3)	ODDZIELANIE DANYCH OSOBOWYCH				

3.4. KATEGORIA CA - OCENA, AUTORYZACJA I MONITOROWANIE

Tabela 3-4 zawiera podsumowanie zabezpieczeń podstawowych i zabezpieczeń rozszerzonych przypisanych do *Kategorii CA - Ocena, Autoryzacja i Monitorowanie*. Zabezpieczenia są przypisane do bazowych zabezpieczeń prywatności oraz do bazowych środków bezpieczeństwa o niskim, umiarkowanym i wysokim poziomie wpływu, w zależności od potrzeb. Zabezpieczenie podstawowe lub zabezpieczenie rozszerzone, które zostało wycofane z katalogu zabezpieczeń lub przeniesione do innej kategorii zabezpieczeń, jest oznaczone symbolem "W" z objaśnieniem dokonanym czcionką kursywa w jasnoszarym kolorze, z podaniem miejsca umieszczenia wycofanego / przeniesionego zabezpieczenia podstawowego lub zabezpieczenia rozszerzonego.

TABELA 3-4: KATEGORIA CA - OCENA, AUTORYZACJA I MONITOROWANIE

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
CA-1	**POLITYKA I PROCEDURY**	X	X	X	X
CA-2	**OCENA ZABEZPIECZEŃ**	X	X	X	X
CA-2(1)	NIEZALEŻNI AUDYTORZY			X	X
CA-2(2)	OCENY SPECJALISTYCZNE				X
CA-2(3)	KORZYSTANIE Z WYNIKÓW UZYSKANYCH OD ORGANIZACJI ZEWNĘTRZNYCH				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
CA-3	**WYMIANA INFORMACJI**		X	X	X
CA-3(1)	*POŁĄCZENIA JAWNYCH BEZPIECZNYCH SYSTEMÓW KRAJOWYCH*	*W: włączone do SC-7(25).*			
CA-3(2)	*POŁĄCZENIA NIEJAWNYCH SYSTEMÓW KRAJOWYCH*	*W: włączone do SC-7(26).*			
CA-3(3)	*POŁĄCZENIA JAWNYCH BEZPIECZNYCH SYSTEMÓW TRANSGRANICZNYCH*	*W: włączone do SC-7(27).*			
CA-3(4)	*POŁĄCZENIA Z SIECIAMI PUBLICZNYMI*	*W: włączone do SC-7(28).*			
CA-3(5)	*OGRANICZENIA DOTYCZĄCE POŁĄCZEŃ SYSTEMÓW ZEWNĘTRZNYCH*	*W: włączone do SC-7(5).*			
CA-3(6)	AUTORYZACJA PRZESYŁU				X
CA-3(7)	POBIERANIE INFORMACJI				
CA-4	*CERTYFIKACJA BEZPIECZEŃSTWA*	*W: włączone do CA-2.*			
CA-5	**PLAN I ETAPY DZIAŁANIA**	X	X	X	X
CA-5(1)	AUTOMATYZACJA WSPIERAJĄCA AKTUALNOŚĆ / SZCZEGÓŁOWOŚĆ PLANÓW				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
CA-6	**AUTORYZACJA**	X	X	X	X
CA-6(1)	AUTORYZACJA WSPÓLNA - WEWNĄTRZORGANIZACYJNA				
CA-6(2)	AUTORYZACJA WSPÓLNA - MIĘDZYORGANIZACYJNA				
CA-7	**CIĄGŁE MONITOROWANIE**	X	X	X	X
CA-7(1)	NIEZALEŻNA OCENA			X	X
CA-7(2)	*RODZAJE OCEN*	*W: włączone do CA-2.*			
CA-7(3)	ANALIZY TRENDÓW				
CA-7(4)	MONITOROWANIE RYZYKA	X	X	X	X
CA-7(5)	ANALIZA SPÓJNOŚCI				
CA-7(6)	AUTOMATYZACJA WSPARCIA MONITOROWANIA				
CA-8	**BADANIE PENETRACYJNE**				X
CA-8(1)	NIEZALEŻNY TESTER LUB ZESPÓŁ PENETRACYJNY				X
CA-8(2)	ĆWICZENIA ZESPOŁU ATAKUJĄCEGO TYPU „RED TEAM”				
CA-8(3)	LOKALNE TESTY PENETRACYJNE				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
CA-9	**POŁĄCZENIA WEWNĘTRZSYSTEMOWE**		X	X	X
CA-9(1)	KONTROLE ZGODNOŚCI				

3.5. KATEGORIA CM - ZARZĄDZANIE KONFIGURACJĄ

Tabela 3-5 zawiera podsumowanie zabezpieczeń podstawowych i zabezpieczeń rozszerzonych przypisanych do *Kategorii CM – Zarządzanie konfiguracją*. Zabezpieczenia są przypisane do bazowych zabezpieczeń prywatności oraz do bazowych środków bezpieczeństwa o niskim, umiarkowanym i wysokim poziomie wpływu, w zależności od potrzeb. Zabezpieczenie podstawowe lub zabezpieczenie rozszerzone, które zostało wycofane z katalogu zabezpieczeń lub przeniesione do innej kategorii zabezpieczeń, jest oznaczone symbolem "W" z objaśnieniem dokonanym czcionką kursywa w jasnoszarym kolorze, z podaniem miejsca umieszczenia wycofanego / przeniesionego zabezpieczenia podstawowego lub zabezpieczenia rozszerzonego.

TABELA 3-5: KATEGORIA CM - ZARZĄDZANIE KONFIGURACJĄ

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
CM-1	**POLITYKA I PROCEDURY**	X	X	X	X
CM-2	**KONFIGURACJA BAZOWA**		X	X	X
CM-2(1)	*PRZEGLĄDY I AKTUALIZACJE*	*W: włączone do CM-2.*			
CM-2(2)	AUTOMATYZACJA WSPIERAJĄCA AKTUALNOŚĆ / SZCZEGÓŁOWOŚĆ			X	X
CM-2(3)	RETENCJA ZACHOWANYCH KONFIGURACJI			X	X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
CM-2(4)	*NIEAUTORYZOWANE OPROGRAMOWANIE*	*W: włączone do CM-7.*			
CM-2(5)	*AUTORYZOWANE OPROGRAMOWANIE*	*W: włączone do CM-7.*			
CM-2(6)	ŚRODOWISKA PROGRAMISTYCZNE I TESTOWE				
CM-2(7)	KONFIGUROWANIE SYSTEMÓW I KOMPONENTÓW W OBSZARACH WYSOKIEGO RYZYKA			X	X
CM-3	**ZABEZPIECZANIE ZMIAN KONFIGURACJI**			X	X
CM-3(1)	AUTOMATYCZNA DOKUMENTACJA / POWIADAMIANIE / ZAKAZ WPROWADZANIA ZMIAN				X
CM-3(2)	TESTY, WALIDACJA I ZMIANY DOKUMENTÓW			X	X
CM-3(3)	AUTOMATYCZNE WPROWADZANIE ZMIAN				
CM-3(4)	FUNKCYJNI DS. BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI			X	X
CM-3(5)	AUTOMATYCZNA REAKCJA BEZPIECZEŃSTWA				
CM-3(6)	ZARZĄDZANIE KRYPTOGRAFICZNE				X
CM-3(7)	PRZEGLĄD ZMIAN W SYSTEMIE				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
CM-3(8)	ZAPOBIEGANIE LUB OGRANICZANIE ZMIAN KONFIGURACJI				
CM-4	**ANALIZY WPŁYWU**	X	X	X	X
CM-4(1)	ODDZIELNE ŚRODOWISKA BADAWCZE				X
CM-4(2)	WERYFIKACJA ZABEZPIECZEŃ			X	X
CM-5	**OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN**		X	X	X
CM-5(1)	AUTOMATYCZNE EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU I ZAPISY Z AUDYTU				X
CM-5(2)	*PRZEGLĄD ZMIAN W SYSTEMIE*	*W: włączone do CM-3(7).*			
CM-5(3)	*PODPISANE KOMPONENTY*	*W: włączone do CM-14.*			
CM-5(4)	PODWÓJNA AUTORYZACJA				
CM-5(5)	OGRANICZANIE PRZYWILEJÓW W ZAKRESIE WYTWARZANIA I EKSPLOATACJI				
CM-5(6)	OGRANICZANIE PRZYWILEJÓW W BIBLIOTEKACH OPROGRAMOWANIA				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
CM-5(7)	AUTOMATYCZNE WDRAŻANIE ŚRODKÓW BEZPIECZEŃSTWA	*W: włączone do SI-7.*			
CM-6	**USTAWIENIA KONFIGURACYJNE**		X	X	X
CM-6(1)	AUTOMATYCZNE ZARZĄDZANIE, STOSOWANIE I WERYFIKACJA				X
CM-6(2)	ODPOWIEDŹ NA NIEAUTORYZOWANE ZMIANY				X
CM-6(3)	*WYKRYWANIE NIEAUTORYZOWANYCH ZMIAN*	*W: włączone do SI-7.*			
CM-6(4)	*PREZENTACJA ZGODNOŚCI*	*W: włączone do CM-4.*			
CM-7	**ZASADA MINIMALNEJ FUNKCJONALNOŚCI**		X	X	X
CM-7(1)	PRZEGLĄDY OKRESOWE			X	X
CM-7(2)	ZAPOBIEGANIE WYKONYWANIU PROGRAMU			X	X
CM-7(3)	STOSOWANIE REJESTRACJI				
CM-7(4)	NIEAUTORYZOWANE OPROGRAMOWANIE („CZARNA LISTA”)				
CM-7(5)	AUTORYZOWANE OPROGRAMOWANIE („BIAŁA LISTA”)			X	X
CM-7(6)	ZAMKNIĘTE ŚRODOWISKA Z OGRANICZONYMI				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
	UPRAWNIENIAMI				
CM-7(7)	WYKONYWANIE KODU W CHRONIONYCH ŚRODOWISKACH				
CM-7(8)	KOD BINARNY LUB KOD WYKONYWALNY (MOBILNY)				
CM-7(9)	ZAKAZ UŻYWANIA NIEAUTORYZOWANEGO SPRZĘTU				
CM-8	**INWENTARYZACJA KOMPONENTÓW SYSTEMU**		X	X	X
CM-8(1)	AKTUALIZACJE INSTALACJI I USUWANIA KOMPONENTÓW			X	X
CM-8(2)	AUTOMATYCZNA KONSERWACJA (UTRZYMYWANIE)				X
CM-8(3)	AUTOMATYCZNE WYKRYWANIE KOMPONENTÓW NIEAUTORYZOWANYCH			X	X
CM-8(4)	INFORMACJA DOTYCZĄCE ODPOWIEDZIALNOŚCI I ROZLICZALNOŚCI				X
CM-8(5)	*BRAK DUPLIKACJI KOMPONENTÓW*	*W: włączone do CM-8.*			
CM-8(6)	OCENA KONFIGURACJI I ZATWIERDZONE ODSTĘPSTWA				
CM-8(7)	SCENTRALIZOWANE REPOZYTORIUM				
CM-8(8)	AUTOMATYCZNE ŚLEDZENIE LOKALIZACJI				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
CM-8(9)	PRZYPISANIE KOMPONENTÓW DO SYSTEMÓW				
CM-9	**PLAN ZARZĄDZANIA KONFIGURACJĄ**			X	X
CM-9(1)	PRZYPISANIE ODPOWIEDZIALNOŚCI				
CM-10	**OGRANICZENIA W UŻYCIU OPROGRAMOWANIA**		X	X	X
CM-10(1)	OPROGRAMOWANIE OTWARTE (OPEN-SOURCE)				
CM-11	**OPROGRAMOWANIE ZAINSTALOWANE PRZEZ UŻYTKOWNIKA**		X	X	X
CM-11(1)	*OSTRZEGANIE O NIEAUTORYZOWANYCH INSTALACJACH*	*W: włączone do CM8(3)*			
CM-11(2)	ZABRONIONA INSTALACJA BEZ POSIADANIA STOSOWNYCH UPRAWNIEŃ				
CM-11(3)	AUTOMATYCZNE EGZEKWOWANIE I MONITOROWANIE				
CM-12	**POŁOŻENIE (LOKACJA) INFORMACJI**			X	X
CM-12(1)	AUTOMATYCZNE NARZĘDZIA DO OBSŁUGI LOKACJI INFORMACJI			X	X
CM-13	**MAPOWANIE DZIAŁAŃ NA DANYCH**				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
CM-14	**PODPISYWANIE KOMPONENTÓW**				

3.6. KATEGORIA CP - PLANOWANIE AWARYJNE / CIĄGŁOŚĆ DZIAŁANIA

Tabela 3-6 zawiera podsumowanie zabezpieczeń podstawowych i zabezpieczeń rozszerzonych przypisanych do *Kategorii CP - Planowanie awaryjne / Ciągłość działania*. Zabezpieczenia są przypisane do bazowych zabezpieczeń prywatności oraz do bazowych środków bezpieczeństwa o niskim, umiarkowanym i wysokim poziomie wpływu, w zależności od potrzeb. Zabezpieczenie podstawowe lub zabezpieczenie rozszerzone, które zostało wycofane z katalogu zabezpieczeń lub przeniesione do innej kategorii zabezpieczeń, jest oznaczone symbolem "W" z objaśnieniem dokonanym czcionką kursywa w jasnoszarym kolorze, z podaniem miejsca umieszczenia wycofanego / przeniesionego zabezpieczenia podstawowego lub zabezpieczenia rozszerzonego.

TABELA 3-6: KATEGORIA CP - PLANOWANIE AWARYJNE / CIĄGŁOŚĆ DZIAŁANIA

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
CP-1	**POLITYKA I PROCEDURY**		X	X	X
CP-2	**PLAN CIĄGŁOŚCI DZIAŁANIA**		X	X	X
CP-2(1)	KOORDYNACJA Z POWIĄZANYMI PLANAMI			X	X
CP-2(2)	PLANOWANIE ZDOLNOŚCI FUNKCJONOWANIA				X
CP-2(3)	WZNAWIANIE PODSTAWOWYCH DZIAŁAŃ I FUNKCJI BIZNESOWYCH			X	X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
CP-2(4)	*PRZYWRÓCENIE DZIAŁANIA WSZYSTKICH FUNKCJI BIZNESOWYCH*	*W: włączone do CP-2(3).*			
CP-2(5)	KONTYNUACJA NIEZBĘDNYCH DZIAŁAŃ / FUNKCJI BIZNESOWYCH				X
CP-2(6)	PROCESY ALTERNATYWNE / ZAPASOWE MIEJSCA PRZETWARZANIA				
CP-2(7)	KOORDYNACJA Z USŁUGODAWCAMI ZEWNĘTRZNYMI				
CP-2(8)	IDENTYFIKACJA ZASOBÓW KRYTYCZNYCH			X	X
CP-3	**SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA**		X	X	X
CP-3(1)	WYDARZENIA SYMULOWANE				X
CP-3(2)	ZAUTOMATYZOWANE ŚRODOWISKA SZKOLENIOWE				
CP-4	**TESTOWANIE PLANU AWARYJNEGO**		X	X	X
CP-4(1)	KOORDYNACJA Z POWIĄZANYMI PLANAMI			X	X
CP-4(2)	ZAPASOWE MIEJSCE PRZETWARZANIA				X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
CP-4(3)	AUTOMATYCZNE TESTOWANIE				
CP-4(4)	PEŁNE ODZYSKIWANIE I ODTWARZANIE				
CP-4(5)	PRÓBNE AWARIE				
CP-5	*AKTUALIZACJA PLANU CIĄGŁOŚCI DZIAŁANIA*	*W: włączone do CP-2.*			
CP-6	**ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII**			X	X
CP-6(1)	SEPARACJA OD MIEJSCA GŁÓWNEGO			X	X
CP-6(2)	CZAS ODZYSKIWANIA I PUNKT ODTWORZENIA DANYCH				X
CP-6(3)	DOSTĘPNOŚĆ			X	X
CP-7	**ZAPASOWE MIEJSCE PRZETWARZANIA**			X	X
CP-7(1)	ODSEPAROWANIE OD LOKALIZACJI PODSTAWOWEJ			X	X
CP-7(2)	DOSTĘPNOŚĆ			X	X
CP-7(3)	PRIORYTET USŁUG			X	X
CP-7(4)	GOTOWOŚĆ DO UŻYCIA				X
CP-7(5)	*ZASTĘPCZE ŚRODKI BEZPIECZEŃSTWA*	*W: włączone do CP-7.*			

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
CP-7(6)	BRAK MOŻLIWOŚCI POWROTU DO LOKALIZACJI PODSTAWOWEJ				
CP-8	**USŁUGI TELEKOMUNIKACYJNE**			X	X
CP-8(1)	PRIORYTETY ŚWIADCZENIA USŁUG			X	X
CP-8(2)	POJEDYNCZE PUNKTY AWARII			X	X
CP-8(3)	ROZDZIELENIE DOSTAWCÓW PODSTAWOWYCH I ALTERNATYWNYCH				X
CP-8(4)	PLAN AWARYJNY DOSTAWCY				X
CP-8(5)	ALTERNATYWNE TESTOWANIE USŁUG TELEKOMUNIKACYJNYCH				
CP-9	**KOPIA ZAPASOWA**		X	X	X
CP-9(1)	BADANIE NIEZAWODNOŚCI NOŚNIKÓW / INTEGRALNOŚCI INFORMACJI			X	X
CP-9(2)	TESTY ODTWORZENIOWE Z WYKORZYSTANIEM PRÓBEK DANYCH				X
CP-9(3)	SEPARACJA PRZECHOWYWANIA INFORMACJI KRYTYCZNYCH				X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
CP-9(4)	*OCHRONA PRZED NIEAUTORYZOWANĄ MODYFIKACJĄ*	*W: włączone do CP-9.*			
CP-9(5)	PRZEKAZANIE KOPII DO ALTERNATYWNEJ LOKALIZACJI				X
CP-9(6)	REDUNDANCJA (NADMIAROWOŚĆ) SYSTEMU				
CP-9(7)	PODWÓJNA AUTORYZACJA				
CP-9(8)	OCHRONA KRYPTOGRAFICZNA			X	X
CP-10	**ODZYSKIWANIE I ODTWARZANIE SYSTEMU**		X	X	X
CP-10(1)	*TESTOWANIE PLANU AWARYJNEGO*	*W: włączone do CP-4.*			
CP-10(2)	ODTWARZANIE TRANSAKCJI			X	X
CP-10(3)	*KOMPENSACYJNE ŚRODKI BEZPIECZEŃSTWA*	*W: omawiane w procesie dostosowywania zabezpieczeń*			
CP-10(4)	PRZYWRACANIE W OKREŚLONYM PRZEDZIALE CZASOWYM				X
CP-10(5)	*PRACE AWARYJNE*	*W: włączone do SI-13.*			
CP-10(6)	OCHRONA KOMPONENETÓW				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
CP-11	**ALTERNATYWNE PROTOKOŁY KOMUNIKACJI**				
CP-12	**TRYB BEZPIECZNY**				
CP-13	**ALTERNATYWNE MECHANIZMY BEZPIECZEŃSTWA**				

3.7. KATEGORIA IA - IDENTYFIKACJI I UWIERZYTELNIANIE

Tabela 3-7 zawiera podsumowanie zabezpieczeń podstawowych i zabezpieczeń rozszerzonych przypisanych do *Kategorii IA - Identyfikacja i uwierzytelnianie*. Zabezpieczenia są przypisane do bazowych zabezpieczeń prywatności oraz do bazowych środków bezpieczeństwa o niskim, umiarkowanym i wysokim poziomie wpływu, w zależności od potrzeb. Zabezpieczenie podstawowe lub zabezpieczenie rozszerzone, które zostało wycofane z katalogu zabezpieczeń lub przeniesione do innej kategorii zabezpieczeń, jest oznaczone symbolem "W" z objaśnieniem dokonanym czcionką kursywa w jasnoszarym kolorze, z podaniem miejsca umieszczenia wycofanego / przeniesionego zabezpieczenia podstawowego lub zabezpieczenia rozszerzonego.

TABELA 3-7: KATEGORIA IA - IDENTYFIKACJA I UWIERZYTELNIANIE

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
IA-1	**POLITYKA I PROCEDURY**		X	X	X
IA-2	**IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI)**		X	X	X
IA-2(1)	UWIERZYTELNIANIE WIELOSKŁADNIKOWE DOSTĘPU DO KONT UPRZYWILEJOWANYCH		X	X	X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
IA-2(2)	UWIERZYTELNIANIE WIELOSKŁADNIKOWE DOSTĘPU DO KONT NIEUPRZYWILEJOWANYCH		X	X	X
IA-2(3)	*DOSTĘP LOKALNY DO KONT UPRZYWILEJOWANYCH*	*W: włączone do IA-2(1)(2).*			
IA-2(4)	*DOSTĘP LOKALNY DO KONT NIEUPRZYWILEJOWANYCH*	*W: włączone do IA-2(1)(2).*			
IA-2(5)	UWIERZYTELNIANIE INDYWIDUALNE PRZED UWIERZYTELNIANIEM GRUPOWYM				X
IA-2(6)	DOSTĘP DO KONT – ODSEPAROWANE URZĄDZENIE				
IA-2(7)	*DOSTĘP SIECIOWY DO KONT NIEUPRZYWILEJOWANYCH – ODSEPAROWANE URZĄDZENIE*	*W: włączone do IA-2(6).*			
IA-2(8)	DOSTĘP DO KONT – ODPORNOŚĆ NA POWTARZANIE		X	X	X
IA-2(9)	DOSTĘP SIECIOWY DO KONT NIEUPRZYWILEJOWANYCH – ODPORNOŚĆ NA POWTARZANIE	*W: włączone do IA-2(8).*			
IA-2(10)	LOGOWANIE POJEDYNCZE (SINGLE SIGN-ON)				
IA-2(11)	*ZDALNY DOSTĘP - ODSEPAROWANE URZĄDZENIE*	*W: włączone do IA-2(6).*			
IA-2(12)	AUTORYZACJA DANYCH DOSTĘPOWYCH		X	X	X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
IA-2(13)	UWIERZYTELNIANIE "POZA PASMEM" (Z WYKORZYSTANIEM DWÓCH ODDZIELNYCH ŚCIEŻEK)				
IA-3	**IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA**			X	X
IA-3(1)	DWUKIERUNKOWE UWIERZYTELNIANIE KRYPTOGRAFICZNE				
IA-3(2)	*DWUKIERUNKOWE SIECIOWE UWIERZYTELNIANIE KRYPTOGRAFICZNE*	*W: włączone do IA-3(1).*			
IA-3(3)	ALOKACJA ADRESU DYNAMICZNEGO				
IA-3(4)	ATESTACJA URZĄDZENIA				
IA-4	**ZARZĄDZANIE IDENTYFIKATOREM**		X	X	X
IA-4(1)	ZAKAZ UŻYWANIA IDENTYFIKATORÓW KONT JAKO IDENTYFIKATORÓW PUBLICZNYCH				
IA-4(2)	*AUTORYZACJA PRZEŁOŻONEGO*	*W: włączone do IA-12(1).*			
IA-4(3)	*WIELE FORM CERTYFIKACJI*	*W: włączone do IA-12(2)*			
IA-4(4)	IDENTYFIKACJA STATUSU UŻYTKOWNIKA			X	X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
IA-4(5)	ZARZĄDZANIE DYNAMICZNE				
IA-4(6)	ZARZĄDZANIE MIĘDZYORGANIZACYJNE				
IA-4(7)	*REJESTRACJA OSOBISTA*	*W: włączone do IA-12(4)*			
IA-4(8)	PAROWANIE IDENTYFIKATORÓW PODCZAS PSEUDONIMIZACJI				
IA-4(9)	UTRZYMANIE I OCHRONA ATRYBUTÓW				
IA-5	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA**		X	X	X
IA-5(1)	UWIERZYTELNIANIE OPARTE O HASŁA		X	X	X
IA-5(2)	UWIERZYTELNIANIE OPARTE O INFRASTRUKTURĘ KLUCZA PUBLICZNEGO			X	X
IA-5(3)	*REJESTRACJA OSOBISTA LUB PRZEZ ZAUFANĄ TRZECIĄ STRONĘ*	*W: włączone do IA-12(4).*			
IA-5(4)	*AUTOMATYCZNE WSPARCIE OKREŚLANIA SIŁY HASŁA*	*W: włączone do IA-5(1).*			
IA-5(5)	ZMIANA METODY UWIERZYTELNIANIA PRZED DOSTAWĄ				
IA-5(6)	OCHRONA METOD UWIERZYTELNIANIA			X	X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
IA-5(7)	BRAK WBUDOWANYCH NIEZASZYFROWANYCH STATYCZNYCH ELEMENTÓW UWIERZYTELNIANIA				
IA-5(8)	JEDNO KONTO W WIELU SYSTEMACH INFORMATYCZNYCH				
IA-5(9)	ZARZĄDZANIE DANYMI UWIERZYTELNIAJĄCYMI MIĘDZY ORGANIZACJAMI				
IA-5(10)	DYNAMICZNE KOJARZENIE DANYCH UWIERZYTELNIAJĄCYCH				
IA-5(11)	*UWIERZYTELNIANIE PRZY UŻYCIU TOKENA*	*W: włączone do IA-2(1) i IA-2(2).*			
IA-5(12)	WYDAJNOŚĆ UWIERZYTELNIANIA BIOMETRYCZNEGO				
IA-5(13)	PRZEDAWNIENIE BUFOROWANYCH ELEMENTÓW UWIERZYTELNIANIA				
IA-5(14)	ZARZĄDZANIE ZAWARTOŚCIĄ ZAUFANYCH MAGAZYNÓW INFRASTRUKTURY KLUCZA PUBLICZNEGO				
IA-5(15)	ZATWIERDZANIE PRODUKÓW I USŁUG WEDŁUG Z GÓRY USTALONYCH REGUŁ				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
IA-5(16)	WYDAWANIE POŚWIADCZEŃ UWIERZYTELNIAJĄCYCH OSOBIŚCIE LUB PRZEZ ZAUFANĄ TRZECIĄ STRONĘ				
IA-5(17)	WYKRYWANIE ATAKÓW PREZENTACYJNYCH PODCZAS UWIERZYTELNIANIA BIOMETRYCZNEGO				
IA-5(18)	MENEDŻER HASEŁ				
IA-6	**OCHRONA PROCESU UWIERZYTELNIANIA**		X	X	X
IA-7	**MODUŁ KRYPTOGRAFICZNY UWIERZYTELNIANIE**		X	X	X
IA-8	**IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI)**		X	X	X
IA-8(1)	AKCEPTACJA POŚWIADCZEŃ TOŻSAMOŚCI WYDANYCH PRZEZ INNE ORGANIZACJE		X	X	X
IA-8(2)	AKCEPTACJA POŚWIADCZEŃ STRON TRZECICH		X	X	X
IA-8(3)	*WYKORZYSTANIE CERTYFIKOWANYCH PRODUKTÓW*	*W: włączone do IA-8(2).*			
IA-8(4)	WYKORZYSTANIE PROFILI WYDAWANYCH PRZEZ STOSOWNE INSTYTUCJE		X	X	X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
IA-8(5)	AKCEPTACJA POŚWIADCZEŃ OSOBISTEJ WERYFIKACJI TOŻSAMOŚCI				
IA-8(6)	NIEPOŁĄCZALNOŚĆ (DEZASOCJACYJNOŚĆ)				
IA-9	**IDENTYFIKACJA I UWIERZYTELNIANIE USŁUG**				
IA-9(1)	*WYMIANA INFORMACJI*	*W: włączone do IA-9.*			
IA-9(2)	*PRZEKAZYWANIE DECYZJI O POZYTYWNEJ IDENTYFIKACJI I UWIERZYTELNIENIU*	*W: włączone do IA-9.*			
IA-10	**UWIERZYTELNIANIE ADAPTACYJNE**				
IA-11	**PONOWNE UWIERZYTELNIENIE**		X	X	X
IA-12	**POTWIERDZENIE TOŻSAMOŚCI**			X	X
IA-12(1)	AUTORYZACJA PRZEŁOŻONEGO				
IA-12(2)	DOWODZENIE TOŻSAMOŚCI			X	X
IA-12(3)	POTWIERDZANIE I WERYFIKACJA DOWODÓW TOŻSAMOŚCI			X	X
IA-12(4)	OSOBISTE ZATWIERDZENIE I WERYFIKACJA				X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
IA-12(5)	POTWIERDZENIE ADRESU			X	X
IA-12(6)	AKCEPTACJA ZEWNĘTRZNYCH TOŻSAMOŚCI				

3.8. KATEGORIA IR - REAGOWANIE NA INCYDENTY

Tabela 3-8 zawiera podsumowanie zabezpieczeń podstawowych i zabezpieczeń rozszerzonych przypisanych do *Kategorii IR – Reagowanie na incydenty*. Zabezpieczenia są przypisane do bazowych zabezpieczeń prywatności oraz do bazowych środków bezpieczeństwa o niskim, umiarkowanym i wysokim poziomie wpływu, w zależności od potrzeb. Zabezpieczenie podstawowe lub zabezpieczenie rozszerzone, które zostało wycofane z katalogu zabezpieczeń lub przeniesione do innej kategorii zabezpieczeń, jest oznaczone symbolem "W" z objaśnieniem dokonanym czcionką kursywa w jasnoszarym kolorze, z podaniem miejsca umieszczenia wycofanego / przeniesionego zabezpieczenia podstawowego lub zabezpieczenia rozszerzonego.

TABELA 3-8: KATEGORIA IR - REAGOWANIE NA INCYDENTY

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
IR-1	**POLITYKA I PROCEDURY**	X	X	X	X
IR-2	**SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY**	X	X	X	X
IR-2(1)	WYDARZENIA SYMULOWANE				X
IR-2(2)	ZAUTOMATYZOWANE ŚRODOWISKA SZKOLENIOWE				X
IR-2(3)	NARUSZENIE	X			

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
IR-3	**TESTOWANIE REAGOWANIA NA INCYDENTY**	X		X	X
IR-3(1)	AUTOMATYCZNE TESTOWANIE				
IR-3(2)	KOORDYNACJA Z POWIĄZANYMI PLANAMI			X	X
IR-3(3)	CIĄGŁE DOSKONALENIE				
IR-4	**OBSŁUGA INCYDENTÓW**	X	X	X	X
IR-4(1)	AUTOMATYCZNE PROCESY OBSŁUGI ZDARZEŃ			X	X
IR-4(2)	DYNAMICZNA REKONFIGURACJA				
IR-4(3)	CIĄGŁOŚĆ OPERACJI				
IR-4(4)	KORELACJA INFORMACJI				X
IR-4(5)	AUTOMATYCZNE WYŁĄCZANIE SYSTEMU				
IR-4(6)	ZAGROŻENIA WEWNĘTRZNE				
IR-4(7)	ZAGROŻENIA WEWNĘTRZNE - KOORDYNACJA WEWNĄTRZ ORGANIZACJI				
IR-4(8)	KOORDYNACJA Z ORGANIZACJAMI ZEWNĘTRZNYMI				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
IR-4(9)	ZDOLNOŚĆ DO REAGOWANIA DYNAMICZNEGO				
IR-4(10)	KOORDYNACJA ŁAŃCUCHA DOSTAW				
IR-4(11)	ZINTEGROWANY ZESPÓŁ REAGOWANIA NA INCYDENTY				X
IR-4(12)	ANALIZA KRYMINALISTYCZNA ZŁOŚLIWEGO KODU				
IR-4(13)	ANALIZA ZACHOWANIA				
IR-4(14)	OPERACYJNE CENTRUM BEZPIECZEŃSTWA (SOC)				
IR-4(15)	RELACJE PUBLICZNE I NAPRAWA REPUTACJI				
IR-5	**MONITOROWANIE INCYDENTÓW**	X	X	X	X
IR-5(1)	AUTOMATYCZNE ŚLEDZENIE, ZBIERANIE DANYCH I ANALIZA				X
IR-6	**ZGŁASZANIE INCYDENTÓW**	X	X	X	X
IR-6(1)	ZGŁASZANIE AUTOMATYCZNE			X	X
IR-6(2)	PODATNOŚĆ NA INCYDENTY				
IR-6(3)	KOORDYNACJA ŁAŃCUCHA DOSTAW			X	X
IR-7	**WSPARCIE REAGOWANIA NA INCYDENTY**	X	X	X	X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
IR-7(1)	AUTOMATYCZNE WSPARCIE DOSTĘPNOŚCI INFORMACJI / OBSŁUGI			X	X
IR-7(2)	KOORDYNACJA Z DOSTAWCAMI ZEWNĘTRZNYMI				
IR-8	**PLAN REAGOWANIA NA INCYDENTY**	X	X	X	X
IR-8(1)	NARUSZENIA	X			
IR-9	**REAKCJA NA WYCIEK / UJAWNIENIE INFORMACJI**				
IR-9(1)	*ODPOWIEDZIALNY PERSONEL*	*W: włączone do IR-9.*			
IR-9(2)	SZKOLENIE				
IR-9(3)	DZIAŁANIA PO UJAWNIENIU				
IR-9(4)	WYSTAWIENIE NA DZIAŁANIA OSÓB NIEAUTORYZOWANYCH				
IR-10	*ZINTEGROWANY ZESPÓŁ DS. ANALIZY BEZPIECZEŃSTWA INFORMACJI*	*W: włączone do IR-4(11).*			

3.9. KATEGORIA MA – UTRZYMANIE I WSPARCIE

Tabela 3-9 zawiera podsumowanie zabezpieczeń podstawowych i zabezpieczeń rozszerzonych przypisanych do *Kategorii MA – Utrzymanie i wsparcie*. Zabezpieczenia są przypisane do bazowych zabezpieczeń prywatności oraz do bazowych środków bezpieczeństwa o niskim, umiarkowanym i wysokim poziomie wpływu, w zależności od potrzeb. Zabezpieczenie podstawowe lub zabezpieczenie rozszerzone, które zostało wycofane z katalogu zabezpieczeń lub przeniesione do innej kategorii zabezpieczeń, jest oznaczone symbolem "W" z objaśnieniem dokonanym czcionką kursywa w jasnoszarym kolorze, z podaniem miejsca umieszczenia wycofanego / przeniesionego zabezpieczenia podstawowego lub zabezpieczenia rozszerzonego.

TABELA 3-9: KATEGORIA MA – UTRZYMANIE I WSPARCIE

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
MA-1	**POLITYKA I PROCEDURY**		X	X	X
MA-2	**NADZÓR NAD UTRZYMANIEM**		X	X	X
MA-2(1)	*ZAWARTOŚĆ REKORDU*	*W: włączone do MA-2.*			
MA-2(2)	AUTOMATYCZNE DZIAŁANIA KONSERWACYJNE				X
MA-3	**NARZĘDZIA UTRZYMANIOWE**			X	X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
MA-3(1)	SPRAWDZANIE NARZĘDZI			X	X
MA-3(2)	SPRAWDZANIE NOŚNIKÓW DANYCH			X	X
MA-3(3)	ZAPOBIEGANIE NIEAUTORYZOWANEMU USUWANIU			X	X
MA-3(4)	OGRANICZANIE UŻYWANIA NARZĘDZI				
MA-3(5)	WYKORZYSTYWANIE PODWYŻSZONYCH UPRAWNIEŃ				
MA-3(6)	AKTUALIZACJE I POPRAWKI OPROGRAMOWANIA				
MA-4	**UTRZYMANIE ZDALNE**		X	X	X
MA-4(1)	AUDYT I PRZEGLĄD				
MA-4(2)	*DOKUMENTY ZDALNEGO UTRZYMANIE*	*W: włączone do MA-1 i MA-4.*			
MA-4(3)	PORÓWNYWALNE POZIOMY BEZPIECZEŃSTWA / SANITYZACJA				X
MA-4(4)	UWIERZYTELNIANIE / SEPARACJA SESJI UTRZYMANIOWYCH				
MA-4(5)	ZGODY I POWIADOMIENIA				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
MA-4(6)	OCHRONA KRYPTOGRAFICZNA				
MA-4(7)	ZDALNA WERYFIKACJA ZAKOŃCZENIA SESJI				
MA-5	**PERSONEL UTZRYMANIOWY**		X	X	X
MA-5(1)	OSOBY NIEPOSIADAJĄCE STOSOWNYCH PRAW DOSTĘPU				X
MA-5(2)	POŚWIADCZENIA BEZPIECZEŃSTWA / SYSTEMY NIEJAWNE				
MA-5(3)	OBYWATELSTWO / SYSTEMY NIEJAWNE				
MA-5(4)	CUDZOZIEMCY				
MA-5(5)	OBSŁUGA NIEZWIĄZANA Z UTRZYMANIEM SYSTEMU				
MA-6	**TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI**			X	X
MA-6(1)	KONSERWACJA ZAPOBIEGAWCZA				
MA-6(2)	KONSERWACJA PLANOWA				
MA-6(3)	AUTOMATYCZNE WSPARCIE W ZAKRESIE KONSERWACJI PROGNOZOWANEJ				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
MA-7	**KONSERWACJA W TERENIE**				

3.10. KATEGORIA MP – OCHRONA NOŚNIKÓW DANYCH

Tabela 3-10 zawiera podsumowanie zabezpieczeń podstawowych i zabezpieczeń rozszerzonych przypisanych do *Kategorii MP – Ochrona nośników danych*. Zabezpieczenia są przypisane do bazowych zabezpieczeń prywatności oraz do bazowych środków bezpieczeństwa o niskim, umiarkowanym i wysokim poziomie wpływu, w zależności od potrzeb. Zabezpieczenie podstawowe lub zabezpieczenie rozszerzone, które zostało wycofane z katalogu zabezpieczeń lub przeniesione do innej kategorii zabezpieczeń, jest oznaczone symbolem "W" z objaśnieniem dokonanym czcionką kursywa w jasnoszarym kolorze, z podaniem miejsca umieszczenia wycofanego / przeniesionego zabezpieczenia podstawowego lub zabezpieczenia rozszerzonego.

TABELA 3-10: KATEGORIA MP - OCHRONA NOŚNIKÓW DANYCH

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
MP-1	**POLITYKA I PROCEDURY**	X	X	X	X
MP-2	**DOSTĘP DO NOŚNIKÓW DANYCH**		X	X	X
MP-2(1)	*OGRANICZONY DOSTĘP AUTOMATYCZNY*	*W: włączone do MP-4(2).*			
MP-2(2)	*OCHRONA KRYPTOGRAFICZNA*	*W: włączone do SC-28(1).*			
MP-3	**OZNAKOWANIE NOŚNIKÓW DANYCH**			X	X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
MP-4	**PRZECHOWYWANIE NOŚNIKÓW DANYCH**			X	X
MP-4(1)	*OCHRONA KRYPTOGRAFICZNA*	*W: włączone do SC-28(1).*			
MP-4(2)	OGRANICZONY DOSTĘP AUTOMATYCZNY				
MP-5	**TRANSPORT NOŚNIKÓW DANYCH**			X	X
MP-5(1)	*OCHRONA POZA STREFAMI KONTROLNYMI*	*W: włączone do MP-5.*			
MP-5(2)	*DOKUMENTOWANIE DZIAŁAŃ*	*W: włączone do MP-5.*			
MP-5(3)	KONWOJENCI				
MP-5(4)	*OCHRONA KRYPTOGRAFICZNA*	*W: włączone do SC-28(1).*			
MP-6	**SANITYZACJA NOŚNIKÓW DANYCH**	X	X	X	X
MP-6(1)	PRZEGLĄD / ZATWIERDZANIE / ŚLEDZENIE / DOKUMENTOWANIE / WERYFIKACJA				X
MP-6(2)	TESTOWANIE SPRZĘTU				X
MP-6(3)	TECHNIKI NIEDESTRUKCYJNE				X
MP-6(4)	*KONTROLOWANE INFORMACJE JAWNE*	*W: włączone do MP-6.*			

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
MP-6(5)	*INFORMACJE NIEJAWNE*	*W: włączone do MP-6.*			
MP-6(6)	*NISZCZENIE NOŚNIKÓW DANYCH*	*W: włączone do MP-6.*			
MP-6(7)	PODWÓJNE UPOWAŻNIENIE				
MP-6(8)	ZDALNE KASOWANIE / WYMAZYWANIE INFORMACJI				
MP-7	**UŻYWANIE NOŚNIKÓW DANYCH**		X	X	X
MP-7(1)	*ZABRONIONE WYKORZYSTANIE NIEZIDENTYFIKOWANEJ WŁASNOŚCI*	*W: włączone do MP-7.*			
MP-7(2)	ZABRONIONE WYKORZYSTANIE MEDIÓW ODPORNYCH NA SANITYZACJĘ				
MP-8	**DEKLASYFIKACJA NOŚNIKÓW DANYCH**				
MP-8(1)	DOKUMENTACJA PROCESU				
MP-8(2)	TESTOWANIE SPRZĘTU				
MP-8(3)	KONTROLOWANE INFORMACJE JAWNE				
MP-8(4)	INFORMACJE NIEJAWNE				

3.11. KATEGORIA PE – OCHRONA FIZYCZNA I ŚRODOWISKOWA

Tabela 3-11 zawiera podsumowanie zabezpieczeń podstawowych i zabezpieczeń rozszerzonych przypisanych do *Kategorii PE – Ochrona fizyczna i środowiskowa*. Zabezpieczenia są przypisane do bazowych zabezpieczeń prywatności oraz do bazowych środków bezpieczeństwa o niskim, umiarkowanym i wysokim poziomie wpływu, w zależności od potrzeb. Zabezpieczenie podstawowe lub zabezpieczenie rozszerzone, które zostało wycofane z katalogu zabezpieczeń lub przeniesione do innej kategorii zabezpieczeń, jest oznaczone symbolem "W" z objaśnieniem dokonanym czcionką kursywa w jasnoszarym kolorze, z podaniem miejsca umieszczenia wycofanego / przeniesionego zabezpieczenia podstawowego lub zabezpieczenia rozszerzonego.

TABELA 3-11: KATEGORIA PE – OCHRONA FIZYCZNA I ŚRODOWISKOWA

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
PE-1	**POLITYKA I PROCEDURY**		X	X	X
PE-2	**ZEZWOLENIA NA DOSTĘP FIZYCZNY**		X	X	X
PE-2(1)	DOSTĘP ZGODNIE Z POSIADANĄ POZYCJĄ / ROLĄ				
PE-2(2)	PODWÓJNA IDENTYFIKACJA				
PE-2(3)	OGRANICZANIE DOSTĘPU BEZ ASYSTY				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
PE-3	**KONTROLA DOSTĘPU FIZYCZNEGO**		X	X	X
PE-3(1)	DOSTĘP DO SYSTEMU				X
PE-3(2)	OBIEKT / OBSZAR SYSTEMU				
PE-3(3)	CIĄGŁOŚĆ OCHRONY FIZYCZNEJ				
PE-3(4)	ZAMYKANE OBUDOWY				
PE-3(5)	OCHRONA PRZED MANIPULACJĄ				
PE-3(6)	*TESTY PENETRACYJNE OBIEKTU*	*W: włączone do CA-8.*			
PE-3(7)	BARIERY FIZYCZNE				
PE-3(8)	ŚLUZY W KONTROLI DOSTĘPU				
PE-4	**KONTROLA DOSTĘPU DO MEDIUM TRANSMISYJNEGO**			X	X
PE-5	**KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA**			X	X
PE-5(1)	*DOSTĘP UPOWAŻNIONYCH OSÓB DO URZĄDZEŃ*	*W: włączone do PE-5.*			

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
PE-5(2)	DOSTĘP DO DANYCH NA PODSTAWIE INDYWIDUALNEJ TOŻSAMOŚCI				
PE-5(3)	*OZNACZANIE URZĄDZEŃ WEJŚCIA - WYJŚCIA*	*W: włączone do PE-22.*			
PE-6	**MONITOROWANIE DOSTĘPU FIZYCZNEGO**		X	X	X
PE-6(1)	ALARMY WŁAMANIOWE I URZĄDZENIA NADZORUJĄCE			X	X
PE-6(2)	AUTOMATYCZNE ROZPOZNAWANIE WŁAMANIA / INFORMOWANIE				
PE-6(3)	MONITORING WIZYJNY				
PE-6(4)	MONITOROWANIE DOSTĘPU FIZYCZNEGO DO SYSTEMÓW				X
PE-7	***KONTROLA GOŚCI***	***W: włączone do PE-2 i PE-3.***			
PE-8	**REJESTRY DOSTĘPU GOŚCI**		X	X	X
PE-8(1)	AUTOMATYCZNA REJESTRACJA / PRZEGLĄD				X
PE-8(2)	*ZAPISY DOTYCZĄCE DOSTĘPU FIZYCZNEGO*	*W: włączone do PE-2.*			
PE-8(3)	OGRANICZANIE ELEMENTÓW DANYCH OSOBOWYCH UMOŻLIWIAJĄCYCH IDENTYFIKACJĘ	X			

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
PE-9	**WYPOSAŻENIE ENERGETYCZNE I OKABLOWANIE**			X	X
PE-9(1)	REDUNDANCJA OKABLOWANIA				
PE-9(2)	AUTOMATYCZNA KONTROLA JAKOŚCI NAPIĘCIA				
PE-10	**WYŁĄCZENIE AWARYJNE**			X	X
PE-10(1)	*PRZYPADKOWA I NIEAUTORYZOWANA AKTYWACJA*	*W: włączone do PE-10.*			
PE-11	**ZASILANIE AWARYJNE**			X	X
PE-11(1)	ALTERNATYWNE ZASILANIE - MINIMALNA ZDOLNOŚĆ OPERACYJNA				X
PE-11(2)	ALTERNATYWNE SAMOOBSŁUGOWE ŹRÓDŁO ZASILANIA				
PE-12	**OŚWIETLENIE AWARYJNE**		X	X	X
PE-12(1)	ZASADNICZE DZIAŁANIA / FUNKCJE BIZNESOWE				
PE-13	**OCHRONA PRZECIWPOŻAROWA**		X	X	X
PE-13(1)	SYSTEMY DETEKCJI - AUTOMATYCZNA AKTYWACJA I POWIADAMIANIE			X	X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
PE-13(2)	SYSTEMY GASZĄCE - AUTOMATYCZNA AKTYWACJA I POWIADOMIENIE				X
PE-13(3)	*AUTOMATYCZNE GASZENIE POŻARU*	*W: włączone do PE-13(2).*			
PE-13(4)	INSPEKCJE				
PE-14	**ZABEZPIECZENIA ŚRODOWISKOWE**		X	X	X
PE-14(1)	STEROWANIE AUTOMATYCZNE				
PE-14(2)	MONITOROWANIE ZA POMOCĄ ALARMÓW I POWIADOMIEŃ				
PE-15	**OCHRONA PRZED ZALANIEM**		X	X	X
PE-15(1)	AUTOMATYCZNE WYKRYWANIE				X
PE-16	**DOSTAWA I USUWANIE**		X	X	X
PE-17	**ZAPASOWE MIEJSCE PRACY**			X	X
PE-18	**LOKALIZACJA KOMPONENTÓW SYSTEMU**				X
PE-18(1)	*LOKALIZACJA OBIEKTU*	*W: włączone do PE-23.*			

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
PE-19	**ULOT INFORMACJI / ELEKTROMAGNETYCZNA EMISJA UJAWNIAJĄCA**				
PE-19(1)	KRAJOWE POLITYKI I PROCEDURY DOTYCZĄCE EMISJI UJAWNIAJĄCEJ				
PE-20	**MONITOROWANIE I ŚLEDZENIE ZASOBÓW**				
PE-21	**OCHRONA PRZED IMPULSEM ELEKTROMAGNETYCZNYM**				
PE-22	**ZNAKOWANIE KOMPONENTÓW**				
PE-23	**LOKALIZACJA OBIEKTU**				

3.12. KATEGORIA PL – PLANOWANIE

Tabela 3-12 zawiera podsumowanie zabezpieczeń podstawowych i zabezpieczeń rozszerzonych przypisanych do *Kategorii PL – Planowanie*. Zabezpieczenia są przypisane do bazowych zabezpieczeń prywatności oraz do bazowych środków bezpieczeństwa o niskim, umiarkowanym i wysokim poziomie wpływu, w zależności od potrzeb. Zabezpieczenie podstawowe lub zabezpieczenie rozszerzone, które zostało wycofane z katalogu zabezpieczeń lub przeniesione do innej kategorii zabezpieczeń, jest oznaczone symbolem "W" z objaśnieniem dokonanym czcionką kursywa w jasnoszarym kolorze, z podaniem miejsca umieszczenia wycofanego / przeniesionego zabezpieczenia podstawowego lub zabezpieczenia rozszerzonego.

TABELA 3-12: KATEGORIA PL – PLANOWANIE

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
PL-1	**POLITYKA I PROCEDURY**	X	X	X	X
PL-2	**PLANY BEZPIECZEŃSTWA SYSTEMU I OCHRONY PRYWATNOŚCI**	X	X	X	X
PL-2(1)	*KONCEPCJA DZIAŁANIA*	*W: włączone do PL-7.*			
PL-2(2)	*ARCHITEKTURA FUNKCJONALNA*	*W: włączone do PL-8.*			
PL-2(3)	*PLANOWANIE / KOORDYNACJA Z INNYMI PODMIOTAMI*	*W: włączone do PL-2.*			

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
	ORGANIZACYJNYMI				
PL-3	***AKTUALIZACJA PLANU BEZPIECZEŃSTWA SYSTEMU***	***W: włączone do PL-2.***			
PL-4	**ZASADY POSTĘPOWANIA**	X	X	X	X
PL-4(1)	MEDIA SPOŁECZNOŚCIOWE I OGRANICZENIA KORZYSTANIA ZE STRON / APLIKACJI ZEWNĘTRZNYCH	X	X	X	X
PL-5	***OCENA WPŁYWU NA PRYWATNOŚĆ***	*W: włączone do RA-8.*			
PL-6	***PLANOWANIE DZIAŁALNOŚCI ZWIĄZANEJ Z BEZPIECZEŃSTWEM***	*W: włączone do PL-2.*			
PL-7	**KONCEPCJA BEZPIECZEŃSTWA DZIAŁAŃ OPERACYJNYCH**				
PL-8	**ARCHITEKTURA BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI**	X		X	X
PL-8(1)	ZABEZPIECZENIE WIELOSTOPNIOWE (OCHRONA WARSTWOWA)				
PL-8(2)	DYWERSYFIKACJA DOSTAWCY				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
PL-9	**ZARZĄDZANIE CENTRALNE**	X			
PL-10	**WYBÓR ZABEZPIECZEŃ BAZOWYCH**		X	X	X
PL-11	**DOSTOSOWYWANIE ZABEZPIECZEŃ BAZOWYCH**		X	X	X

3.13. KATEGORIA PM – PROGRAMY ZARZĄDZANIA

Tabela 3-13 zawiera podsumowanie zabezpieczeń podstawowych i zabezpieczeń rozszerzonych przypisanych do *Kategorii PM – Programy zarządzania*. Zabezpieczenia te są wdrażane na poziomie organizacji i nie są ukierunkowane na poszczególne systemy informatyczne. Program zarządzania zabezpieczeniami ma na celu osiągnięcie zgodności z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami i standardami.

TABELA 3-13: KATEGORIA PM – PROGRAMY ZARZĄDZANIA

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
PM-1	PLAN PROGRAMU BEZPIECZEŃSTWA INFORMACJI		Wdrożone na poziomie organizacji. Wspierają program bezpieczeństwa informacji. Nie mają związku z bazowymi środkami bezpieczeństwa.		
PM-2	ROLE KIEROWNICZE PROGRAMU BEZPIECZEŃSTWA INFORMACJI				
PM-3	ZASOBY W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI I OCHRONY PRYWATNOŚCI	X			
PM-4	PLAN DZIAŁANIA I ETAPY WPROWADZANIA ZABEZPIECZEŃ	X			
PM-5	INWENTARYZACJA SYSTEMU				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
PM-5(1)	REJESTR DANYCH OSOBOWYCH	X	**Niezależne od poziomu wpływu na system.**		
PM-6	**MIARY WYDAJNOŚCI**	X			
PM-7	**STRUKTURA ORGANIZACYJNA**	X			
PM-7(1)	ODCIĄŻENIA				
PM-8	**PLAN INFRASTRUKTURY KRYTYCZNEJ**	X			
PM-9	**STRATEGIA ZARZĄDZANIA RYZYKIEM**	X			
PM-10	**PROCES AUTORYZACJI**	X			
PM-11	**DEFINICJA MISJI I PROCESU BIZNESOWEGO**	X			
PM-12	**ZAGROŻENIA WEWNĘTRZNE**		**Wdrożone na poziomie organizacji.** **Wspierają program bezpieczeństwa informacji.**		
PM-13	**PESONEL BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI**	X			
PM-14	**TESTOWANIE, SZKOLENIA I MONITOROWANIE**	X			
PM-15	**GRUPY I STOWARZYSZENIA ZAJMUJĄCE SIĘ BEZPIECZEŃSTWEM I OCHRONĄ PRYWATNOŚCI**				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
PM-16	**OSTRZEGANIE O ZAGROŻENIACH**		**Nie mają związku z bazowymi środkami bezpieczeństwa.** **Niezależne od poziomu wpływu na system.** **Wdrożone na poziomie**		
PM-16(1)	ZAUTOMATYZOWANE ŚRODKI WYMIANY INFORMACJI O ZAGROŻENIACH				
PM-17	**OCHRONA NADZOROWANYCH INFORMACJI JAWNYCH PRZETWARZANYCH W SYSTEMACH ZEWNĘTRZNYCH**	X			
PM-18	**PLAN PROGRAMU OCHRONY PRYWATNOŚCI**	X			
PM-19	**ROLE KIEROWNICZE PROGRAMU OCHRONY PRYWATNOŚCI**	X			
PM-20	**ROZPOWSZECHNIANIE INFORMACJI O PROGRAMIE OCHRONY PRYWATNOŚCI**	X			
PM-20(1)	POLITYKA PRYWATNOŚCI PREZENTOWANE NA STRONACH INTERNETOWYCH, W APLIKACJACH I USŁUGACH CYFROWYCH	X			
PM-21	**REJESTROWANIE UJAWNIEŃ**	X			
PM-22	**ZARZĄDZANIE JAKOŚCIĄ DANYCH OSOBOWYCH**	X			
PM-23	**ORGAN ZARZĄDZANIA DANYMI**				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
PM-24	**RADA DS. INTEGRALNOŚCI DANYCH**	X	**organizacji. Wspierają program bezpieczeństwa informacji. Nie mają związku z bazowymi środkami bezpieczeństwa. Niezależne od poziomu wpływu na system.**		
PM-25	**MINIMALIZACJA DANYCH OSOBOWYCH WYKORZYSTYWANYCH W TESTACH, SZKOLENIACH I BADANIACH**	X			
PM-26	**ZARZĄDZANIE SKARGAMI**	X			
PM-27	**SPRAWOZDAWCZOŚĆ W ZAKRESIE OCHRONY PRYWATNOŚCI**	X			
PM-28	**OPRACOWYWANIE RAM RYZYKA**	X			
PM-29	**ROLE KIEROWNICZE PROGRAMU ZARZĄDZANIA RYZYKIEM**				
PM-30	**STRATEGIA ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW**				
PM-30(1)	DOSTAWCY ELEMENTÓW KRYTYCZNYCH LUB ISTOTNYCH Z PUNKTU WIDZENIA MISJI				
PM-31	**STRATEGIA CIĄGŁEGO MONITORINGU**	X			
PM-32	**PRZEZNACZENIE**				

3.14. KATEGORIA PS – BEZPIECZEŃSTWO OSOBOWE

Tabela 3-14 zawiera podsumowanie zabezpieczeń podstawowych i zabezpieczeń rozszerzonych przypisanych do *Kategorii PS – Bezpieczeństwo osobowe*. Zabezpieczenia są przypisane do bazowych zabezpieczeń prywatności oraz do bazowych środków bezpieczeństwa o niskim, umiarkowanym i wysokim poziomie wpływu, w zależności od potrzeb. Zabezpieczenie podstawowe lub zabezpieczenie rozszerzone, które zostało wycofane z katalogu zabezpieczeń lub przeniesione do innej kategorii zabezpieczeń, jest oznaczone symbolem "W" z objaśnieniem dokonanym czcionką kursywa w jasnoszarym kolorze, z podaniem miejsca umieszczenia wycofanego / przeniesionego zabezpieczenia podstawowego lub zabezpieczenia rozszerzonego.

TABELA 3-14: KATEGORIA PS – BEZPIECZEŃSTWO OSOBOWE

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
PS-1	**POLITYKA I PROCEDURY**		X	X	X
PS-2	**OKREŚLANIE RYZYKA DLA STANOWISKA PRACY**		X	X	X
PS-3	**DOBÓR PERSONELU**		X	X	X
PS-3(1)	INFORMACJE NIEJAWNE				
PS-3(2)	POSTĘPOWANIA SPRAWDZAJĄCE				
PS-3(3)	INFORMACJE WYMAGAJĄCE SZCZEGÓLNEJ OCHRONY				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
PS-3(4)	WYMAGANIA DOTYCZĄCE OBYWATELSTWA				
PS-4	**ZAKOŃCZENIE ZATRUDNIENIA**		X	X	X
PS-4(1)	ZOBOWIĄZANIA PO ZAKOŃCZENIU ZATRUDNIENIA				
PS-4(2)	AUTOMATYCZNE POWIADAMIANIE				X
PS-5	**OBSADZENIE LUB PRZENIESIENIE STANOWISKA**		X	X	X
PS-6	**UMOWY DOSTĘPU / WSPÓŁPRACY**	X	X	X	X
PS-6(1)	*INFORMACJE WYMAGAJĄCE SZCZEGÓLNEJ OCHRONY*	*W: włączone do PS-3.*			
PS-6(2)	INFORMACJE NIEJAWNE WYMAGAJĄCE OCHRONY SPECJALNEJ				
PS-6(3)	WYMOGI PO ZAKOŃCZENIU ZATRUDNIENIA				
PS-7	**BEZPIECZEŃSTWO OSOBOWE STRON TRZECICH**		X	X	X
PS-8	**SANKCJE PERSONALNE**		X	X	X
PS-9	**OPISY STANOWISK PRACY**		X	X	X

3.15. KATEGORIA PT – PRZEJRZYSTOŚĆ PRZETWARZANIA DANYCH OSOBOWYCH

W tabeli 3-15 przedstawiono podsumowanie zabezpieczeń podstawowych i zabezpieczeń rozszerzonych przypisanych do *Kategorii – Przejrzystość przetwarzania danych osobowych*. Zabezpieczenia te są przypisane do zabezpieczeń bazowych prywatności zgodnie z kryteriami wyboru określonymi w Sekcji 2.2. Zabezpieczenie podstawowe lub zabezpieczenie rozszerzone, które zostało wycofane z katalogu zabezpieczeń lub przeniesione do innej kategorii zabezpieczeń, jest oznaczone symbolem "W" z objaśnieniem dokonanym czcionką kursywa w jasnoszarym kolorze, z podaniem miejsca umieszczenia wycofanego / przeniesionego zabezpieczenia podstawowego lub zabezpieczenia rozszerzonego.

TABELA 3-15: KATEGORIA PT- PRZEJRZYSTOŚĆ PRZETWARZANIA DANYCH OSOBOWYCH

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
PT-1	**POLITYKA I PROCEDURY**	X	**Ochrona przejrzystości przetwarzania danych osobowych nie jest przypisana do bazowych środków bezpieczeństwa.** **Zabezpieczenia bazowe**		
PT-2	**UPRAWNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH**	X			
PT-2(1)	OZNACZANIE DANYCH				
PT-2(2)	AUTOMATYZACJA				
PT-3	**CELE PRZETWARZANIA DANYCH OSOBOWYCH**	X			
PT-3(1)	OZNACZANIE DANYCH				
PT-3(2)	AUTOMATYZACJA				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
PT-4	**ZGODY**	X	**prywatności są wybierane na podstawie tych kryteriów wyboru określonych w Sekcji 2.2.** **Ochrona przejrzystości przetwarzania danych osobowych nie jest przypisana do bazowych środków bezpieczeństwa.** **Zabezpieczenia bazowe prywatności są**		
PT-4(1)	ZGODA NA PODSTAWIE ART. 6 UST. 1 RODO				
PT-4(2)	ZGODA TYPU „JUST-IN TIME”				
PT-4(3)	WYCOFANIE ZGODY				
PT-5	**INFORMACJA O OCHRONIE PRYWATNOŚCI**	X			
PT-5(1)	INFORMACJA NA ŻĄDANIE				
PT-5(2)	OŚWIADCZENIE O OCHRONIE PRYWATNOŚCI	X			
PT-6	**SYSTEM ZAWIADOMIEŃ O REJESTRACH**	X			
PT-6(1)	RUTYNOWE ZASTOSOWANIE	X			
PT-6(2)	ZASADY WYŁĄCZENIA	X			
PT-7	**SZCZEGÓŁOWE KATEGORIE DANYCH OSOBOWYCH**	X			
PT-7(1)	IDENTYFIKATOR OSOBY - NP. NR PESEL	X			
PT-7(2)	PRZETWARZANIE WRAŻLIWYCH DANYCH OSOBOWYCH	X			

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
PT-8	**WYMAGANIA DOTYCZĄCE ZGODNOŚCI PRZY PRZETWARZANIU KOMPUTEROWOWYM**	X	**wybierane na podstawie tych kryteriów wyboru określonych w Sekcji 2.2.**		

3.16. KATEGORIA RA – OCENA RYZYKA

Tabela 3-16 zawiera podsumowanie zabezpieczeń podstawowych i zabezpieczeń rozszerzonych przypisanych do *Kategorii RA – Ocena ryzyka*. Zabezpieczenia są przypisane do bazowych zabezpieczeń prywatności oraz do bazowych środków bezpieczeństwa o niskim, umiarkowanym i wysokim poziomie wpływu, w zależności od potrzeb. Zabezpieczenie podstawowe lub zabezpieczenie rozszerzone, które zostało wycofane z katalogu zabezpieczeń lub przeniesione do innej kategorii zabezpieczeń, jest oznaczone symbolem "W" z objaśnieniem dokonanym czcionką kursywa w jasnoszarym kolorze, z podaniem miejsca umieszczenia wycofanego / przeniesionego zabezpieczenia podstawowego lub zabezpieczenia rozszerzonego.

TABELA 3-16: KATEGORIA RA - OCENA RYZYKA

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
RA-1	**POLITYKA I PROCEDURY**	X	X	X	X
RA-2	**KATEGORYZACJA BEZPIECZEŃSTWA**		X	X	X
RA-2(1)	PRIORYTETYZACJA POZIOMÓW WPŁYWU				
RA-3	**SZACOWANIE RYZYKA**	X	X	X	X
RA-3(1)	SZACOWANIE RYZYKA ŁAŃCUCHA DOSTAW		X	X	X
RA-3(2)	WYMIANA INFORMACJI O ZAGROŻENIACH				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
RA-3(3)	ŚWIADOMOŚĆ DYNAMIKI ZAGROŻEŃ				
RA-3(4)	PROGNOZOWANIA CYBERANALITYKA				
RA-4	*AKTUALIZACJA SZACOWANIA RYZYKA*	*W: włączone do RA-3.*			
RA-5	**MONITOROWANIE I SKANOWANIE PODATNOŚCI**		X	X	X
RA-5(1)	*AKTUALIZACJA NARZĘDZI*	***W: włączone do RA-5.***			
RA-5(2)	NADZOROWANIE WYKRYTYCH PODATNOŚCI		X	X	X
RA-5(3)	ZAKRES PODATNOŚCI				
RA-5(4)	WYKRYWANIE SKANOWANIA				X
RA-5(5)	DOSTĘP UPRZYWILEJOWANY			X	X
RA-5(6)	AUTOMATYCZNE ANALIZY TRENDÓW				
RA-5(7)	*AUTOMATYCZNE WYKRYWANIE I POWIADAMIANIE O NIEAUTORYZOWANYCH KOMPONENTACH*	*W: włączone do CM-8.*			
RA-5(8)	PRZEGLĄD HISTORYCZNYCH LOGÓW AUDYTU				
RA-5(9)	*TESTY PENETRACYJNE I ANALIZY*	*W: włączone do CA-8.*			

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
RA-5(10)	*KORELACJA SKANOWANYCH DANYCH*				
RA-5(11)	PROGRAM UPUBLICZNIANIA PODATNOŚCI		X	X	X
RA-6	**TECHNICZNE ZABEZPIECZENIE PRZED PODGLĄDEM I PODSŁUCHEM**				
RA-7	**REAKCJA NA RYZYKO**	X	X	X	X
RA-8	**OCENY WPŁYWU NA PRYWATNOŚĆ**	X			
RA-9	**ANALIZA KRYTYCZNOŚCI**			X	X
RA-10	**WYSZUKIWANIE ZAGROŻEŃ**				

3.17. KATEGORIA SA – NABYWANIE SYSTEMU I USŁUG

Tabela 3-17 zawiera podsumowanie zabezpieczeń podstawowych i zabezpieczeń rozszerzonych przypisanych do *Kategorii SA – Nabywanie systemu i usług*. Zabezpieczenia są przypisane do bazowych zabezpieczeń prywatności oraz do bazowych środków bezpieczeństwa o niskim, umiarkowanym i wysokim poziomie wpływu, w zależności od potrzeb. Zabezpieczenie podstawowe lub zabezpieczenie rozszerzone, które zostało wycofane z katalogu zabezpieczeń lub przeniesione do innej kategorii zabezpieczeń, jest oznaczone symbolem "W" z objaśnieniem dokonanym czcionką kursywa w jasnoszarym kolorze, z podaniem miejsca umieszczenia wycofanego / przeniesionego zabezpieczenia podstawowego lub zabezpieczenia rozszerzonego.

TABELA 3-17: KATEGORIA SA - NABYWANIE SYSTEMU I USŁUGI

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SA-1	**POLITYKA I PROCEDURY**	X	X	X	X
SA-2	**PRZYDZIAŁ ZASOBÓW**	X	X	X	X
SA-3	**CYKL ŻYCIA SYSTEMU**	X	X	X	X
SA-3(1)	ZARZĄDZANIE ŚRODOWISKIEM PRZEDPRODUKCYJNYM				
SA-3(2)	WYKORZYSTYWANIE DANYCH BIEŻĄCYCH LUB OPERACYJNYCH				
SA-3(3)	ODŚWIEŻANIE TECHNOLOGII				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SA-4	**PROCES NABYCIA**	X	X	X	X
SA-4(1)	WŁAŚCIWOŚCI FUNKCJONALNE ZABEZPIECZEŃ			X	X
SA-4(2)	PROJEKTOWANIE / IMPLEMENTACJA ZABEZPIECZEŃ			X	X
SA-4(3)	METODY, TECHNIKI I PRAKTYKI ROZWOJU				
SA-4(4)	*PRZYPISANIE KOMPONENTÓW DO SYSTEMÓW*	*W: włączone do CM-8(9)*			
SA-4(5)	KONFIGURACJA SYSTEMU, KOMPONENTÓW I USŁUG				X
SA-4(6)	KORZYSTANIE Z PRODUKTÓW ZAPEWNIAJĄCYCH BEZPIECZEŃSTWO INFORMACJI				
SA-4(7)	ZATWIERDZONE PROFILE OCHRONY				
SA-4(8)	PLAN CIĄGŁEGO MONITOROWANIA ZABEZPIECZEŃ				
SA-4(9)	FUNKCJE, PORTY, PROTOKOŁY / USŁUGI			X	X
SA-4(10)	WYKORZYSTANIE ZATWIERDZONYCH PRODUKTÓW		X	X	X
SA-4(11)	SYSTEM DOKUMENTOWANIA				
SA-4(12)	WŁASNOŚĆ DANYCH				
SA-5	**DOKUMENTACJA SYSTEMU**		X	X	X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SA-5(1)	*WŁAŚCIWOŚCI FUNKCJONALNE ZABEZPIECZEŃ*	*W: włączone do SA-4(1).*			
SA-5(2)	*BEZPIECZEŃSTWO INTERFEJSÓW SYSTEMU ZEWNĘTRZNEGO*	*W: włączone do SA-4(2).*			
SA-5(3)	*PROJEKTOWANIE WYSOKOPOZIOMOWE*	*W: włączone do SA-4(2).*			
SA-5(4)	*PROJEKTOWANIE NISKOPOZIOMOWE*	*W: włączone do SA-4(2).*			
SA-5(5)	*KOD ŹRÓDŁOWY*	*W: włączone do SA-4(2).*			
SA-6	***OGRANICZENIA W UŻYCIU OPROGRAMOWANIA***	***W: włączone do CM-10 i SI-7.***			
SA-7	***OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA***	***W: włączone do CM-11 i SI-7.***			
SA-8	**ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI**		X	X	X
SA-8(1)	PRZEJRZYSTE ABSTRAKCJE				
SA-8(2)	MINIMALIZACJA MECHANIZMÓW WSPÓLNYCH				
SA-8(3)	MODUŁOWOŚĆ I WARSTWOWOŚĆ				
SA-8(4)	UPORZĄDKOWANIE ZALEŻNOŚCI POMIĘDZY SEGMENTAMI SYSTEMU				
SA-8(5)	DOSTĘP Z EFEKTYWNĄ MEDIACJĄ				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SA-8(6)	MINIMALIZACJA WSPÓŁUŻYTKOWANIA				
SA-8(7)	ZMNIEJSZONA ZŁOŻONOŚĆ				
SA-8(8)	BEZPIECZNA EWOLUCJA				
SA-8(9)	ZAUFANE KOMPONENTY				
SA-8(10)	ZAUFANIE HIERARCHICZNE				
SA-8(11)	ODWROTNY PRÓG MODYFIKACJI				
SA-8(12)	OCHRONA HIERARCHICZNA				
SA-8(13)	MINIMALIZACJA ELEMENTÓW BEZPIECZEŃSTWA				
SA-8(14)	ZASADA NAJMNIEJSZEGO UPRZYWILEJOWANIA				
SA-8(15)	PREDYKAT ZEZWOLEŃ				
SA-8(16)	SAMOISTNA WIARYGODNOŚĆ				
SA-8(17)	BEZPIECZNY SKŁAD ROZPROSZONY				
SA-8(18)	ZAUFANE KANAŁY KOMUNIKACJI				
SA-8(19)	CIĄGŁA OCHRONA				
SA-8(20)	BEZPIECZNE ZARZĄDZANIE METADANYMI				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SA-8(21)	SAMOANALIZY				
SA-8(22)	ROZLICZALNOŚĆ I IDENTYFIKOWALNOŚĆ				
SA-8(23)	ZABEZPIECZENIA DOMYŚLNE				
SA-8(24)	BEZPIECZNA AWARIA I ODZYSKIWANIE DANYCH				
SA-8(25)	BEZPIECZEŃSTWO EKONOMICZNE				
SA-8(26)	PEWNOŚĆ DZIAŁANIA				
SA-8(27)	BEZPIECZEŃSTWO UWZGLĘDNIAJĄCE CZYNNIK LUDZKI				
SA-8(28)	AKCEPTOWALNY POZIOM BEZPIECZEŃSTWA				
SA-8(29)	POWTARZALNE I UDOKUMENTOWANE PROCEDURY				
SA-8(30)	RYGOR PROCEDURALNY				
SA-8(31)	BEZPIECZNA MODYFIKACJA SYSTEMU				
SA-8(32)	MIEZBĘDNA DOKUMENTACJA				
SA-8(33)	ZASADA MINIMALIZACJA	X			
SA-9	**USŁUGI SYSTEMU ZEWNĘTRZNEGO**	X	X	X	X
SA-9(1)	OCENY RYZYKA / ZATWIERDZENIA ORGANIZACYJNE				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SA-9(2)	IDENTYFIKACJA FUNKCJI, PORTÓW, PROTOKOŁÓW I USŁUG			X	X
SA-9(3)	TWORZENIE / UTRZYMANIE RELACJI ZAUFANIA Z DOSTAWCAMI				
SA-9(4)	ZGODNOŚĆ INTERESÓW KONSUMENTÓW I DOSTAWCÓW				
SA-9(5)	OBSZAR PROCESOWANIA, PRZECHOWYWANIA I OBSŁUGI TECHNICZNEJ				
SA-9(6)	NADZOROWANIE ZARZĄDZANIA KLUCZAMI KRYPTOGRAFICZNYMI PRZEZ ORGANIZACJĘ				
SA-9(7)	ORGANIZACYJNIE KONTROLOWANE ZABEZPIECZENIA INTEGRALNOŚCI				
SA-9(8)	MIEJSCE PRZETWARZANIA I PRZECHOWYWANIA - JURYSDYKCJA KRAJOWA				
SA-10	**ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA**			X	X
SA-10(1)	WERYFIKACJA INTEGRALNOŚCI PROGRAMÓW I OPROGRAMOWANIA UKŁADOWEGO				
SA-10(2)	ALTERNATYWNE PROCESY ZARZĄDZANIA KONFIGURACJĄ				
SA-10(3)	WERYFIKACJA INTEGRALNOŚCI SPRZĘTU				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SA-10(4)	ZAUFANA GENERACJA				
SA-10(5)	INTEGRALNOŚĆ MAPOWANIA KONTROLI WERSJI				
SA-10(6)	ZAUFANA DYSTRYBUCJA				
SA-10(7)	PERSONEL BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI				
SA-11	**TESTOWANIE I OCENA PRZEZ DEWELOPERA**	X		X	X
SA-11(1)	ANALIZA KODU STATYCZNEGO				
SA-11(2)	MODELOWANIE ZAGROŻEŃ I ANALIZA PODATNOŚCI NA ZAGROŻENIA				
SA-11(3)	NIEZALEŻNA WERYFIKACJA PLANÓW OCENY / EWIDENCJA				
SA-11(4)	MANUALNY PRZEGLĄD KODU				
SA-11(5)	TESTOWANIE PENETRACYJNE				
SA-11(6)	PRZEGLĄD PŁASZCZYZNY ATAKU				
SA-11(7)	WERYFIKACJA ZAKRESU TESTU / OCENA				
SA-11(8)	DYNAMICZNA ANALIZA KODU				
SA-11(9)	INTERAKTYWNE TESTOWANIE BEZPIECZEŃSTWA APLIKACJI				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SA-12	***BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW***	***W: włączone do Kategorii SR.***			
SA-12(1)	*STRATEGIE ZAKUPÓW, NARZĘDZIA I METODY*	*W: włączone do SR-5.*			
SA-12(2)	*DYWERSYFIKACJA DOSTAWCÓW*	*W: włączone do SR-6.*			
SA-12(3)	*ZAUFANA WYSYŁKA I MAGAZYNOWANIE*	*W: włączone do SR-3.*			
SA-12(4)	*RÓŻNORODNOŚĆ DOSTAWCÓW*	*W: włączone do SR-3(1).*			
SA-12(5)	*OGRANICZENIE SZKODY*	*W: włączone do SR-3(2).*			
SA-12(6)	*MINIMALIZACJA CZASU ZAMÓWIENIA*	*W: włączone do SR-5(1).*			
SA-12(7)	*OCENY PRZED WYBOREM / ODBIOREM / AKTUALIZACJĄ*	*W: włączone do SR-5(2).*			
SA-12(8)	*POZYSKIWANIE INFORMACJI Z WSZYSTKICH DOSTĘPNYCH ŹRÓDEŁ*	*W: włączone do RA-3(2).*			
SA-12(9)	*BEZPIECZEŃSTWO OPERACYJNE*	*W: włączone do SR-7.*			
SA-12(10)	*OCENA ORYGINALNOŚCI I NIEZMIENNOŚCI*	*W: włączone do SR-4(3).*			
SA-12(11)	*TESTOWANIE PENETRACYJNE / ANALIZA ELEMENTÓW, PROCESÓW I WYKONAWCÓW*	*W: włączone do SR-6(1).*			
SA-12(12)	*UMOWY MIĘDZYORGANIZACYJNE*	*W: włączone do SR-8.*			

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SA-12(13)	*KOMPONENTY KRYTYCZNE SYSTEMU INFORMATYCZNEGO*	*W: włączone do MA-6 i RA-9.*			
SA-12(14)	*IDENTYFIKACJA I ŚLEDZENIE*	*W: włączone do SR-4(1) i SR-4(2).*			
SA-12(15)	*MECHANIZMY ADRESOWANIA SŁABYCH STRON LUB WAD*	*W: włączone do SR-3.*			
SA-13	***WIARYGODNOŚĆ***	***W: włączone do SA-8.***			
SA-14	***ANALIZA KRYTYCZNOŚCI***	***W: włączone do RA-9.***			
SA-14(1)	*KRYTYCZNE KOMPONENTY POZBAWIONE ALTERNATYWNEGO ŹRÓDŁA ZAOPATRZENIA*	*W: włączone do SA-20.*			
SA-15	**PROCES ROZWOJU, STANDARDY I NARZĘDZIA**			X	X
SA-15(1)	METRYKI JAKOŚCI				
SA-15(2)	NARZĘDZIA DO MONITOROWANIA BEZPIECZEŃSTWA I PRYWATNOŚCI				
SA-15(3)	ANALIZA KRYTYCZNOŚCI			X	X
SA-15(4)	*MODELOWANIE ZAGROŻEŃ / ANALIZA PODATNOŚCI*	*W: włączone do SA-11(2).*			
SA-15(5)	OGRANICZANIE PŁASZCZYZNY ATAKU				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SA-15(6)	CIĄGŁE DOSKONALENIE				
SA-15(7)	ZAUTOMATYZOWANA ANALIZA PODATNOŚCI				
SA-15(8)	PONOWNIE UŻYCIE INFORMACJI O ZAGROŻENIACH I PODATNOŚCI				
SA-15(9)	*KREATYWNE WYKORZYSTANIE DANYCH*	*W: włączone do SA-3(2).*			
SA-15(10)	PLAN ODPOWIEDZI NA INCYDENT				
SA-15(11)	ARCHIWIZACJA SYSTEMU LUB KOMPONENTU				
SA-15(12)	MINIMALIZACJA INFORMACJI UMOŻLIWIAJĄCYCH IDENTYFIKACJĘ OSOBY				
SA-16	**SZKOLENIA PROWADZONE PRZEZ DEWELOPERA**				X
SA-17	**ARCHITEKTURA ORAZ PROJEKT BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI DEWELOPERA**				X
SA-17(1)	FORMALNY MODEL POLITYKI				
SA-17(2)	BAZOWE ELEMENTY BEZPIECZEŃSTWA				
SA-17(3)	FORMALNA SPECYFIKACJA				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SA-17(4)	NIEFORMALNE SPECYFIKACJE				
SA-17(5)	PROJEKT PROSTY KONCEPCYJNIE				
SA-17(6)	STRUKTURA DO TESTOWANIA				
SA-17(7)	STRUKTURA DLA NAJNIŻSZYCH UPRAWNIEŃ				
SA-17(8)	ARANŻACJA (ORKIESTRACJA)				
SA-17(9)	ROZPROSZENIE PROJEKTOWANIA				
SA-18	***ODPORNOŚĆ NA SABOTAŻ I WYKRYWANIE MANIPULACJI***	***W: włączone do SR-9.***			
SA-18(1)	*WIELOFAZOWOŚĆ CYKLU ŻYCIA SYSTEMU*	*W: włączone do SR-9(1).*			
SA-18(2)	*KONTROLA SYSTEMÓW INFORMATYCZNYCH, KOMPONENTÓW LUB URZĄDZEŃ*	*W: włączone do SR-10.*			
SA-19	***AUTENTYCZNOŚĆ KOMPONENTÓW***	***W: włączone do SR-11.***			
SA-19(1)	*SZKOLENIE / ROZPOZNAWANIE AUTENTYCZNOŚCI*	*W: włączone do SR-11(1).*			
SA-19(2)	*KONTROLA KONFIGURACJI NA POTRZEBY SERWISOWANIA / NAPRAWY KOMPONENTÓW*	*W: włączone do SR-11(2).*			
SA-19(3)	*UTYLIZACJA KOMPONENTÓW*	*W: włączone do SR-12.*			

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SA-19(4)	*SKANOWANIE AUTENTYCZNOŚCI*	*W: włączone do SR-10(3).*			
SA-20	**NIESTANDARDOWA (NA ZAMÓWIENIE) ROZBUDOWA KOMPONENTÓW KRYTYCZNYCH**				
SA-21	**DOBÓR DEWELOPERÓW**				X
SA-21(1)	*OCENA PRZEGLĄDU*	*W: włączone do SA-21.*			
SA-22	**KOMPONENTY SYSTEMU BEZ WSPARCIA**		X	X	X
SA-22(1)	**ALTERNATYWNE ŹRÓDŁA STAŁEGO WSPARCIA**	*W: włączone do SA-22.*			
SA-23	**SPECJALIZACJA**				

3.18. KATEGORIA SC – OCHRONA SYSTEMÓW I SIECI TELEKOMUNIKACYJNYCH

Tabela 3-18 zawiera podsumowanie zabezpieczeń podstawowych i zabezpieczeń rozszerzonych przypisanych do *Kategorii SC – Ochrona systemów i sieci telekomunikacyjnych*. Zabezpieczenia są przypisane do bazowych zabezpieczeń prywatności oraz do bazowych środków bezpieczeństwa o niskim, umiarkowanym i wysokim poziomie wpływu, w zależności od potrzeb. Zabezpieczenie podstawowe lub zabezpieczenie rozszerzone, które zostało wycofane z katalogu zabezpieczeń lub przeniesione do innej kategorii zabezpieczeń, jest oznaczone symbolem "W" z objaśnieniem dokonanym czcionką kursywa w jasnoszarym kolorze, z podaniem miejsca umieszczenia wycofanego / przeniesionego zabezpieczenia podstawowego lub zabezpieczenia rozszerzonego.

TABELA 3-18: KATEGORIA SC – OCHRONA SYSTEMÓW I SIECI TELEKOMUNIKACYJNYCH

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SC-1	**POLITYKA I PROCEDURY**		X	X	X
SC-2	**ROZDZIELENIE FUNKCJONALNOŚCI SYSTEMU I UŻYTKOWNIKA**			X	X
SC-2(1)	INTERFEJSY DLA UŻYTKOWNIKÓW NIEUPRZYWILEJOWANYCH				
SC-2(2)	NIEPOŁĄCZALNOŚĆ (DEZASOCJACJA)				
SC-3	**IZOLACJA FUNKCJI BEZPIECZEŃSTWA**				X
SC-3(1)	SEPARACJA SPRZĘTOWA				
SC-3(2)	FUNKCJE KONTROLI DOSTĘPU I PRZEPŁYWU				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SC-3(3)	MINIMALIZACJA FUNKCJONALNOŚCI NIE ZWIĄZANYCH Z BEZPIECZEŃSTWEM				
SC-3(4)	MODUŁ SPRZĘŻENIA I SPÓJNOŚCI				
SC-3(5)	STRUKTURY WARSTWOWE				
SC-4	**INFORMACJE NA WSPÓŁDZIELONYCH ZASOBACH SYSTEMOWYCH**			X	X
SC-4(1)	*POZIOMY BEZPIECZEŃSTWA*	*W: włączone do SC-4.*			
SC-4(2)	PRZETWARZANIE WIELOPOZIOMOWE LUB OKRESOWE				
SC-5	**OCHRONA PRZED BLOKADĄ USŁUG (DoS)**		X	X	X
SC-5(1)	OGRANICZENIE MOŻLIWOŚCI ATAKOWANIA INNYCH SYSTEMÓW				
SC-5(2)	PRZEPUSTOWOŚĆ, SZEROKOŚĆ PASMA I NADMIAROWOŚĆ				
SC-5(3)	WYKRYWANIE I MONITOROWANIE				
SC-6	**DOSTĘPNOŚĆ ZASOBÓW**				
SC-7	**OCHRONA POŁĄCZEŃ BRZEGOWYCH**		X	X	X
SC-7(1)	*FIZYCZNIE ODDZIELONE PODSIECI*	*W: włączone do SC-7.*			
SC-7(2)	*DOSTĘP PUBLICZNY*	*W: włączone do SC-7.*			
SC-7(3)	PUNKTY DOSTĘPOWE			X	X
SC-7(4)	ZEWNĘTRZNE USŁUGI TELEKOMUNIKACYJNE			X	X
SC-7(5)	ODRZUĆ DOMYŚLNIE / POZWÓL NA WYJĄTEK			X	X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SC-7(6)	*ODPOWIEDŹ NA ROZPOZNANE AWARIE*	*W: włączone do SC-7(18).*			
SC-7(7)	DZIELONE TUNELOWANIE URZĄDZEŃ ZDALNYCH			X	X
SC-7(8)	RUCH TELEKOMUNIKACYJNY DO AUTORYZOWANYCH SERWERÓW PROXY			X	X
SC-7(9)	OGRANICZENIE ZAGROŻEŃ WYJŚCIOWEGO RUCHU TELEKOMUNIKACYJNEGO				
SC-7(10)	ZAPOBIEGANIE EKSFILTRACJI				
SC-7(11)	OGRANICZENIE PRZYCHODZĄCEGO RUCHU KOMUNIKACYJNEGO				
SC-7(12)	SYSTEM OCHRONY KOMPUTERA GŁÓWNEGO TYPU HOST				
SC-7(13)	IZOLACJA NARZĘDZI BEZPIECZEŃSTWA / MECHANIZMÓW / KOMPONENTÓW WSPARCIA				
SC-7(14)	OCHRONA PRZED NIEAUTORYZOWANYMI POŁĄCZENIAMI FIZYCZNYMI				
SC-7(15)	SIECIOWY DOSTĘP UPRZYWILEJOWANY				
SC-7(16)	ZAPOBIEGANIE WYKRYWANIU KOMPONENTÓW SYSTEMU				
SC-7(17)	AUTOMATYCZNE EGZEKWOWANIE FORMATÓW PROTOKOŁU				
SC-7(18)	BŁĄD BEZPIECZEŃSTWA				X
SC-7(19)	BLOKOWANIE KOMUNIKACJI Z HOSTAMI SPOZA ORGANIZACJI				
SC-7(20)	DYNAMICZNA IZOLACJA I SEGREGACJA				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SC-7(21)	IZOLACJA ELEMENTÓW SYSTEMU				X
SC-7(22)	ODDZIELNE PODSIECI DO PODŁĄCZENIA DO RÓŻNYCH DOMEN BEZPIECZEŃSTWA				
SC-7(23)	WYŁĄCZENIE INFORMACJI ZWROTNEJ NADAWCY W PRZYPADKU AWARII PROTOKOŁU UWIERZYTELNIAJĄCEGO				
SC-7(24)	DANE OSOBOWE	X			
SC-7(25)	BEZPIECZNE POŁĄCZENIA KRAJOWYCH SYSTEMÓW JAWNYCH				
SC-7(26)	BEZPIECZNE POŁĄCZENIA KRAJOWYCH SYSTEMÓW NIEJAWNYCH				
SC-7(27)	BEZPIECZNE POŁĄCZENIA TRANSGRANICZNYCH SYSTEMÓW JAWNYCH				
SC-7(28)	POŁĄCZENIA Z SIECIAMI PUBLICZNYMI				
SC-7(29)	SEPARACJA PODSIECI W CELU ODIZOLOWANIA FUNKCJI				
SC-8	**POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI**			X	X
SC-8(1)	OCHRONA KRYPTOGRAFICZNA			X	X
SC-8(2)	OBSŁUGA „PRZED" I „PO" TRANSMISJI				
SC-8(3)	OCHRONA KRYPTOGRAFICZNA ZEWNĘTRZNYCH KOMUNIKATÓW				
SC-8(4)	UKRYWANIE LUB RANDOMIZOWANIE KOMUNIKACJI				
SC-8(5)	CHRONIONY SYSTEM DYSTRYBUCJI				
SC-9	*POUFNOŚĆ TRANSMISJI*	*W: włączone do SC-8.*			

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SC-10	**ZAKOŃCZENIE POŁĄCZENIA SIECIOWEGO**			X	X
SC-11	**ZAUFANA ŚCIEŻKA KOMUNIKACYJNA**				
SC-11(1)	NIEPODWAŻALNA ŚCIEŻKA KOMUNIKACYJNA				
SC-12	**GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI**		X	X	X
SC-12(1)	DOSTĘPNOŚĆ				X
SC-12(2)	KLUCZE SYMETRYCZNE				
SC-12(3)	KLUCZE ASYMETRYCZNE				
SC-12(4)	*CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO*	*W: włączone do SC-12(3).*			
SC-12(5)	*CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO / TOKENY SPRZĘTOWE*	*W: włączone do SC-12(3).*			
SC-12(6)	FIZYCZNE ZABEZPIECZENIE KLUCZY KRYPTOGRAFICZNYCH				
SC-13	**OCHRONA KRYPTOGRAFICZNA**		X	X	X
SC-13(1)	*KRYPTOGRAFIA KOMERCYJNA*	*W: włączone do SC-13.*			
SC-13(2)	*KRYPTOGRAFIA ZATWIERDZONA PRZEZ KRAJOWĄ WŁADZĘ BEZPIECZEŃSTWA*	*W: włączone do SC-13.*			
SC-13(3)	*OSOBY NIEPOSIADAJĄCE FORMALNYCH ZEZWOLEŃ NA DOSTĘP*	*W: włączone do SC-13.*			
SC-13(4)	*PODPISY CYFROWE*	*W: włączone do SC-13.*			
SC-14	***OCHRONA DOSTĘPU PUBLICZNEGO***	*W: włączone do AC-2, AC-3, AC-5, SI-3, SI-4, SI-5, SI-7, SI-10.*			

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SC-15	**WSPÓŁPRACUJĄCE URZĄDZENIA I APLIKACJE**		X	X	X
SC-15(1)	ODŁĄCZENIE FIZYCZNE LUB LOGICZNE				
SC-15(2)	*BLOKOWANIE RUCHU WEJŚCIOWEGO / WYJŚCIOWEGO*	*W: włączone do SC-7.*			
SC-15(3)	DEZAKTYWACJA / USUWANIE W CHRONIONYCH OBSZARACH PRACY				
SC-15(4)	WYRAŹNIE WYKAZANIE AKTUALNYCH UŻYTKOWNIKÓW				
SC-16	**TRANSMISJA ATRYBUTÓW BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI**				
SC-16(1)	WERYFIKACJA INTEGRALNOŚCI				
SC-16(2)	MECHANIZMY ANTYSPOOFINGOWE				
SC-16(3)	POWIĄZANIE KRYPTOGRAFICZNE				
SC-17	**CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO**			X	X
SC-18	**KOD MOBILNY**			X	X
SC-18(1)	IDENTYFIKACJA NIEDOPUSZCZALNEGO KODU / PODEJMOWANIE DZIAŁAŃ NAPRAWCZYCH				
SC-18(2)	NABYCIE / OPRACOWYWANIE / UŻYTKOWANIE				
SC-18(3)	ZAPOBIEGANIE POBIERANIU I WYKONYWANIU				
SC-18(4)	ZAPOBIEGANIE AUTOMATYCZNEMU WYKONANIU				
SC-18(5)	POZWALANIE NA WYKONANIE TYLKO W OGRANICZONYCH ŚRODOWISKACH				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SC-19	*PROTOKÓŁ TRANSMISJI PAKIETOWEJ (VOIP)*	*Specyficzne dla danej technologii; uwzględnione w zabezpieczeniach innych protokołów.*			
SC-20	**BEZPIECZEŃSTWO NAZW DOMEN / ADRESÓW IP (AUTENTYCZNOŚĆ POCHODZENIA)**		X	X	X
SC-20(1)	*STREFA PODRZĘDNA (PODPRZESTRZEŃ)*	*W: włączone do SC-20.*			
SC-20(2)	INTEGRALNOŚĆ DANYCH				
SC-21	**BEZPIECZEŃSTWO NAZW DOMEN / USŁUGA USTALANIA ADRESU IP**		X	X	X
SC-21(1)	*INTEGRALNOŚĆ*	*W: włączone do SC-21.*			
SC-22	**ARCHITEKTURA NAZW DOMEN / ADRESÓW IP / ZAMAWIANIE USŁUGI DNS**		X	X	X
SC-23	**AUTENTYCZNOŚĆ SESJI**			X	X
SC-23(1)	UNIEWAŻNIENIE IDENTYFIKATORÓW SESJI PO WYLOGOWANIU				
SC-23(2)	*WYLOGOWANIE INICJOWANE PRZEZ UŻYTKOWNIKA / WYŚWIETLANIE WIADOMOŚCI*	W: włączone do AC-12(1).			
SC-23(3)	UNIKATOWE IDENTYFIKATORY SESJI GENEROWANE PRZEZ SYSTEM				
SC-23(4)	*LOSOWE UNIKALNE IDENTYFIKATORY SESJI*	W: włączone do SC-23(3).			
SC-23(5)	AUTORYZOWANE URZĘDY CERTYFIKACYJNE				
SC-24	**PRZEJŚCIE DO OKREŚLONEGO STANU SYSTEMU PO BŁĘDZIE**				X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SC-25	**THIN NODES / TERMINALOWE STACJE ROBOCZE**				
SC-26	**WABIKI**				
SC-26(1)	*WYKRYWANIE KODU ZŁOŚLIWEGO*	*W: włączone do SC-35.*			
SC-27	**WIELOPLATFORMOWOŚĆ APLIKACJI**				
SC-28	**OCHRONA DANYCH W SKŁADOWANIU / KOPIE KONFIGURACJI SYSTEMU**			X	X
SC-28(1)	OCHRONA KRYPTOGRAFICZNA			X	X
SC-28(2)	PRZECHOWYWANIE W TRYBIE OFF-LINE				
SC-28(3)	KLUCZE KRYPTOGRAFICZNE				
SC-29	**HETEROGENICZNOŚĆ SYSTEMU**				
SC-29(1)	TECHNIKI WIRTUALIZACJI				
SC-30	**MASKOWANIE I DEZINFORMACJA**				
SC-30(1)	*TECHNIKI WIRTUALIZACJI*	*W: włączone do SC-29(1).*			
SC-30(2)	LOSOWOŚĆ				
SC-30(3)	*ZMIANA LOKALIZACJI PRZETWARZANIA / PRZECHOWYWANIA*				
SC-30(4)	INFORMACJE DEZINFORMUJĄCE				
SC-30(5)	UKRYWANIE KOMPONENTÓW SYSTEMU				
SC-31	**ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI**				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SC-31(1)	TESTOWANIE KANAŁÓW UKRYTYCH POD KĄTEM MOŻLIWOŚCI ICH WYKORZYSTANIA				
SC-31(2)	MAKSYMALNA PRZEPUSTOWOŚĆ ŁĄCZA				
SC-31(3)	POMIAR PRZEPUSTOWOŚCI W ŚRODOWISKU OPERACYJNYM				
SC-32	**DZIELENIE SYSTEMU NA PARTYCJE**				
SC-32(1)	FIZYCZNE WYDZIELONE DOMENY DLA FUNKCJI UPRZYWILEJOWANYCH				
SC-33	***INTEGRALNOŚĆ TRANSMISJI***	*W: włączone do SC-8.*			
SC-34	**NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE**				
SC-34(1)	NIEZAPISYWALNE PAMIĘCI				
SC-34(2)	OCHRONA INTEGRALNOŚCI / NOŚNIKI TYLKO DO ODCZYTU				
SC-34(3)	*OCHRONA SPRZĘTOWA*	*W: włączone do SC-51.*			
SC-35	**ZEWNĘTRZNA IDENTYFIKACJA ZŁOŚLIWEGO KODU**				
SC-36	**PRZETWARZANIE I PRZECHOWYWANIE ROZPROSZONE**				
SC-36(1)	TECHNIKI PRZEGLĄDANIA CYKLICZNEGO				
SC-36(2)	SYNCHRONIZACJA				
SC-37	**KANAŁY POZAPASMOWE**				
SC-37(1)	GWARANTOWANA DOSTAWA / TRANSMISJA				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SC-38	**BEZPIECZEŃSTWO OPERACJI**				
SC-39	**IZOLACJA PROCESÓW**		X	X	X
SC-39(1)	SEPARACJA SPRZĘTOWA				
SC-39(2)	ODDZIELNA DOMENA WYKONAWCZA DLA KAŻDEGO WĄTKU				
SC-40	**OCHRONA ŁĄCZA BEZPRZEWODOWEGO**				
SC-40(1)	INTERFERENCJA ELEKTROMAGNETYCZNA				
SC-40(2)	REDUKCJA POTENCJALNEJ DETEKCJI				
SC-40(3)	NAŚLADOWCZE LUB MANIPULACYJNE OSZUSTWO TELEKOMUNIKACYJNE				
SC-40(4)	IDENTYFIKACJA PARAMETRÓW SYGNAŁU				
SC-41	**DOSTĘP DO PORTÓW I URZĄDZEŃ WEJŚCIA / WYJŚCIA**				
SC-42	**CZUJNIKI**				
SC-42(1)	RAPORTOWANIE DO UPOWAŻNIONYCH OSÓB LUB RÓL				
SC-42(2)	*AUTORYZOWANE UŻYCIE*				
SC-42(3)	*ZABRONIONE WYKORZYSTANIE URZĄDZEŃ*	*W: włączone do SC-42.*			
SC-42(4)	POWIADOMIENIE O ZBIERANIU DANYCH				
SC-42(5)	MINIMALIZACJA GROMADZENIA DANYCH				
SC-43	**OGRANICZENIA UŻYCIA**				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SC-44	**KOMORY DETONACYJNE**				
SC-45	**SYNCHRONIZACJA CZASU SYSTEMOWEGO**				
SC-45(1)	SYNCHRONIZACJA Z AUTORYZOWANYM ŹRÓDŁEM CZASU ODNIESIENIA				
SC-45(2)	WTÓRNE AUTORYTATYWNE ŹRÓDŁO CZASU				
SC-46	**EGZEKWOWANIE POLITYKI MIĘDZYDOMENOWEJ**				
SC-47	**ALTERNATYWNE ŚCIEŻKI KOMUNIKACYJNE**				
SC-48	**ROZMIWSZCZENIE CZUJNIKÓW**				
SC-48(1)	DYNAMICZNE PRZEMIESZCZANIE CZUJNIKÓW LUB URZĄDZEŃ MONITORUJĄCYCH				
SC-49	**EGZEKWOWANIE SEPARACJI SPRZĘTOWEJ / POLITYKA EGZEKWOWANIA**				
SC-50	**EGZEKWOWANIE SEPARACJI PROGRAMOWEJ / POLITYKA EGZEKWOWANIA**				
SC-51	**OCHRONA SPRZĘTOWA**				

3.19. KATEGORIA SI – INTEGRALNOŚĆ SYSTEMU I INFORMACJI

Tabela 3-19 zawiera podsumowanie zabezpieczeń podstawowych i zabezpieczeń rozszerzonych przypisanych do *Kategorii SI – Integralność systemu i informacji*. Zabezpieczenia są przypisane do bazowych zabezpieczeń prywatności oraz do bazowych środków bezpieczeństwa o niskim, umiarkowanym i wysokim poziomie wpływu, w zależności od potrzeb. Zabezpieczenie podstawowe lub zabezpieczenie rozszerzone, które zostało wycofane z katalogu zabezpieczeń lub przeniesione do innej kategorii zabezpieczeń, jest oznaczone symbolem "W" z objaśnieniem dokonanym czcionką kursywa w jasnoszarym kolorze, z podaniem miejsca umieszczenia wycofanego / przeniesionego zabezpieczenia podstawowego lub zabezpieczenia rozszerzonego.

TABELA 3-19: KATEGORIA SI - INTEGRALNOŚCI SYSTEMU I INFORMACJI

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SI-1	**POLITYKA I PROCEDURY**	X	X	X	X
SI-2	**USUWANIE USTEREK**		X	X	X
SI-2(1)	*ZARZĄDZANIE CENTRALNE*	W: włączone do PL-9.			
SI-2(2)	ZAUTOMATYZOWANE USUWANIE USTEREK			X	X
SI-2(3)	CZAS DO USUNIĘCIA USTERKI / STANDARDY DZIAŁAŃ NAPRAWCZYCH				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SI-2(4)	AUTOMATYCZNE ŚCIEŻKI ZARZĄDZANIA NARZĘDZIAMI				
SI-2(5)	AUTOMATYCZNE AKTUALIZACJE APLIKACJI / OPROGRAMOWANIA UKŁADOWEGO				
SI-2(6)	USUWANIE POPRZEDNICH WERSJI APLIKACJI / OPROGRAMOWANIA UKŁADOWEGO				
SI-3	**ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM**		X	X	X
SI-3(1)	*ZARZĄDZANIE CENTRALNE*	*W: włączone do PL-9.*			
SI-3(2)	*AUTOMATYCZNE AKTUALIZACJE*	*W: włączone do SI-3.*			
SI-3(3)	*NIEUPRZYWILEJOWANI UŻYTKOWNICY*	*W: włączone do AC-6(10).*			
SI-3(4)	AKTUALIZACJE WYŁĄCZNIE PRZEZ UPRAWNIONYCH UŻYTKOWNIKÓW				
SI-3(5)	*PRZENOŚNE URZĄDZENIA MAGAZYNUJĄCE*	*W: włączone do MP-7.*			
SI-3(6)	TESTOWANIE I WERYFIKACJA				
SI-3(7)	*WYKRYWANIE BEZSYGNATUROWE*	*W: włączone do SI-3.*			
SI-3(8)	WYKRYWANIE NIEAUTORYZOWANYCH KOMEND				
SI-3(9)	*ZDALNE POLECENIA AUTENTYFIKACYJNE*	*W: włączone do AC-17(10).*			

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SI-3(10)	ANALIZA KODU ZŁOŚLIWEGO				
SI-4	**MONITOROWANIE SYSTEMU**		X	X	X
SI-4(1)	SYSTEM WYKRYWANIA WŁAMAŃ I NAPADÓW W CAŁYM SYSTEMIE				
SI-4(2)	AUTOMATYCZNE NARZĘDZIA I MECHANIZMY ANALIZY W CZASIE RZECZYWISTYM			X	X
SI-4(3)	AUTOMATYCZNA INTEGRACJA NARZĘDZI I MECHANIZMÓW				
SI-4(4)	WEJŚCIOWY / WYJŚCIOWY RUCH TELEKOMUNIKACYJNY			X	X
SI-4(5)	ALERTY SYSTEMOWE			X	X
SI-4(6)	*OGRANICZANIE NIEUPRZYWILEJOWANYCH UŻYTKOWNIKÓW*	*W: włączone do AC-6(10).*			
SI-4(7)	AUTOMATYCZNA ODPOWIEDŹ NA PODEJRZANE ZDARZENIA				
SI-4(8)	*OCHRONA INFORMACJI MONITORUJĄCYCH*	*W: włączone do SI-4.*			
SI-4(9)	TESTOWANIE NARZĘDZI I MECHANIZMÓW MONITORUJĄCYCH				
SI-4(10)	INSPEKCJA ZASZYFROWANYCH KOMUNIKATÓW				X
SI-4(11)	ANALIZA ANOMALII RUCHU TELEKOMUNIKACYJNEGO				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SI-4(12)	AUTOMATYCZNE ALERTY GENEROWANE PRZEZ ORGANIZACJĘ				X
SI-4(13)	ANALIZA MODELU RUCHU / ZDARZEŃ TELEKOMUNIKACYJNYCH				
SI-4(14)	WYKRYWANIE ATAKÓW BEZPRZEWODOWYCH				X
SI-4(15)	TELEKOMUNIKACJA BEZPRZEWODOWA / PRZEWODOWA				
SI-4(16)	KORELOWANIE INFORMACJI MONITORUJĄCYCH				
SI-4(17)	ZINTEGROWANA ŚWIADOMOŚĆ SYTUACYJNA				
SI-4(18)	ANALIZA RUCHU / ZAPOBIEGANIE EKSFILTRACJI				
SI-4(19)	RYZYKO ZE STRONY OSÓB				
SI-4(20)	UPRZYWILEJOWANI UŻYTKOWNICY				X
SI-4(21)	OKRESY PRÓBNE				
SI-4(22)	NIEAUTORYZOWANE USŁUGI SIECIOWE				X
SI-4(23)	KOMPUTER GŁÓWNY (HOST)				
SI-4(24)	WSKAŹNIKI RYZYKA				
SI-4(25)	ANALIZY OPTYMALIZACJI RUCHU SIECIOWEGO				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SI-5	**ALERTY BEZPIECZEŃSTWA, PORADY I DYREKTYWY**		X	X	X
SI-5(1)	AUTOMATYCZNE ALERTY I PORADY				X
SI-6	**WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI**				X
SI-6(1)	*POWIADOMIENIE O NIEUDANYCH TESTACH BEZPIECZEŃSTWA*	*W: włączone do SI-6.*			
SI-6(2)	WSPARCIE AUTOMATYZACYJNE BADAŃ ROZPROSZONYCH				
SI-6(3)	RAPORT Z WYNIKÓW WERYFIKACJI				
SI-7	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI**			X	X
SI-7(1)	KONTROLE INTEGRALNOŚCI			X	X
SI-7(2)	AUTOMATYCZNE POWIADOMIENIA O NARUSZENIACH INTEGRALNOŚCI				X
SI-7(3)	NARZĘDZIA DO CENTRALNEGO ZARZĄDZANIA INTEGRALNOŚCIĄ				
SI-7(4)	*OCHRONA PRZED NARUSZENIAMI*	W: włączone do SR-9.			

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SI-7(5)	AUTOMATYCZNA ODPOWIEDŹ NA NARUSZENIA INTEGRALNOŚCI				X
SI-7(6)	OCHRONA KRYPTOGRAFICZNA				
SI-7(7)	INTEGRACJA WYKRYWANIA I ODPOWIEDZI			X	X
SI-7(8)	ZDOLNOŚĆ AUDYTU ISTOTNYCH ZDARZEŃ				
SI-7(9)	WERYFIKACJA PROCESU URUCHAMIANIA				
SI-7(10)	OCHRONA URUCHAMIANIA OPROGRAMOWANIA UKŁADOWEGO				
SI-7(11)	*ZAMKNIĘTE ŚRODOWISKO Z OGRANICZONYMI UPRAWNIENIAMI*	*W: włączone do CM-7(6).*			
SI-7(12)	WERYFIKACJA INTEGRALNOŚCI				
SI-7(13)	*WYKONANIE KODU W ŚRODOWISKACH CHRONIONYCH*	*W: włączone do CM-7(7).*			
SI-7(14)	*KOD WYKONYWALNY BINARNY LUB MASZYNOWY*	*W: włączone do CM-7(8).*			
SI-7(15)	AUTORYZACJA KODU				X
SI-7(16)	LIMIT CZASU NA WYKONANIE PROCESU BEZ NADZORU				
SI-7(17)	SAMOOCHRONA APLIKACJI ŚRODOWISKA WYKONAWCZEGO				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SI-8	**OCHRONA PRZED SPAMEM**			X	X
SI-8(1)	*ZARZĄDZANIE CENTRALNE*	*W: włączone do PL-9.*			
SI-8(2)	AUTOMATYCZNE AKTUALIZACJE			X	X
SI-8(3)	CIĄGŁA ZDOLNOŚĆ DO NAUKI				
SI-9	*OGRANICZENIA WPROWADZANIA INFORMACJI*	*W: włączone do AC-2, AC-3, AC-5, AC-6.*			
SI-10	**WERYFIKACJA WPROWADZANYCH INFORMACJI**			X	X
SI-10(1)	RĘCZNE ZASTĘPOWANIE				
SI-10(2)	PRZEGLĄD / USUWANIE BŁĘDÓW				
SI-10(3)	PRZEWIDYWALNE ZACHOWANIE				
SI-10(4)	INTERAKCJE CZASOWE				
SI-10(5)	OGRANICZANIE DANYCH WEJŚCIOWYCH DO ZAUFANYCH ŹRÓDEŁ I ZATWIERDZONYCH FORMATÓW				
SI-10(6)	ZAPOBIEGANIE WSTRZYKIWANIU NIEZAUFANYCH DANYCH				
SI-11	**OBSŁUGA BŁĘDÓW**			X	X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SI-12	**ZARZĄDZANIE I RETENCJA DANYCH**	X	X	X	X
SI-12(1)	OGRANICZANIE ELEMENTÓW DANYCH OSOBOWYCH	X			
SI-12(2)	MINIMALIZOWANIE WYKORZYSTYWANIA DANYCH OSOBOWYCH PODCZAS TESTÓW, SZKOLEŃ I BADAŃ	X			
SI-12(3)	USUWANIE INFORMACJI	X			
SI-13	**PRZEWIDYWANIE AWARII**				
SI-13(1)	PRZENIESIENIE ODPOWIEDZIALNOŚCI KOMPONENTÓW				
SI-13(2)	*LIMIT CZASU NA WYKONANIE PROCESU BEZ NADZORU*	*W: włączone do SI-7(16).*			
SI-13(3)	RĘCZNY TRANSFER MIĘDZY SKŁADNIKAMI				
SI-13(4)	INSTALACJA KOMPONENTÓW Z LISTY REZERWOWEJ / POWIADOMIENIE				
SI-13(5)	PRZEŁĄCZANIE AWARYJNE				
SI-14	**ZAPOBIEGANIE ZAAWANSOWANYM DŁUGOTRWAŁYM ATAKOM TYPU APT)**				
SI-14(1)	ODŚWIEŻANIE Z ZAUFANYCH ŹRÓDEŁ				
SI-14(2)	ZMIENNOŚĆ INFORMACJI				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SI-14(3)	ZMIENNOŚĆ POŁĄCZEŃ				
SI-15	**FILTROWANIE INFORMACJI WYJŚCIOWYCH**				
SI-16	**OCHRONA PAMIĘCI**			X	X
SI-17	**PROCEDURY TESTOWANIA AWARYJNEGO „FAIL-SAFE”**				
SI-18	**OPERACJE SPRAWDZAJĄCE JAKOŚĆ DANYCH OSOBOWYCH**	X			
SI-18(1)	AUTOMATYZACJA WSPARCIA				
SI-18(2)	ZNACZNIKI DANYCH				
SI-18(3)	ZBIERANIE DANYCH				
SI-18(4)	ZGŁOSZENIA USUNIĘCIA DANYCH	X			
SI-18(5)	ZAWIADOMIENIE O KOREKCIE LUB USUNIĘCIU				
SI-19	**DE-IDENTYFIKACJA**	X			
SI-19(1)	ZBIERANIE DANYCH				
SI-19(2)	ARCHIWIZACJA DANYCH				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SI-19(3)	UJAWNIANIE DANYCH				
SI-19(4)	USUWANIE, MASKOWANIE, SZYFROWANIE, HASZOWANIE LUB WYMIANA IDENTYFIKATORÓW BEZPOŚREDNICH				
SI-19(5)	ZABEZPIECZENIE UJAWNIANIA DANYCH STATYSTYCZNYCH				
SI-19(6)	ZRÓŻNICOWANA PRYWATNOŚĆ				
SI-19(7)	ZATWIERDZONE ALGORYTMY I OPROGRAMOWANIE				
SI-19(8)	ZMOTYWOWANY INTRUZ				
SI-20	**SKAŻENIE**				
SI-21	**ODŚWIEŻANIE INFORMACJI**				
SI-22	**RÓŻNICOWANIE INFORMACJI**				
SI-23	**FRAGMENTACJA INFORMACJI**				

3.20. KATEGORIA SR - ZARZĄDZANIE RYZYKIEM W ŁAŃCUCHU DOSTAW

Tabela 3-20 zawiera podsumowanie zabezpieczeń podstawowych i zabezpieczeń rozszerzonych przypisanych do *Kategorii SR – Zarządzanie ryzykiem w łańcuchu dostaw*. Zabezpieczenia są przypisane do bazowych zabezpieczeń prywatności oraz do bazowych środków bezpieczeństwa o niskim, umiarkowanym i wysokim poziomie wpływu, w zależności od potrzeb. Zabezpieczenie podstawowe lub zabezpieczenie rozszerzone, które zostało wycofane z katalogu zabezpieczeń lub przeniesione do innej kategorii zabezpieczeń, jest oznaczone symbolem "W" z objaśnieniem dokonanym czcionką kursywa w jasnoszarym kolorze, z podaniem miejsca umieszczenia wycofanego / przeniesionego zabezpieczenia podstawowego lub zabezpieczenia rozszerzonego.

TABELA 3-20: KATEGORIA SR - ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SR-1	**POLITYKA I PROCEDURY**		X	X	X
SR-2	**PLAN ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW**		X	X	X
SR-2(1)	POWOŁANIE ZESPOŁU ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW		X	X	X
SR-3	**ZABEZPIECZENIA I PROCESY W ŁAŃCUCHU DOSTAW**		X	X	X

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SR-3(1)	ZRÓŻNICOWANA BAZA DOSTAW				
SR-3(2)	OGRANICZANIE SZKODY				
SR-3(3)	PODWYKONAWCY				
SR-4	**POCHODZENIE**				
SR-4(1)	TOŻSAMOŚĆ				
SR-4(2)	ŚLEDZENIE PRZESYŁEK				
SR-4(3)	POTWIERDZANIE AUTENTYCZNOŚCI I NIEZMIENNOŚCI				
SR-4(4)	INTEGRALNOŚĆ ŁAŃCUCHA DOSTAW - POCHODZENIE				
SR-5	**STRATEGIE, NARZĘDZIA I METODY NABYCIA**		X	X	X
SR-5(1)	ODPOWIEDNIE ZAOPATRZENIE				
SR-5(2)	OCENY PRZED WYBOREM, AKCEPTACJĄ, MODYFIKACJĄ LUB AKTUALIZACJĄ				
SR-6	**OCENY I RECENZJE DOSTAWCÓW**			X	X
SR-6(1)	BADANIA I ANALIZA				

NUMER ZABEZPIECZENIA	NAZWA ZABEZPIECZENIA PODSTAWOWEGO NAZWA ZABEZPIECZENIA ROZSZERZONEGO	ZABEZPIECZENIA BAZOWE PRYWATNOŚCI	BAZOWE ŚRODKI BEZPIECZEŃSTWA		
			NISKI	UMIARKOWANY	WYSOKI
SR-7	**BEZPIECZEŃSTWO OPERACJI W RAMACH ŁAŃCUCHA DOSTAW**				
SR-8	**UMOWY DOTYCZĄCE POWIADOMIEŃ**		X	X	X
SR-9	**ODPORNOŚĆ NA MANIPULACJE I WYKRYWANIE SABOTAŻU**				X
SR-9(1)	WIELOETAPOWY CYKL ŻYCIA SYSTEMU				X
SR-10	**KONTROLA SYSTEMÓW / KOMPONENTÓW**		X	X	X
SR-11	**AUTENTYCZNOŚĆ KOMPONENTU**		X	X	X
SR-11(1)	SZKOLENIE Z ZAKRESU ZAPOBIEGANIA FAŁSZERSTWOM		X	X	X
SR-11(2)	ZABEZPIECZENIE KONFIGURACJI SERWISOWANYCH I NAPRAWIANYCH KOMPONENTÓW		X	X	X
SR-11(3)	SKANOWANIE ANTYFAŁSZERSKIE				
SR-12	**USUWANIE KOMPONENTÓW**		X	X	X

REFERENCJE

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA	
NSC 199	Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199
NSC 200	Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych – na podstawie FIPS 200
NSC 500-92	Architektura referencyjna chmury obliczeniowej – rekomendacje – na podstawie NIST SP 500-292
NSC 800-18	Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych – na podstawie NIST SP 800- 18
NSC 800-30	Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne – na podstawie NIST SP 800-30
NSC 800-34	Poradnik planowania awaryjnego – na podstawie NIST SP 800-34
NSC 800-37	Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu – na podstawie NIST SP 800-37
NSC 800-53	Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji – na podstawie NIST SP 800-53
NSC 800-53A	Ocena środków bezpieczeństwa i ochrony prywatności systemów informatycznych oraz organizacji. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A
NSC 800-53B	Zabezpieczenia bazowe systemów informatycznych oraz organizacji – na podstawie NIST SP 800-53B
NSC 800-60	Wytyczne w zakresie określania kategorii bezpieczeństwa informacji I kategorii bezpieczeństwa systemu informatycznego – na podstawie NIST SP 800-60
NSC 800-61	Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego – na podstawie NIST SP 800-61

NSC 800-210	Ogólne wytyczne dotyczące kontroli dostępu do systemów chmury obliczeniowej – na podstawie NIST SP 800-210

LAWS, POLICIES, INSTRUCTIONS, STANDARDS, GUIDELINES, AND INTERNAL REPORTS

LAWS	
[FISMA]	Federal Information Security Modernization Act (P.L. 113-283), December 2014. https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[FOIA96]	Freedom of Information Act (FOIA), 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996. https://www.govinfo.gov/content/pkg/PLAW-104publ231/pdf/PLAW-104publ231.pdf
[PRIVACT]	Privacy Act (P.L. 93-579), December 1974. https://www.govinfo.gov/content/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf
[44 USC 3552]	Title 44 U.S. Code, Sec. 3552, Definitions. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapII-sec3552
POLICIES AND INSTRUCTIONS	
[CNSSI 1253]	Committee on National Security Systems Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*, March 2014. https://www.cnss.gov/CNSS/issuances/Instructions.cfm
[CNSSP 22]	Committee on National Security Systems Policy No. 22, *Cybersecurity Risk Management Policy*, August 2016. https://www.cnss.gov/CNSS/issuances/Policies.cfm
[DODI 8510.01]	Department of Defense Instruction 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, March 2014. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf?ver=2019-02-26-101520-300

[OMB A-130]	Office of Management and Budget Memorandum Circular A-130, *Managing Information as a Strategic Resource*, July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf
STANDARDS, GUIDELINES, AND INTERNAL REPORTS	
[FIPS 199]	National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199
[FIPS 200]	National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 200. https://doi.org/10.6028/NIST.FIPS.200
[SP 800-18]	Swanson MA, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-18, Rev. 1. https://doi.org/10.6028/NIST.SP.800-18r1
[SP 800-30]	Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1
[SP 800-37]	Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2
[SP 800-39]	Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[SP 800-53]	Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53r5
[SP 800-59]	Barker W (2003) Guideline for Identifying an Information System as a National Security System. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-59. https://doi.org/10.6028/NIST.SP.800-59
[SP 800-60-1]	Stine KM, Kissel RL, Barker WC, Fahlsing J, Gulick J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 1, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v1r1
[SP 800-60-2]	Stine KM, Kissel RL, Barker WC, Lee A, Fahlsing J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v2r1
[SP 800-82]	Stouffer K, Lightman S, Pillitteri V, Abrams M, Hahn, A (2015) Guide to Industrial Control System (ICS) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-82, Rev. 2. https://doi.org/10.6028/NIST.SP.800-82r2
[IR 8011 v1]	Dempsey KL, Eavy P, Moore G (2017) Automation Support for Security Control Assessments: Volume 1: Overview. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal (NISTIR) 8011, Volume 1. https://doi.org/10.6028/NIST.IR.8011-1
[IR 8062]	Brooks S, Garcia M, Lefkovitz N, Lightman S, Nadeau E (2017) An Introduction to Privacy Engineering and Risk Management in Federal Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (NISTIR) 8062. https://doi.org/10.6028/NIST.IR.8062

MISCELLANEOUS PUBLICATIONS AND WEBSITES	
[DSB 2017]	Department of Defense, Defense Science Board (2017) *Task Force on Cyber Deterrence* (Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington, DC). https://apps.dtic.mil/dtic/tr/fulltext/u2/1028516.pdf
[NIST CSRC]	National Institute of Standards and Technology (2020) *Computer Security Resource Center (CSRC)*. https://csrc.nist.gov
[SCOR]	National Institute of Standards and Technology (2020) *Security Control Overlay Repository (SCOR)*. https://csrc.nist.gov/projects/risk-management/scor

SŁOWNIK

PATRZ: NSC 7298, SŁOWNIK KLUCZOWYCH POJĘĆ Z ZAKRESU CYBERBEZPIECZEŃSTWA

AKRONIMY

PATRZ: NSC 7298, SŁOWNIK KLUCZOWYCH POJĘĆ Z ZAKRESU CYBERBEZPIECZEŃSTWA

NAKŁADKI

DODATKOWE SPERSONALIZOWANE OPCJE ZABEZPIECZEŃ BAZOWYCH

W niektórych sytuacjach korzystne dla organizacji może okazać się zastosowanie wskazówek dotyczących dostosowywania zestawów zabezpieczeń do potrzeb konkretnych grup odbiorców (organizacji) lub w celu uwzględnienie specjalistycznych wymagań, wdrożonych technologii, specyficznych misji lub środowisk działania. Organizacja może podjąć decyzję o ustanowieniu zestawu zabezpieczeń dla konkretnych zastosowań lub przypadków użycia, takich jak usługi w chmurze, które mogłyby być stosowane przez organizacje zamawiające lub wdrażające takie usługi; systemy zabezpieczeń przemysłowych wytwarzające lub przekazujące energię elektryczną lub kontrolujące systemy środowiskowe w obiektach; systemy przetwarzania, przechowywania lub przekazywania informacji niejawnych; lub systemy kontrolujące bezpieczeństwo systemów transportowych. W tych przykładach nakładki mogą być tworzone dla każdego sektora, obszaru technologicznego, specyficznej sytuacji, lub środowiska naturalnego i rozpowszechniane wśród dużych grup interesu – w celu osiągnięcia standardowych możliwości w zakresie bezpieczeństwa i ochrony prywatności, konsekwentnego wdrażania zabezpieczeń oraz opłacalnych kosztowo rozwiązań w zakresie bezpieczeństwa i ochrony prywatności.

W celu zaspokojenia zapotrzebowania na specjalistyczne zestawy zabezpieczeń dla konkretnych grup odbiorców, systemów i organizacji, wprowadza się koncepcję *nakładek. Nakładka* może być w pełni określonym zestawem zabezpieczeń podstawowych, zabezpieczeń rozszerzonych i innych informacji pomocniczych (np. wartości parametrów), które wynikają z zastosowania wytycznych dotyczących dostosowania do zabezpieczeń bazowych[39,40] lub mogą być uzyskane niezależnie od zabezpieczeń bazowych.[41] Nakładki są

[39] Publikacja [NIST SP800-82] przedstawia przykład nakładki zawierającej pełną specyfikację zestawu zabezpieczeń przemysłowych systemów sterowania. Alternatywnie, nakładki mogą obejmować określony zestaw istotnych zabezpieczeń, które odnoszą się do konkretnej potrzeby danego odbiorcy i uzupełniają zabezpieczenia bazowe.

[40] Zabezpieczenia bazowe mogą obejmować: zabezpieczenia bazowe określone w rozdziale trzecim; zabezpieczenia bazowe opracowane przez organizacje sektora państwowego; lub zabezpieczenia bazowe opracowane przez organizacje sektora prywatnego (np. producentów, konsorcja, stowarzyszenia handlowe, przemysł i sektory infrastruktury krytycznej).

[41] Nakładki, które są niezależne od zabezpieczeń bazowych, często odnoszą się do bardzo specyficznych okoliczności (np. ochrona informacji niejawnych), sytuacji i/lub warunków.

opracowywane w celu zastosowania w różnorodnych systemach w ramach potrzeb danych grup społecznych, uzupełniając i udoskonalając zabezpieczenia bazowe poprzez:

- Umożliwienie zainteresowanej społeczności dodawanie, modyfikację lub usuwanie zabezpieczeń;
- Zapewnienie możliwości zastosowania zabezpieczeń i interpretacji konkretnych technologii, paradygmatów obliczeniowych, środowisk pracy, rodzajów systemów, rodzajów misji/operacji, trybów pracy, sektorów przemysłu oraz wymogów ustawowych/regulacyjnych;
- Ustalanie wartości parametrów dla operacji dostosowywania i wyboru zabezpieczeń podstawowych i zabezpieczeń rozszerzonych, które są zgodne z interesem danej grupy odbiorców (organizacji).

Organizacje stosują koncepcję nakładek, jeżeli istnieje rozbieżność z podstawowymi założeniami wykorzystywanymi do tworzenia zabezpieczeń bazowych lub gdy niezbędne są specyficzne zabezpieczenia w celu ochrony poszczególnych technologii lub przeciwdziałania konkretnemu zagrożeniu. Nakładki mogą wymagać dostosowania, jak opisano w rozdziale trzecim, w celu zapewnienia, że implementowane zabezpieczenia dokładnie odzwierciedlają wymagania w zakresie bezpieczeństwa i prywatności dla każdego systemu, komponentu systemu i środowiska operacyjnego, do którego nakładka jest stosowana. Koncepcja nakładek ma zastosowanie do grup podobnych technologii, systemów lub wspólnot interesów (tzn. koncepcja stosowania nakładek nie jest odpowiednia dla pojedynczego systemu, ponieważ proces dostosowywania jest wykorzystywany do dopasowania poziomów zabezpieczeń bazowych dla poszczególnych systemów).

Pełen zakres działań dostosowujących może być wykorzystywany przez organizacje w celu zapewnienia zorganizowanego podejścia do tworzenia nakładek wspierających opisane powyżej obszary. Nakładki zapewniają możliwość budowania konsensusu w zainteresowanych społecznościach oraz opracowywania planów bezpieczeństwa i ochrony prywatności systemów i organizacji, mających szerokie wsparcie dla konkretnych okoliczności, sytuacji lub warunków. Kategorie nakładek, które mogą być użyte czne obejmują:

- Wspólnoty interesów, sektory przemysłu, koalicje lub stowarzyszenia, takie jak opieka zdrowotna, organy ścigania, działalność informacyjna, finanse, produkcja, transport, energia, a także współpraca lub współużytkowanie;
- Technologie informacyjne i paradygmaty obliczeniowe, takie jak systemy zwirtualizowane, chmury obliczeniowe, urządzenia mobilne, inteligentne sieci energetyczne i rozwiązania międzydomenowe;
- Środowiska działania, takie jak operacje powietrzne, taktyczne lub morskie;
- Rodzaje systemów i trybów działania, takie jak przemysłowe lub procesowe systemy sterowania, systemy uzbrojenia, systemy jednoużytkownikowe, systemy autonomiczne oraz urządzenia i czujniki Internetu rzeczy (*ang. Internet of things - IoT*;
- Rodzaje misji lub operacji, takie jak antyterroryzm, pierwszy kontakt, badania, rozwój, testowanie i ocena;
- Rodzaje zagrożeń, takie jak zaawansowane trwałe zagrożenia (zagrożenia typu APT – *ang. advanced persistent threats*) lub zagrożenia wewnętrzne;
- Wymogi ustawowe lub wykonawcze.

Nakładki zapewniają jednolitość i skuteczność dobieranych zabezpieczeń, prezentując właścicielom systemów odpowiedzialnym za wdrażanie i utrzymanie systemów opcje dostosowywania opracowane przez ekspertów ds. bezpieczeństwa i ochrony prywatności oraz innych ekspertów merytorycznych. Istnieje wiele opcji, które mogą być wykorzystane do budowy nakładek, w zależności od specyfiki pożądanej przez twórców nakładek. Niektóre nakładki mogą być bardzo specyficzne w odniesieniu do sprzętu, oprogramowania układowego i aplikacji programowych, które tworzą kluczowe komponenty docelowych typów systemów i środowisk, w których systemy te działają. Inne nakładki mogą być bardziej abstrakcyjne, aby można je było zastosować do większej klasy systemów, które mogą być wdrażane w różnych środowiskach operacyjnych.

PUBLIKACJA NAKŁADEK

Nakładki mogą być publikowane niezależnie w różnych miejscach i publikacjach, w tym w standardach cyberbezpieczeństwa, standardach i poradnikach branżowych.

Repozytorium Nakładek Środków Bezpieczeństwa (*ang. Security Control Overlay Repository - SCOR*) zapewnia zainteresowanym stronom platformę do dobrowolnego udostępniania nakładek środków bezpieczeństwa. Celem uzyskania więcej informacji o repozytorium, w tym zapoznaniu się z instrukcjami dotyczącymi przedstawiania nakładek oraz listą opublikowanych nakładek, zobacz rozdział Referencje, pozycja [SCOR].

Organizacje mogą korzystać z poniższego konspektu przy tworzeniu nakładek.[42] Konspekt ten jest podany tylko jako przykład. Organizacje mogą korzystać z dowolnego formatu w oparciu o konkretne potrzeby organizacyjne i rodzaj opracowywanej nakładki. Poziom szczegółowości nakładki zależy od decyzji organizacji lub wspólnoty interesów inicjującej nakładkę, ale powinien być wystarczająco szeroki i dogłębny, aby zapewnić odpowiednie uzasadnienie i przesłanki dla nakładki, w tym wszelkie decyzje oparte na ryzyku podjęte podczas procesu opracowywania nakładki. Przykładowy konspekt nakładki obejmuje następujące pozycje:

- Identyfikacja,
- Charakterystyka nakładki,
- Zastosowanie,
- Podsumowanie,

[42] Jakkolwiek zachęca się organizacje do stosowania koncepcji nakładek, to jednak opracowanie znacznie różniących się od siebie nakładek na ten sam temat może przynieść efekt przeciwny do zamierzonego. Koncepcja nakładek jest najbardziej efektywna, gdy zainteresowane społeczności współpracują ze sobą w celu stworzenia nakładek opartych na konsensusie, które nie powielają się.

- Specyfikacje zabezpieczeń nakładki,
- Aspekty dostosowania,
- Terminy i definicje,
- Dodatkowe informacje lub instrukcje.

Identyfikacja

Organizacje identyfikują nakładkę poprzez nadanie unikalnej nazwy, numeru wersji i daty, wersji standardu NSC 800-53 użytego do jej stworzenia, innej dokumentacji wykorzystanej do stworzenia nakładki, autora lub grupy autorów i punktu kontaktowego oraz rodzaju otrzymanej aprobaty organizacyjnej. Organizacje określają czas obowiązywania nakładki oraz wszelkie zdarzenia, które mogą spowodować aktualizację nakładki, inne niż zmiany w dokumencie NSC 800-53 lub wytyczne dotyczące danej organizacji. Jeśli nie wystąpią unikalne zdarzenia, które mogą wywołać aktualizację nakładki, w sekcji Identyfikacja zawiera się odpowiednią adnotację.

Charakterystyka nakładki

Organizacje opisują cechy, które określają przeznaczenie nakładki, aby pomóc potencjalnym użytkownikom wybrać najbardziej stosowną nakładkę odpowiednią dla ich misji lub funkcji biznesowych, w tym:

- Opis środowiska fizycznego, w którym systemy, komponenty systemu lub technologie, których dotyczy nakładka, będą użytkowane lub będą działały (np. w chronionym obiekcie w kraju, w bezzałogowym pojeździe kosmicznym, podczas służbowej podróży zagranicznej do państwa, które jest znane z prób uzyskania dostępu do informacji szczególnie chronionych lub niejawnych, lub w pojeździe mobilnym, który znajduje się w bliskiej odległości od nieprzyjaznych podmiotów);
- Typ(-y) informacji, które będą przetwarzane, przechowywane lub przekazywane przez systemy, komponenty systemu lub technologie, których dotyczy nakładka (np. informacje dotyczące tożsamości i uwierzytelniania; informacje dotyczące zarządzania finansami; obiekty, flota, oraz informacje dotyczące zarządzania sprzętem; informacje w zakresie obronności i bezpieczeństwa narodowego; informacje dotyczące rozwoju systemu);

- Funkcjonalność w ramach docelowych systemów, komponentów systemu, technologii lub rodzajów systemów (np. systemy autonomiczne, przemysłowe lub sterowania procesem, lub systemy międzydomenowe)
- Inne cechy związane z nakładką, które mają chronić funkcje organizacyjne lub biznesowe, systemy, informacje lub osoby przed określonym zestawem zagrożeń, które mogą nie być uwzględnione w założeniach opisanych w pkt 2.3.

Zastosowanie

Organizacje zapewniają kryteria pomagające użytkownikom nakładki w określeniu, czy nakładka dotyczy konkretnego systemu, komponentu systemu, technologii lub środowiska pracy. Typowe formaty mogą obejmować listę pytań lub drzewo decyzyjne oparte na opisie cech charakterystycznych docelowej nakładki (w tym powiązanych z nią aplikacji) i jej środowiska działania, na poziomie szczegółowości właściwym dla danej nakładki.

Podsumowanie

Organizacje przedstawiają krótkie podsumowanie charakterystyki nakładki. Podsumowanie może wskazywać zabezpieczenia podstawowe i zabezpieczenia rozszerzone, na które nakładka ma wpływ; wskazanie (na podstawie szczególnych cech i założeń zawartych w nakładce, wytycznych dotyczących dostosowania do potrzeb klienta przedstawionych w sekcji 2.4 lub wszelkich wytycznych dotyczących konkretnej organizacji) do których zabezpieczeń podstawowych i zabezpieczeń rozszerzonych dana nakładka się odnosi; wybrane zabezpieczenia podstawowe i zabezpieczenia rozszerzone, w tym wartości parametrów; oraz odniesienia do obowiązujących przepisów, rozporządzeń, dyrektyw, instrukcji, zaleceń, polityk lub standardów.

Specyfikacje zabezpieczeń nakładki

Organizacje zapewniają kompleksowe omówienie zabezpieczeń podstawowych i zabezpieczeń rozszerzonych w ramach procesu dostosowywania. Może to obejmować uzasadnienie wyboru lub odrzucenia konkretnego elementu zabezpieczeń podstawowych i zabezpieczeń rozszerzonych; modyfikacje w części *Omówienie* dotyczącej zabezpieczeń, które odnoszą się do właściwości nakładki i środowiska, w którym nakładka ma być stosowana; jednoznaczne wartości parametrów w zakresie wyboru lub przypisania

zabezpieczeń; szczególne wymogi ustawowe lub regulacyjne, które są spełnione przez element zabezpieczenia podstawowego i zabezpieczenia rozszerzonego; zalecenia dotyczące zabezpieczeń kompensacyjnych (w stosownych przypadkach); oraz wytyczne rozszerzające możliwości zabezpieczeń podstawowych i zabezpieczeń rozszerzonych o dodatkowe funkcje, zmianę siły mechanizmu lub dodanie lub ograniczenie opcji wdrożenia.

Aspekty dostosowania

Organizacje dostarczają właścicielom systemów i osobom autoryzującym informacje do uwzględnienia w procesie dostosowywania zestawu zabezpieczeń podstawowych i zabezpieczeń rozszerzonych, mających zastosowanie do ich konkretnych systemów, komponentów systemu lub technologii. Jest to szczególnie ważne w przypadku, gdy są one stosowane w środowisku pracy innym niż to, które zostało przyjęte w rozdziale trzecim. Ponadto organizacje mogą dostarczyć wytyczne dotyczące stosowania wielu nakładek w odniesieniu do zabezpieczeń bazowych oraz odnieść się do wszelkich potencjalnych konfliktów, które mogą powstać pomiędzy zabezpieczeniami bazowymi i nakładkami.

Terminy i definicje

Organizacje podają wszelkie terminy i związane z nimi definicje, które są unikalne i istotne dla nakładki. Jeśli nie ma specyficznych terminów lub definicji dla nakładki, należy to opisać w tej sekcji.

Dodatkowe informacje lub instrukcje

Organizacje udzielają wszelkich dodatkowych informacji lub instrukcji związanych z nakładką, które nie zostały omówione w poprzednich sekcjach.