NSC NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA	Narodowy Standard Cyberbezpieczeństwa		
Nazwa standardu	Symbol	Wersja	Data wydania
Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego	**NSC 800-60 Część I**	1.0	01/09/2021

Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego

Część I

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]

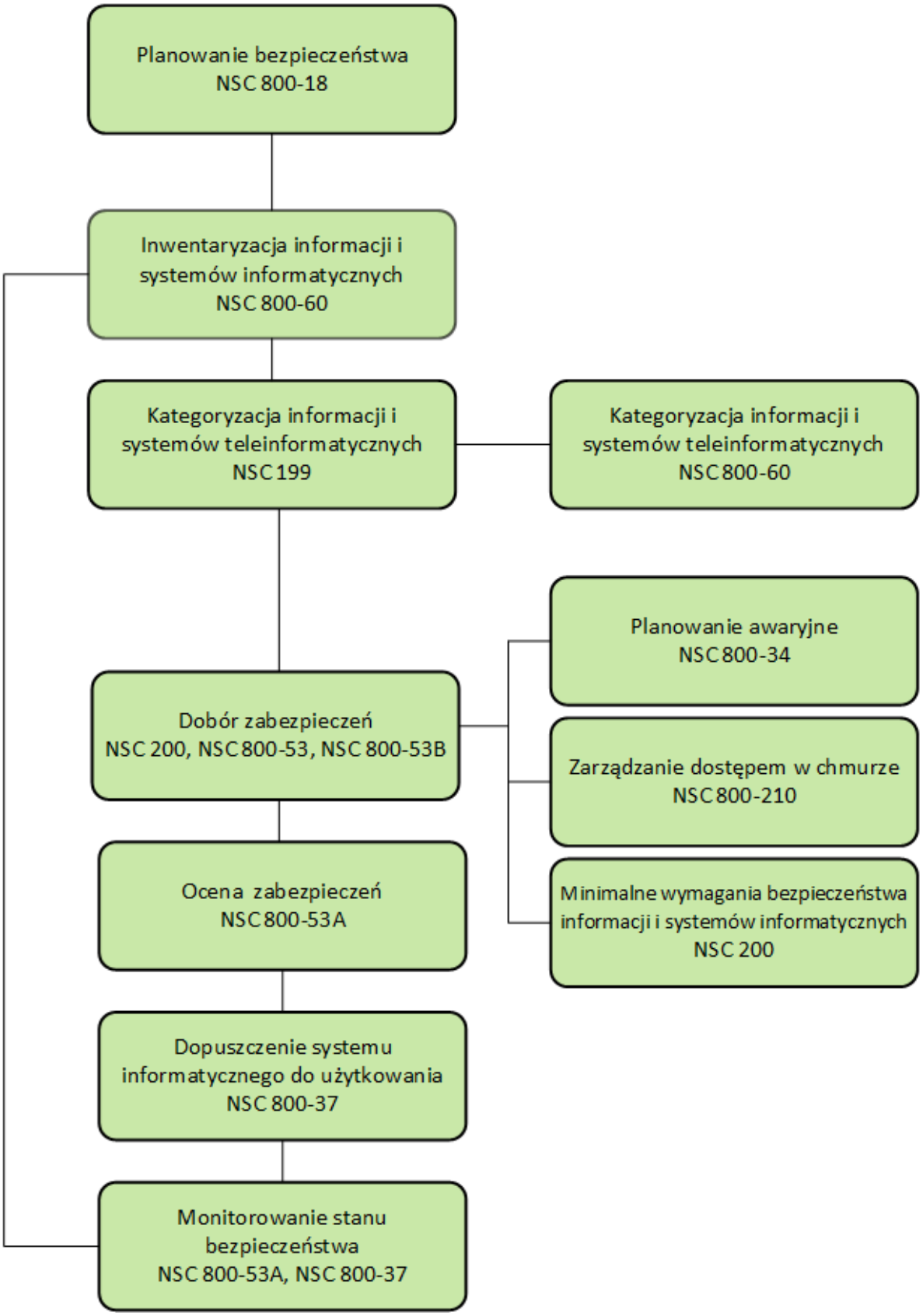
- NSC[2] 199, Standardy *kategoryzacji bezpieczeństwa* – na podstawie FIPS 199;
- NSC 200, *Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych* – na podstawie FIPS 200;
- NSC 500-92, *Architektura referencyjna chmury obliczeniowej – rekomendacje* – na podstawie 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 informatyczn*ego – 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 informacyjnych, ocenę tych zabezpieczeń, wzajemną akceptację dowodów oceny bezpieczeństwa i ochrony prywatności oraz decyzji autoryzacyjnych, a także dzięki jednolitemu podejściu, ułatwia wymianę informacji i współpracę pomiędzy różnymi podmiotami.

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

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

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

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

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

Niniejsza publikacja, ***Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego,*** opracowana została za zgodą National Institute of Science and Technology (NIST) na podstawie specjalnej publikacji NIST SP 800-60 vol. 1, Rev. 1.

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

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

SPIS TREŚCI

PODSUMOWANIE ZARZĄDCZE

Niniejsze wytyczne stanowią przewodnik metodyczny pozwalający na określenie poziomu wpływu potencjalnego incydentu na bezpieczeństwo informacji oraz na dostępność systemu informatycznego, w którym te informacje są przetwarzane.

Wytyczne mają na celu ułatwienie przypisania odpowiedniego poziomu bezpieczeństwa informacji zgodnie z poziomami wpływu zakłóceń / incydentów, które mogą wynikać z nieuprawnionego ujawnienia, modyfikacji lub wykorzystania systemu informatycznego lub informacji. Wytyczne te zakładają, że użytkownik zapoznał się ze standardami kategoryzacji bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych (Narodowy Standard Cyberbezpieczeństwa - NSC 199).

Zawarte w dokumencie kategorie informacji, jakkolwiek mające swoje źródło w systemach informacyjnych administracji federalnej USA, nadają się do zastosowania w polskiej administracji rządowej, a znacznym stopniu w ogóle w podmiotach realizujących zadania publiczne.

W celu dokonania kategoryzacji systemów informatycznych i informacji przetwarzanych w tych systemach, należy:

- Zapoznać się z terminami i definicjami kategoryzacji bezpieczeństwa zawartymi w NSC 199;
- Ustanowić proces kategoryzacji bezpieczeństwa;
- Do identyfikacji rodzajów informacji i systemów informacyjnych wykorzystać kategorie zawarte w niniejszej publikacji lub w miarę potrzeb dodać nowe, unikając jednak nadmiernemu rozdrobnieniu rodzajów informacji;
- Korzystając z niniejszej publikacji wyznaczyć **wstępne** poziomy wpływu zakłócenia / incydentu dla typowych rodzajów informacji przetwarzanych w poszczególnych działach administracji. Jest to **wstępna kategoryzacja**, która po przeprowadzeniu szacowania ryzyka, jeśli zachodzi taka potrzeba, **może podlegać modyfikacjom**;

- Dla konkretnego systemu teleinformatycznego rozpatrzeć poszczególne atrybuty bezpieczeństwa informacji, które mogą skutkować odchyleniami od wstępnego przypisania poziomu wpływu zakłócenia / incydentu na te atrybuty;
- Ustanowić sumaryczną kategorię systemu informatycznego, która będzie później wykorzystywana do ustanawiania zabezpieczeń zgodnie z publikacją NSC 800-53.

Niniejszy dokument ma służyć jako źródło informacji, a nie obligatoryjne wymaganie i nie wszystkie zawarte w nim materiały będą odpowiednie dla wszystkich podmiotów. Dokument ten obejmuje dwa tomy: Część I - Podstawowe wytyczne i Część II - Załączniki. Użytkownicy powinni zapoznać się z wytycznymi zawartymi w Części I, a następnie odwołać się tylko do tego konkretnego materiału z Części II (załączników), który dotyczy ich własnych systemów i aplikacji. Wstępne przypisania poziomu wpływu zakłócenia / incydentu podano w Części II, załącznik A i B.

1. WPROWADZENIE

Identyfikacja informacji przetwarzanych w systemie informatycznym jest niezbędna do właściwego wyboru zabezpieczeń w celu zapewnienia poufności, integralności oraz dostępności systemu i przetwarzanym w tym systemie informacjom. W celu udzielenia pomocy podmiotom publicznym w wypełnienia obowiązków nałożonych przepisami prawa w zakresie cyberbezpieczeństwa opracowano publikację NSC 800-60.

1.1. CEL I ZASTOSOWANIE

NSC 800-60 odnosi się do minimalnych wymagań w stosunku do systemów informatycznych mając na celu opracowania wytycznych zalecających ustanowienie kategorii wpływu zakłócenia / incydentu na poszczególne systemy informatyczne podmiotów publicznych. Wytyczne te mają pomóc podmiotom w konsekwentnym mapowaniu poziomów wpływu na bezpieczeństwo z uwzględnieniem rodzajów: (i) informacji (np. dane osobowe, medyczne, wrażliwe, finansowe, tajemnica przedsiębiorcy, postępowania w zakresie ścigania przestępstw); oraz (ii) systemów informatycznych (np. o znaczeniu krytycznym, wsparcia działalności podmiotu, administracji). Wytyczne te dotyczą wszystkich systemów podmiotów publicznych innych niż systemy przetwarzające informacje niejawne w rozumieniu ustawy o ochronie informacji niejawnych i systemy informatyczne Sił Zbrojnych RP.

1.2. GRUPA DOCELOWA

Niniejsza publikacja ma służyć różnorodnym odbiorcom spośród specjalistów ds. systemów informatycznych i bezpieczeństwa informacji podmiotów publicznych, w tym: (i) osobom odpowiedzialnym za zarządzanie i nadzór nad systemami informatycznymi (np. ang. *chief information oficer - CIO, ang. senior agency information oficer - SAISO*, osób autoryzujących (*ang. authorizing official - AO*) [3]; (ii) pracownikom organizacji mających szczególny interes w realizacji celu działania podmiotu (np. właściciele obszaru biznesowego, właściciele

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

informacji); (iii) osobom odpowiedzialnym za rozwój systemu informatycznego (np. kierownicy programów i projektów, twórcy systemów informatycznych); oraz (iv) osobom odpowiedzialnym za wdrażanie bezpieczeństwa informacji i działania operacyjne (np. właściciele systemów informatycznych, właściciele informacji; *information system security officer - ISSO*).[4]

1.3. POWIĄZANIA Z INNYMI STANDARDAMI

Publikacja NSC 800-60 jest członkiem rodziny publikacji związanych Narodowymi Standardami Cyberbezpieczeństwa NSC, w tym:

- NSC 199, *Standardy Kategoryzacji Bezpieczeństwa*;
- NSC 200, *Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych*;
- NSC 800-53, *Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji;*
- NSC 800-37, *Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu*.

Wymienione dokumenty mają na celu zapewnienie ustrukturyzowanych, ale elastycznych ram dla wybierania, określania, stosowania, oceny i monitorowania zabezpieczeń w systemach informatycznych podmiotów publicznych – a tym samym w znacznym stopniu przyczynia się do spełnienia przepisów prawa w stosunku do minimalnych wymagań dla systemów informatycznych tych podmiotów. Mimo, że publikacje te mają pewne zależności, w większości przypadków można je skutecznie wykorzystywać niezależnie od siebie.

Kategorie bezpieczeństwa informacji wskazane w NSC 800-60 i związane z nimi poziomy wpływu zakłócenia / incydentu na bezpieczeństwo oparte są na uogólnionych analizach dokonanych przez właścicieli systemów informatycznych w poszczególnych działach

[4] Uwaga: dotyczy całego dokumentu. Opisy stanowisk i ról oraz rozwinięcia angielskich akronimów – patrz NSC 800-37.

administracji rządowej. Znajdujący się w Załączniku D wstępny poziom wpływu zakłócenia / incydentu na atrybuty bezpieczeństwa informacji wymaga dostosowania z uwzględnieniem okoliczności właściwych dla konkretnego systemu informatycznego.

1.4. STRUKTURA PUBLIKACJI

Publikacja NSC 800-60 składa się z dwóch części. Część I zawiera podstawowe wytyczne dotyczące mapowania typów informacji i systemów informatycznych na kategorie bezpieczeństwa. Załączniki, w tym zalecenia dotyczące kategoryzacji bezpieczeństwa dla typów informacji związanych z celem działania danego podmiotu publicznego oraz uzasadnienie zaleceń dotyczących kategoryzacji bezpieczeństwa, są publikowane jako osobna Część II.

Część I zawiera następujące podstawowe informacje i wytyczne dotyczące mapowania:

- **Rozdział 2**: Zawiera przegląd procesu kategoryzacji systemów informatycznych i informacji, programów bezpieczeństwa i ogólnego zarządzania technologiami informatycznymi (IT) oraz roli publikacji w cyklu życia systemu, procesu certyfikacji i akredytacji oraz ram zarządzania ryzykiem NSC.
- **Rozdział 3**: Określa cele bezpieczeństwa i odpowiadające im poziomy wpływu zakłócenia / incydentu na bezpieczeństwo określone w Standardzie kategoryzacji bezpieczeństwa NSC 199;
- **Rozdział 4**: Identyfikuje proces, w tym wytyczne dotyczące identyfikacji rodzajów informacji przetwarzanych w związku z celem działania podmiotu oraz proces stosowany do wyboru poziomów wpływu zakłócenia /incydentu na bezpieczeństwo, ogólne uwagi dotyczące przypisania wpływu na bezpieczeństwo, wytyczne dotyczące kategoryzacji bezpieczeństwa systemu oraz uwagi i wytyczne dotyczące stosowania oraz powiązania wyników kategoryzacji systemów z misją podmiotu, infrastrukturą wspierającą i połączeniami z innymi systemami.

Część II zawiera:

- **Załącznik A**: Wstępne przypisanie poziomu wpływu zakłócenia / incydentu na bezpieczeństwo oraz uzasadnienie informacji zarządczych i pomocniczych (informacje administracyjne, zarządcze i serwisowe);
- **Załącznik B**: Wstępne przypisanie poziomu wpływu zakłócenia / incydentu na bezpieczeństwo oraz uzasadnienie informacji związanych z celem działania podmiotu (informacje o celu działania i mechanizmach świadczenia usług);

2. PRZEGLĄD PUBLIKACJI

Kategoryzacja bezpieczeństwa stanowi istotny krok w integracji bezpieczeństwa z funkcjami zarządzania celem działania i technologiami informatycznymi podmiotu publicznego oraz stanowi podstawę standaryzacji bezpieczeństwa wśród ich systemów informatycznych. Kategoryzacja bezpieczeństwa rozpoczyna się od ustalenia, jakie informacje są wykorzystywane w celu realizacji zadania publicznego. Kolejne kroki koncentrują się na ocenie potrzeby zapewnienia bezpieczeństwa informacji pod względem poufności, integralności i dostępności. Rezultatem jest silne powiązanie między celem działania, informacjami i systemami informatycznymi przy uzasadnionych kosztach wdrażania zabezpieczeń.

2.1. REALIZACJA PROCESU KATEGORYZACJI BEZPIECZEŃSTWA W PODMIOCIE PUBLICZNYM

Podmioty publiczne realizują proces kategoryzacji, ustanawiając typy informacji niezbędne do osiągnięcia celu działania podmiotu. Podejście do ustalania typów informacji w podmiocie rozpoczyna się od udokumentowania celu działania i obszarów biznesowych / zadań podmiotu. W przypadku informacji niezbędnych do realizacji zadań odpowiedzialne osoby, w koordynacji z zarządem, operatorem, architekturą korporacyjną i interesariuszami bezpieczeństwa, powinny kompleksowo zidentyfikować te zadania. Ponadto osoby odpowiedzialne powinny zidentyfikować odpowiednie podfunkcje niezbędne do realizacji zadań podmiotu. Na przykład w przypadku zadania jednego podmiotu, związanego z rozwojem gospodarczym, podfunkcje będące częścią tego zadania mogą obejmować rozwój przedsiębiorczości i przemysłu, ochronę własności intelektualnej lub nadzór sektora finansowego. Każda z tych podfunkcji reprezentuje określony typ informacji.

Podmioty publiczne powinny przeprowadzać kategoryzację bezpieczeństwa swoich systemów informatycznych według NSC 199, obejmując nią cały podmiot, przy udziale kierownictwa wyższego szczebla i innych kluczowych pracowników podmiotu (np. właścicieli misji/procesów biznesowych, osób autoryzujących, *RE*, *CIO, SAISO*, właścicieli systemów

informatycznych i właścicieli informacji), tak aby zapewnić, że każdy system informatyczny otrzymuje odpowiedni nadzór zarządzania i że odzwierciedlone zostały potrzeby organizacji, jako całości. Nadzór kierownictwa wyższego szczebla nad procesem kategoryzacji bezpieczeństwa jest niezbędny, aby kolejne kroki w ramach zarządzania ryzykiem (np. wybór zabezpieczeń) mogły zostać przeprowadzone w sposób skuteczny i spójny w całym podmiocie.

2.2. WARTOŚĆ DLA CELU DZIAŁANIA PODMIOTU, PROGRAMÓW BEZPIECZEŃSTWA I ZARZĄDZANIA IT

Osiągnięcie celu działania podmiotów publicznych jest w dużym stopniu zależne od informacji i systemów informatycznych. W związku z rosnącą złożoności systemów informatycznych, a także stale zmieniającemu się środowiskiem w zakresie ryzyka, niezbędną funkcją stało się zapewnienie bezpieczeństwa informacji. Zapewnienie bezpieczeństwa musi być wykonywane w sposób, który zmniejsza ryzyko dla informacji powierzonej podmiotowi, utraty zdolności do osiągnięcia celu działania oraz jej wsparcia w działalności gospodarczej i służenia obywatelom. Ostatecznie bezpieczeństwo informacji jako funkcja staje się czynnikiem umożliwiającym prowadzenie działalności poprzez staranne i skuteczne zarządzanie ryzykiem dotyczącym poufności, integralności i dostępności informacji.

Wyznaczenie wartość kategorii bezpieczeństwa informacji umożliwia podmiotom publicznym proaktywne wdrożenie odpowiednich zabezpieczeń informacji w oparciu o oszacowany potencjalny wpływ zakłócenia / incydentu na poufność, integralność i dostępność informacji, a tym samym na realizację zadań z uwzględnieniem optymalizacji wydatków na zabezpieczenia. Niepoprawna analiza wpływu zakłócenia / incydentu na system informacyjny (tj. nieprawidłowa kategoryzacja bezpieczeństwa wg NSC 199) może spowodować, że podmiot albo nadmiernie zabezpieczy system informatyczny, marnując w ten sposób środki finansowe i zasoby ludzkie, albo zabezpieczenia systemu informatycznego będą zbyt słabe i narażą na ryzyko utraty zdolności do realizacji zadań i straty materialne. Kumulacja takich błędów na poziomie całego podmiotu może dodatkowo spotęgować problem.

Przeprowadzając analizę wpływu zakłócenia / incydentu zgodnie z NSC, 199 jako działanie obejmujące cały podmiot z udziałem kluczowych pracowników (np. *CIO*, *SAISO*, osób autoryzujących, właścicieli systemów) na wielu poziomach może umożliwić podmiotowi wykorzystanie efektu skali poprzez skuteczne zarządzanie i wdrażanie zabezpieczeń na poziomie podmiotu. Z takiego podejścia do systematycznego realizowania procesu określania kategoryzacji bezpieczeństwa i stosowania odpowiednich zabezpieczeń jest lepsze ogólne zrozumienie celu działania podmiotu i zakresu odpowiedzialności poszczególnych pracowników.

Wskazówka dotycząca implementacji

Aby umożliwić odpowiedni poziom wsparcia celu działania oraz staranne wdrażanie obecnych i przyszłych wymagań w zakresie bezpieczeństwa informacji, każdy podmiot powinien ustanowić formalny proces sprawdzania kategoryzacji bezpieczeństwa na poziomie systemu pod względem priorytetów podmiotu. Pozwoli to nie tylko promować porównywalną ocenę systemów, ale także przyniesie dodatkowe korzyści, takie jak wykorzystanie zabezpieczeń wspólnych i ustanowienie szczegółowej ochrony.

2.3. ROLA W CYKLU ŻYCIA SYSTEMU

Wstępna kategoryzacja bezpieczeństwa powinna nastąpić na wczesnym etapie cyklu życia systemu (SDLC). Wynikająca z tego kategoria bezpieczeństwa posłuży do identyfikacji wymagań bezpieczeństwa (później przekształci się w zabezpieczenia) i innych działań powiązanych, takich jak analiza wpływu na bezpieczeństwo danych osobowych lub analiza w zakresie infrastruktury krytycznej. Ostatecznie zidentyfikowane wymagania bezpieczeństwa i wybrane mechanizmy zabezpieczeń są wprowadzane do standardowego procesu inżynierii systemów, aby skutecznie zintegrować zabezpieczenia z wymaganiami funkcjonalnymi i operacyjnymi systemów informatycznych, a także innymi istotnymi wymaganiami systemowymi (np. niezawodność, łatwość konserwacji, wsparcie).

2.4. ROLA W PROCESIE CERTYFIKACJI I AKREDYTACJI

Kategoryzacja bezpieczeństwa stanowi podstawę działalności w zakresie certyfikacji i akredytacji (C&A) poprzez określenie poziomu rygoryzmu wymaganego do certyfikacji i ogólnego testowania zabezpieczeń, a także dodatkowych działań, które mogą być potrzebne (tj. ochrony danych osobowych i infrastruktury krytycznej). Pomaga zatem w określeniu poziomu wysiłku C&A i związanego z nim czasu na te działania.

Kategoryzacja bezpieczeństwa jest warunkiem wstępnym procesu C&A. Kategoryzacja powinna być weryfikowana, co najmniej, co trzy lata lub w przypadku znaczącej zmiany w systemie lub otoczeniu biznesowym. Zmiany sytuacji poza systemem lub podmiotem mogą wymagać ponownej oceny kategoryzacji (tj. zmiany w zadaniach, zmiany w zarządzaniu, zmiany związane z pojawieniem się nowych zagrożeń).

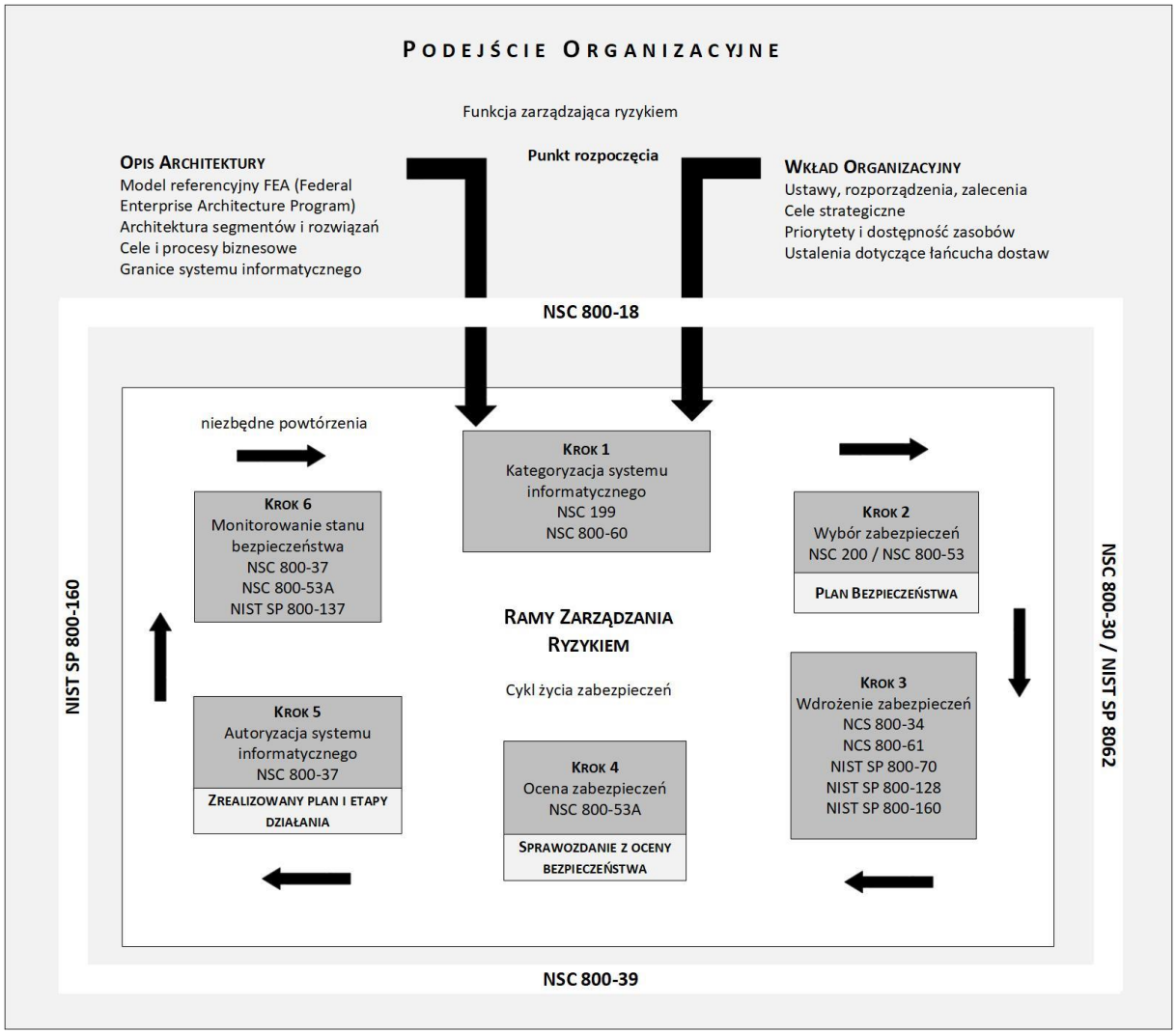
Wskazówka dotycząca implementacji

Ważne jest rutynowe przeglądanie kategoryzacji bezpieczeństwa, ponieważ zmieniają się zadania i otoczenie co powoduje, że poziomy wpływu zakłócenia / incydentu, a nawet typy informacji mogą ulec zmianie.

2.5. ROLA W RAMACH ZARZĄDZANIA RYZYKIEM WG. NSC

Kategoryzacja bezpieczeństwa jest kluczowym, **pierwszym krokiem (Krok 1)** w Ramach Zarządzania Ryzykiem ze względu na jej wpływ na wszystkie pozostałe kroki zarządzaniu ryzykiem, od wyboru zabezpieczeń do wysiłku w ocenie skuteczności zabezpieczeń.

Rysunek 1, *Ramy Zarządzania Ryzykiem NSC*, przedstawia rolę standardów bezpieczeństwa i wytycznych NSC dla bezpieczeństwa systemu informatycznego.



Rysunek 1. Ramy Zarządzania Ryzykiem

Proces kategoryzacji bezpieczeństwa udokumentowany w tej publikacji zapewnia wkład w następujące procesy:

- **Krok 2:** Wybierz początkowy zestaw zabezpieczeń dla systemu informatycznego w oparciu o kategoryzację bezpieczeństwa NSC 199 i zastosuj odpowiednio wytyczne dotyczące dostosowywania, aby uzyskać punkt wyjścia dla wymaganych zabezpieczeń, określonych w NSC 200 i NSC 800-53.

Korzystając z NSC 800-53, uzupełnij początkowy zestaw zastosowanych zabezpieczeń w oparciu o ocenę ryzyka i warunki lokalne, w tym specyficzne dla organizacji wymagania bezpieczeństwa, szczegółowe informacje o zagrożeniu, analizę kosztów i korzyści lub inne szczególne okoliczności.

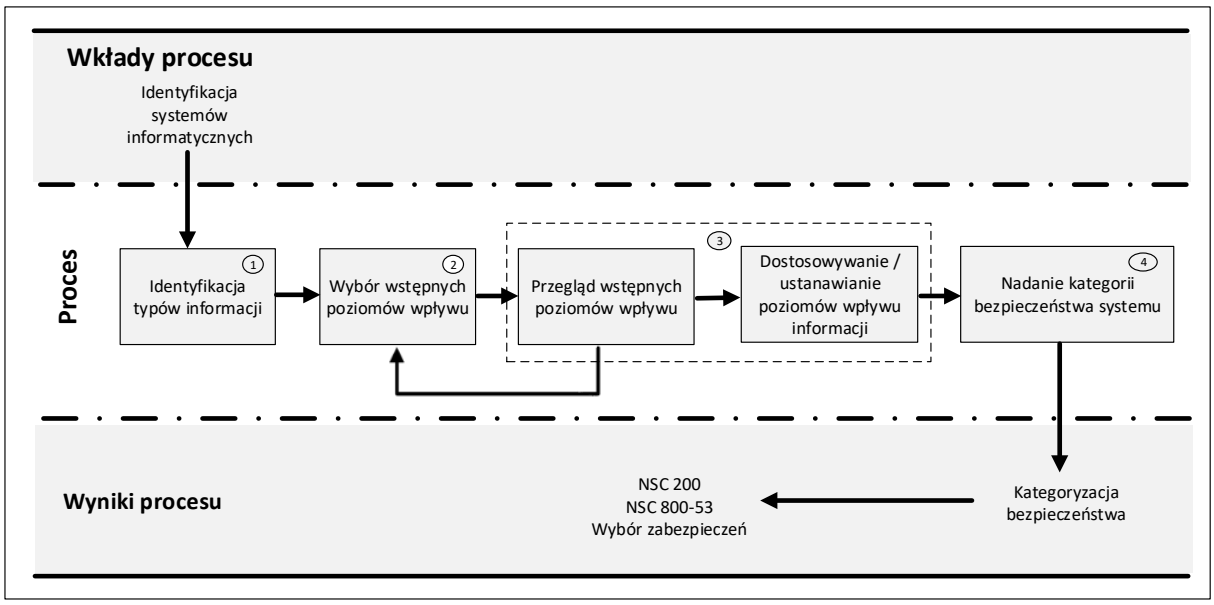
- **Krok 3:** Wprowadź zabezpieczenia w systemie informatycznym.
- **Krok 4:** Oceń zabezpieczenia, stosując odpowiednie metody i procedury, tak aby określić, w jakim stopniu zabezpieczenia są prawidłowo wdrożone, działają zgodnie z przeznaczeniem i dają pożądany wynik w odniesieniu do spełnienia wymagań bezpieczeństwa dla systemu, jak określono w NSC 800-53A.
- **Krok 5:** Autoryzuj eksploatację systemu informatycznego na podstawie określenia ryzyka dotyczącego operacji organizacyjnych, majątku organizacyjnego lub osób fizycznych, wynikającego z funkcjonowania systemu informatycznego oraz decyzji akceptujących to ryzyko, jak określono w NSC 800-37.
- **Krok 6:** Monitoruj i oceniaj w sposób ciągły wybrane środki bezpieczeństwa w systemie informatycznym, w tym dokumentuj zmiany w systemie, przeprowadzaj analizy wpływu zmian na bezpieczeństwo oraz regularnie informuj właściwy personel organizacyjny o stanie bezpieczeństwa systemu, jak określono w NSC 800-37 i NSC 800-53A.

3. KATEGORYZACJA BEZPIECZEŃSTWA INFORMACJI I SYSTEMÓW INFORMATYCZNYCH

PATRZ PUBLIKACJA NSC 199, *STANDARDY KATEGORYZACJI BEZPIECZEŃSTWA*.

4. USTALANIE POZIOMU WPŁYWU INCYDENTU / ZAKŁÓCENIA ORAZ KATEGORYZACJA BEZPIECZEŃSTWA

Ten rozdział zawiera metodologię przypisywania poziomów wpływu incydentu / zakłócenia na bezpieczeństwo i kategoryzacji bezpieczeństwa dla typów informacji i systemów informatycznych zgodnych z celem działania i funkcjami biznesowymi organizacji opartą na NSC 199 *Standardy Kategoryzacji Bezpieczeństwa*. Dokument zakłada, że użytkownik przeczytał i zna NSC 199. Rysunek 2 ilustruje czteroetapowy proces kategoryzacji bezpieczeństwa i sposób, w jaki steruje on wyborem podstawowych zabezpieczeń.



Rysunek 2. Proces kategoryzacji bezpieczeństwa

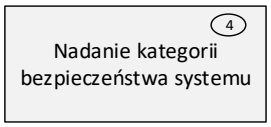
Tabela 3 zawiera krok po kroku plan działania pozwalający na identyfikowanie typów informacji, ustanawiania poziomów wpływu zakłócenia / incydentu na bezpieczeństwo w aspekcie utraty poufności, integralności i dostępności informacji oraz przypisywania kategorii bezpieczeństwa dla typów informacji i systemów informatycznych. Kategoryzacja bezpieczeństwa jest podstawą do określenia początkowego podstawowego zestawu zabezpieczeń dla systemu informatycznego. Każdy funkcjonalny etap procesu wyjaśniono szczegółowo w sekcjach 4.1–4.4.

Krok procesu	Działanie	Role
Wkład procesu: identyfikacja systemu informatycznego	Podmioty powinny opracować własne zasady dotyczące identyfikacji systemu informatycznego do celów kategoryzacji bezpieczeństwa. Na ogół z systemem informatycznym związany jest obwód zabezpieczeń (granica akredytacji systemu).	CIO; SAISO; Właściciel misji

Krok procesu	Działanie	Role
Krok 1 ① Identyfikacja typów informacji	• Dokumentuj obszary działalności i cel działania podmiotu. • Zidentyfikuj wszystkie typy informacji, które są wprowadzane, przechowywane, przetwarzane i / lub wyprowadzane z każdego systemu [sekcja 4.1]: ✓ Zidentyfikuj kategorie typów informacji wynikające z celu działania w oparciu z uwzględnieniem procesów biznesowych FEA [sekcja 4.1.1]; ✓ W razie potrzeby należy określić kategorie typów informacji w procesach zarządzania i wsparcia na podstawie wsparcia procesów biznesowych FEA [sekcja 4.1.2]; ✓ Dla zidentyfikowanych kategorii podaj odpowiednie podfunkcje wynikające z celu działania oraz w zakresie zarządzania i wsparcia [część II, Załączniki A i B]; ✓ W razie potrzeby zidentyfikuj inne wymagane typy informacji [sekcje 4.1.3, 4.1.4]. • Udokumentuj typy informacji mające zastosowanie do zidentyfikowanego systemu informacyjnego wraz z podstawą wyboru rodzaju informacji [sekcja 4.5].	Właściciel misji; Właściciel informacji

Krok procesu	Działanie	Role
Krok 2 (2) Wybór wstępnych poziomów wpływu	• Dla zidentyfikowanych typów informacji wybierz poziomy wpływu na bezpieczeństwo: ✓ spośród zalecanych wstępnych poziomów wpływu dla każdego zidentyfikowanego rodzaju informacji [tom II, dodatki A i B); ✓ albo według kryteriów NSC 199 podanych w tabeli 7 sekcja 4.2.1 i sekcja 4.2.2. • Określ kategorię bezpieczeństwa (SC) dla każdego typu informacji: $SC_{\text{typ informacji}}$ = {(poufność, wpływ), (integralność, wpływ), (dostępność, wpływ)}. • Udokumentuj tymczasowy poziom poufności, integralności i dostępności związany z typem informacji systemu [Sekcja 4.5].	ISSO

Krok procesu	Działanie	Role
Step 3 ③ Przegląd wstępnych poziomów wpływu Dostosowywanie / ustanawianie poziomów wpływu informacji	• Dokonaj przeglądu stosowności wstępnych poziomów wpływu na podstawie uwarunkowań organizacji, środowiska, celu działania, wykorzystania i udostępniania danych [sekcja 4.3]. • W razie potrzeby dostosuj poziomy oddziaływania w oparciu o następujące kryteria: ✓ czynniki oddziaływujące na poufność, integralność, dostępność [sekcja 4.2.2]; ✓ czynniki sytuacyjne i operacyjne (czas, cykl życia itp.) [sekcja 4.3]; ✓ czynniki prawne. • Udokumentuj wszystkie korekty poziomów wpływu i podaj uzasadnienie korekt [Rozdział 4.5].	SAISO; ISSO; Właściciel misji; Właściciel informacji

Krok procesu	Działanie	Role
Krok 4 	• Przejrzyj zidentyfikowane kategorie bezpieczeństwa w celu agregacji typów informacji. • Określ kategoryzację bezpieczeństwa systemu, identyfikując wskaźnik wysokiego poziomu bezpieczeństwa dla każdego z atrybutów (poufność, integralność, dostępność): $SC_{System\ X}$ = {(poufność, wpływ), (integralność, wpływ), (dostępność, wpływ)} • W razie potrzeby przyjmij wysoki poziom wpływu na poziom bezpieczeństwa dla każdego celu bezpieczeństwa systemu, stosując czynniki omówione w sekcji 4.4.2. • Przypisz ogólny poziom wpływu na system informatyczny na podstawie najwyższego poziomu wpływu dla atrybutów bezpieczeństwa systemu (poufność, integralność, dostępność). • Postępuj zgodnie z procesem nadzorczym podmiotu w celu przeglądu, zatwierdzenia i dokumentacji wszystkich ustaleń lub decyzji [sekcja 4.5].	CIO, SAISO; ISSO; Właściciel misji; Właściciel informacji

Krok procesu	Działanie	Role
Wynik procesu: kategoria bezpieczeństwa systemu informatycznego	• Dane wyjściowe można wykorzystać jako dane wejściowe przy wyborze zestawu zabezpieczeń niezbędnych dla danego systemu i ocenie ryzyka w tym systemie. • Minimalne zabezpieczenia zalecane dla każdej kategorii bezpieczeństwa systemu można znaleźć w NSC 800-53.	CIO; ISSO; Osoba autoryzująca; Deweloperzy systemu

Tabela 3. Działania w procesie NSC 800-60

4.1. KROK 1: IDENTYFIKACJA TYPÓW INFORMACJI

Zgodnie z NSC 199 podmioty publiczne identyfikują wszystkie mające zastosowanie typy informacji, które są reprezentatywne dla danych wejściowych, przechowywanych, przetwarzanych i / lub wyjściowych w odniesieniu do każdego systemu. Początkową czynnością polegającą na mapowaniu typów systemów informatycznych i informacji podmiotów publicznych do celów bezpieczeństwa i poziomów wpływu jest opracowanie taksonomii informacyjnej lub stworzenie katalogu typów informacji.[5] Cztery obszary biznesowe dzielą operacje podmiotów publicznych na kategorie najwyższego poziomu w zakresie dotyczącym:

- Celu działalności podmiotu publicznego (usługi dla obywateli);
- Mechanizmów stosowanych przez podmioty publiczne do osiągnięcia celu (sposób dostawy);

[5] Jednym z zagadnień związanych z działalnością taksonomiczną jest określenie stopnia szczegółowości. Jeśli kategorie są zbyt szerokie, wówczas wytyczne dotyczące przypisywania poziomów oddziaływania incydentu / zakłócenia mogą być zbyt ogólne, aby były przydatne. Z drugiej strony, jeśli podejmie się próbę dostarczenia wytycznych dla każdego elementu informacji przetwarzanego przez każdy podmiot publiczny, wytyczne mogą być niewygodne w stosowaniu i wymagać nadmiernie częstych zmian.

- Funkcji wsparcia niezbędnych do prowadzenia operacji podmiotów publicznych (wsparcie świadczenia usług);
- Funkcji zarządzania zasobami, które wspierają wszystkie obszary działalności podmiotów publicznych (zarządzanie zasobami podmiotów publicznych).

Dwa pierwsze obszary biznesowe, usługi dla obywateli i sposób dostarczenia reprezentują typy informacji bezpośrednio związane z celem działania podmiotu i zostaną omówione w następnej sekcji, natomiast wsparcie w zakresie świadczenia usług i zarządzania zasobami podmiotów publicznych zostaną przedstawione w sekcji 4.1.2.

Chociaż wytyczne te identyfikują wiele typów informacji prawdopodobnie tylko kilka zidentyfikowanych typów zostanie przetworzonych przez dowolny pojedynczy system. Ponadto każdy system może przetwarzać informacje, które nie mieszczą się w jednym z wymienionych typów informacji. Po wybraniu zestawu rodzajów informacji określonych w niniejszych wytycznych, rozsądnie jest przejrzeć informacje przetwarzane przez każdy poddany przeglądowi system, aby sprawdzić, czy konieczne jest zidentyfikowanie dodatkowych typów do celów oceny wpływu. Ponadto zaleca się, aby pracownicy podmiotów prowadzili odpowiednią dokumentację zidentyfikowanych typów informacji dla każdego systemu informacyjnego wraz z podstawą wyboru rodzaju informacji. Wskazówki dotyczące dokumentowania rodzajów informacji znajdują się w sekcji 4.5.

4.1.1. IDENTYFIKACJA TYPÓW INFORMACJI ZWIĄZANYCH Z CELEM DZIAŁANIA PODMIOTU

W tej sekcji opisano proces identyfikowania typów informacji na podstawie celu działania podmiotu oraz określania wpływu nieuprawnionego ujawnienia, modyfikacji lub niedostępności tych informacji. Typy informacji wypływające z celu działania podmiotu są z definicji specyficzne dla poszczególnych działów i podmiotów. Usługi dla obywateli stanowią podstawowe ramy odniesienia dla określania poziomów wpływu na atrybuty bezpieczeństwa informacji i systemów informatycznych wynikających z celu działania podmiotu. Konsekwencje lub wpływ nieuprawnionego ujawnienia informacji, modyfikacji lub

jej zniszczenia oraz zakłócenia dostępu do informacji lub możliwości ich wykorzystania są określone przez charakter i beneficjenta świadczonej lub wspieranej usługi.

Tabela 4 przedstawia 26 usług bezpośrednich i usług wsparcia wraz z 98 powiązanymi rodzajami informacji.

Tabela 4. Typy informacji wynikające z zadań administracji rządowej oraz mechanizmy ich realizacji

B.1 Obrona i bezpieczeństwo narodowe Obrona narodowa na poziomie: ✓ strategicznym ✓ operacyjnym ✓ taktycznym
B.2 Bezpieczeństwo wewnętrzne ✓ Bezpieczeństwo granic i transportu ✓ Ochrona kluczowych aktywów i infrastruktury krytycznej ✓ Ochrona przed skutkami katastrof i klęsk żywiołowych
B.3 Operacje wywiadowcze ✓ Planowanie wywiadowcze ✓ Zbieranie danych wywiadowczych ✓ Analiza i opracowania wywiadu ✓ Rozpowszechnianie danych wywiadowczych ✓ Przetwarzanie danych wywiadowczych

B.4 Zarządzanie kryzysowe

- ✓ Monitorowanie i przewidywanie
- ✓ Przygotowanie i planowanie na wypadek katastrof
- ✓ Działania naprawcze i odtworzeniowe
- ✓ Działania ratunkowe

B.5 Sprawy zagraniczne i handel międzynarodowy

- ✓ Sprawy zagraniczne
- ✓ Rozwój międzynarodowy i pomoc humanitarna
- ✓ Handel międzynarodowy

B.6 Zasoby naturalne

- ✓ Zarządzanie zasobami wodnymi
- ✓ Ochrona zasobów, gospodarka morska i gospodarka przestrzenna
- ✓ Zarządzanie zasobami rekreacyjnymi i turystyka
- ✓ Modernizacja i rozwój rolnictwa

B.7 Energia

- ✓ Źródła energii
- ✓ Oszczędzanie energii
- ✓ Zarządzanie zasobami energetycznymi
- ✓ Produkcja energii

B.8 Zarządzanie środowiskiem

- ✓ Monitorowanie i prognozowanie
- ✓ Przeciwdziałanie zmianom klimatycznym
- ✓ Kontrola i zapobieganie skażeniom

B.9 Rozwój ekonomiczny

- ✓ Rozwój usług i produkcji
- ✓ Ochrona własności intelektualnej
- ✓ Nadzór nad sektorem finansowym
- ✓ Stabilizacja dochodów sektora przemysłowego

B.10 Usługi społeczne i socjalne

- ✓ Promocja mieszkalnictwa
- ✓ Rozwój społeczny i regionalny
- ✓ Służby socjalne
- ✓ Usługi pocztowe

B.11 Transport

- ✓ Transport lądowy
- ✓ Transport wodny
- ✓ Transport powietrzny
- ✓ Operacje kosmiczne

B.12 Edukacja

- ✓ Edukacja
- ✓ Szkolnictwo wyższe
- ✓ Ochrona dziedzictwa narodowego
- ✓ Wystawy i muzea

B.13 Sprawy pracy

- ✓ Szkolenie zawodowe i zatrudnianie
- ✓ Prawo pracy
- ✓ Bezpieczeństwo pracy (BHP)

B.14 Zdrowie

- ✓ Dostęp do opieki zdrowotnej
- ✓ Zdrowie publiczne i bezpieczeństwo konsumentów
- ✓ Administracja opieki zdrowotnej
- ✓ Usługi dostarczania opieki zdrowotnej
- ✓ Badania w zakresie opieki zdrowotnej i edukacja pracowników opieki zdrowotnej

B.15 Zabezpieczenie społeczne

- ✓ Emerytury i renty
- ✓ Zasiłek dla bezrobotnych
- ✓ Pomoc społeczna
- ✓ Odszkodowania

B.16 Egzekwowanie prawa

- ✓ Ściganie w sprawach karnych
- ✓ Dochodzenia i śledztwa
- ✓ Ochrona obywateli
- ✓ Ochrona rządu
- ✓ Ochrona własności
- ✓ Kontrola substancji
- ✓ Zapobieganie przestępczości
- ✓ Kontrola obrotu

B.17 Postępowania sądowe i arbitrażowe

- ✓ Procesy sądowe
- ✓ Obrona prawna
- ✓ Dochodzenie prawne
- ✓ Prokuratura i spory sądowe
- ✓ Postępowanie arbitrażowe

B.18 Więziennictwo i resocjalizacja

- ✓ Sprawy więziennictwa
- ✓ Resocjalizacja przestępców

B.19 Nauka i innowacyjność

- ✓ Badania naukowe i technologiczne oraz innowacje
- ✓ Eksploracja kosmosu i innowacje

B.20 Tworzenie i zarządzanie wiedzą

- ✓ Badania i rozwój
- ✓ Statystyka publiczna
- ✓ Doradztwo i konsultacje
- ✓ Upowszechnianie wiedzy

B.21 Zgodność i egzekwowanie przepisów

- ✓ Kontrole i audyty
- ✓ Standaryzacja
- ✓ Zgody i licencje

B.22 Tworzenie i zarządzanie dobrami publicznymi

- ✓ Produkcja przemysłowa
- ✓ Budownictwo
- ✓ Zarządzanie zasobami publicznymi, zarządzaniem infrastrukturą
- ✓ Zarządzanie infrastrukturą informatyczną

B.23 Pomoc publiczna

- ✓ Dotacje państwowe
- ✓ Bezpośredni transfer środków do podmiotów
- ✓ Ulgi podatkowe

B.24 Kredyty i ubezpieczenia ✓ Kredyty bezpośrednie ✓ Poręczenia kredytowe ✓ Ogólne ubezpieczenia
B.25 Przepływy finansowe Rząd - JST ✓ Dotacje ✓ Dofinansowanie projektów ✓ Dotacje celowe ✓ Pożyczki rządowe
B.26 Bezpośrednie usługi dla obywateli ✓ Operacje wojskowe ✓ Operacje cywilne

Podejście do ustanawiania typów informacji związanych z celem działania na poziomie danego podmiotu rozpoczyna się od udokumentowania celów i obszarów działalności. Właściciel każdego systemu informatycznego jest odpowiedzialny za identyfikację typów informacji przechowywanych, przetwarzanych lub generowanych przez ten system informatyczny. W przypadku informacji związanych z celem działania odpowiedzialne osoby, w koordynacji z zainteresowanymi stronami z zakresu zarządzania, operacji i bezpieczeństwa, powinny opracować kompleksowy zestaw procesów prowadzonych przez podmiot. Ponadto osoby odpowiedzialne powinny zidentyfikować odpowiednie podfunkcje niezbędne do prowadzenia działalności podmiotu. Na przykład jednym z celów działania podmiotu może być egzekwowanie prawa. Funkcje podrzędne, które są częścią celu działania organów ścigania, mogą obejmować dochodzenie i śledztwa, zatrzymania i aresztowania,

uwięzienie, ochronę obywateli, zapobieganie przestępczości i ochronę mienia. Każda z tych podfunkcji reprezentowałaby określony typ informacji.

Wstępnie zidentyfikowane typy informacji przetwarzanych przez systemy informatyczne podmiotów publicznych są przedstawione w tabeli 4, a szczegóły przedstawione w Części II, Załącznik B „Przykłady określania wpływu incydentu / zakłócenia na systemy informatyczne i informacje opartych niezbędne do realizacji zadania publicznego".

Wskazówka dotycząca implementacji

Podmiot realizujący zadanie publiczne w celu świadczenia usług wykorzystuje co najmniej jeden z typów informacji opisanych w tabeli 4. Jednak niektóre systemy informacyjne mogą pełnić jedynie rolę wspierającą cel działania podmiotu, a nie przetwarzać bezpośrednio jeden ze wskazanych typów informacji.

4.1.2. IDENTYFIKACJA INFORMACJI ZARZĄDCZEJ I WSPIERAJĄCEJ

Wiele informacji znajdujących się w podmiocie publicznym oraz wiele pomocniczych systemów informatycznych nie jest wykorzystywanych bezpośrednio do świadczenia usług wynikających z celu działania podmiotu, ale wspiera świadczenie tych usług lub zarządzanie zasobami podmiotu. Usługi wsparcia w zakresie świadczenia usług i zarządzania zasobami składają się łącznie z 13 procesów biznesowych (tabele 5 i 6). Procesy te podzielone są na 72 podfunkcje. Usługi wsparcia w zakresie świadczenia usług i zarządzania obszarami biznesowymi związanymi z zasobami są wspólne dla większości podmiotów publicznych, a informacje związane z każdą z ich podfunkcji są określone w niniejszych wytycznych, jako typ informacji w zakresie zarządzania i wsparcia. W celu uwzględnienia informacji o danych osobowych określono cztery dodatkowe typy informacji w zakresie zarządzania i wsparcia. Określono jeden dodatkowy typ informacji w zakresie zarządzania i wsparcia, tak aby zaadresować Informacje ogólne jako typ informacji typu „wszystko inne", który może wystąpić w przypadku specyfiki danego podmiotu. W związku z tym podmioty mogą uznać za konieczne zidentyfikowanie dodatkowych typów informacji, które nie zostały zdefiniowane i przypisać powiązane poziomy bezpieczeństwa dla tych typów.

4.1.2.1. INFORMACJA WSPIERAJĄCA ŚWIADCZENIE USŁUG PUBLICZNYCH

Większość systemów informatycznych wykorzystywanych zarówno do świadczenia usług wsparcia, jak i zarządzania zasobami angażuje się w co najmniej jedną z ośmiu usług wsparcia świadczenia usług. Każdy typ informacji związany z podfunkcjami świadczenia usług jest podany w Tabeli 5. Część II, Załącznik A.2, „Funkcje wsparcia świadczenia usług", zaleca wstępne poziomy wpływu zakłócenia / incydentu na atrybuty bezpieczeństwa w postaci poufności, integralności i dostępności. Funkcje wsparcia usług to codzienne działania niezbędne do zapewnienia krytycznych podstaw politycznych, programowych i zarządczych, które wspierają operacje podmiotów realizujących zadania publiczne. Bezpieczeństwo usług wsparcia jest istotnym czynnikiem zapewniającym bezpieczeństwo usług związanych z celem działania danego podmiotu.

Tabela 5. Informacje w procesach zarządczych i wspierających

A.2.1 Kontrola i nadzór
✓ Działania naprawcze (zasady / akty prawa)
✓ Ewaluacja zadań
✓ Monitorowanie realizacji zadań
A.2.2 Tworzenie zasad regulacyjnych
✓ Opracowywanie zasad i wytycznych
✓ Konsultacje społeczne
✓ Tworzenie przepisów
✓ Publikacja przepisów

A.2.3 Planowanie i budżetowanie

- ✓ Tworzenie budżetu
- ✓ Planowanie środków
- ✓ Architektura korporacyjna
- ✓ Planowanie strategiczne
- ✓ Wykonanie budżetu
- ✓ Planowanie zatrudnienia
- ✓ Kontrola zarządcza
- ✓ Integracja budżetowania i efektywności
- ✓ Polityka podatkowa i fiskalna

A.2.4 Zarządzanie ryzykiem i jego ograniczanie

- ✓ Planowanie awaryjne
- ✓ Ciągłość operacji
- ✓ Odzyskiwanie usług

A.2.5 Realizacja dochodów

- ✓ Windykacja
- ✓ Pobieranie opłat od użytkownika
- ✓ Sprzedaż aktywów

A.2.6 Sprawy publiczne

- ✓ Obsługa klienta
- ✓ Oficjalne rozpowszechnianie informacji
- ✓ Informowanie o usługach
- ✓ Komunikacja wewnętrzna i zewnętrzna

A.2.7 Relacje legislacyjne

- ✓ Śledzenie ustawodawstwa
- ✓ Opinie prawne
- ✓ Opracowanie wniosków de lege ferenda
- ✓ Współpraca z parlamentem

A.2.8 Ogólne zarządzanie

- ✓ Centralne operacje fiskalne
- ✓ Funkcje legislacyjne
- ✓ Funkcje wykonawcze
- ✓ Centralne zarządzanie własnością Skarbu Państwa
- ✓ Centralne zarządzanie personelem
- ✓ Zarządzanie podatkami
- ✓ Centralne zarządzanie dokumentacją i statystykami
- ✓ Informacje o dochodach
- ✓ Tożsamość osób i uwierzytelnianie
- ✓ Informacje o zdarzeniu związanym z uprawnieniami
- ✓ Informacje o reprezentacji odbiorcy płatności
- ✓ Informacje ogólne

4.1.2.2. INFORMACJE W ZAKRESIE ZARZĄDZANIA ZASOBAMI PODMIOTÓW PUBLICZNYCH

Obszar działalności dotyczącej zarządzania zasobami podmiotów publicznych obejmuje zaplecze biurowe (*ang. back office*) działania wspierające, które umożliwiają podmiotowi efektywne działanie. Pięć obszarów biznesowych zarządzania zasobami podmiotów publicznych oraz podfunkcje związane z każdym typem informacji są określone w tabeli 6. Część II, dodatek A.3, „Informacje o zarządzaniu zasobami podmiotów publicznych", zaleca wstępne poziomy wpływu na atrybutu bezpieczeństwa w postaci poufności, integralności i dostępności. Wiele podmiotów publicznych prowadzi własne systemy wsparcia. Inni uzyskują przynajmniej niektóre usługi wsparcia od innych organizacji. Cel działania niektórych podmiotów publicznych polega przede wszystkim na wsparciu innych podmiotów w prowadzaniu ich działań. Jak wskazano powyżej, atrybuty bezpieczeństwa i związane z nimi poziomy wpływu na bezpieczeństwo informacji i systemów administracyjnych i zarządczych są określone przez charakter obsługiwanych usług wynikających z celu działania i obszarów, które są wspierane.

Tabela 6. Informacje związane z zarządzaniem zasobami podmiotów publicznych

A.3.1 Zarządzanie administracyjne
✓ Zarządzanie infrastrukturą, flotą i wyposażeniem
✓ Usługi pomocy technicznej
✓ Zarządzanie bezpieczeństwem
✓ Delegacje
✓ Organizacja miejsc pracy

A.3.2 Zarządzanie finansami

- ✓ Księgowość
- ✓ Kontrola funduszy
- ✓ Płatności
- ✓ Świadczenia i należności
- ✓ Zarządzanie aktywami i pasywami
- ✓ Raportowanie i informacje
- ✓ Rachunek kosztów / pomiar efektywności

A.3.3 Zarządzanie zasobami ludzkimi

- ✓ Strategia HR
- ✓ Pozyskiwanie personelu
- ✓ Organizacja i zarządzanie stanowiskiem
- ✓ Zarządzanie wynagrodzeniami
- ✓ Zarządzanie świadczeniami
- ✓ Zarządzanie wydajnością pracowników
- ✓ Relacje między pracownikami
- ✓ Stosunki pracy
- ✓ Zarządzanie separacją
- ✓ Rozwój zasobów ludzkich

A.3.4 Zarządzanie łańcuchem dostaw

- ✓ Nabywanie towarów
- ✓ Nabywanie usług
- ✓ Inwentaryzacja
- ✓ Zarządzanie logistyczne

A.3.5 Zarządzanie informacją i technologiami

- ✓ Zarządzanie cyklem życia / zmianą
- ✓ Konserwacja systemu
- ✓ Utrzymanie infrastruktury IT
- ✓ Bezpieczeństwo informacji
- ✓ Przechowywanie dokumentacji
- ✓ Zarządzanie informacją
- ✓ Monitorowanie systemu i sieci
- ✓ Udostępnianie informacji

4.1.3. OKREŚLONE PRZEPISAMI KOMPETENCJE WYKONAWCZE W ZAKRESIE INFORMACJI

Podczas identyfikacji rodzajów informacji w systemie informatycznym personel podmiotu powinien poświęcić szczególną uwagę właściwemu zaadresowaniu kompetencji w zakresie zarządzania przetwarzanymi informacjami wspierającymi cel działania podmiotu. Część II, załącznik C zawiera regulacji prawnych w tym zakresie.

4.1.4. IDENTYFIKACJA TYPÓW INFORMACJI NIEWYMIENIONYCH W NINIEJSZYCH WYTYCZNYCH

Przedstawione typy informacji są podane jedynie jako wytyczna taksonomiczna. Nie wszystkie informacje przetwarzane przez system informacyjny można zidentyfikować z tabel

4–6. Dlatego podmiot może zidentyfikować unikatowe typy informacji niewymienione w niniejszych wytycznych lub może nie wybierać wstępnych poziomów wpływu z Części II, dodatek A (dla informacji w zakresie zarządzania i wsparcia) lub Część II, dodatek B (dla typów informacji wynikających z celu działania). Sekcje 4.2.1–4.2.3 niniejszych wytycznych zapewniają podmiotom pomoc w przypisywaniu wstępnych kategorii bezpieczeństwa do poszczególnych typów informacji i systemów informatycznych określonych przez podmiot.

Ponadto NSC 800-60 zapewnia identyfikację informacji w zakresie podfunkcji zarządzania i wsparcia jako typ „informacje ogólne", który może być wykorzystywany przez podmiot, jako sposób identyfikacji i kategoryzacji informacji niezawartych w niniejszych wytycznych. Pełny opis informacji o typie informacji ogólnych należy umieścić w dokumentacji związanej z identyfikacją informacji.

4.2. KROK 2: WSTĘPNY WYBÓR POZIOMU WPŁYWU INCYDENTU / ZAKŁÓCENIA

W kroku 2 podmioty powinny ustalić wstępne poziomy wpływu incydentu / zakłócenia w odniesieniu do typów informacji zidentyfikowane w kroku 1. Wstępne poziomy wpływu to pierwotne poziomy wpływu przypisane atrybutom poufności, integralności dostępności informacji podane w Części II, przed wszelkimi korektami. Na tym etapie jest ustalana i dokumentowana również wstępna kategoryzacja bezpieczeństwa dla typu informacji.

Część II, załącznik A sugeruje wstępne poziomy wpływu na poufność, integralność i dostępność dla typów informacji dotyczących zarządzania i wsparcia, a Część II, załącznik B zawiera przykłady wstępnego przypisania poziomu wpływu dla typów informacji odnoszących się do celu działania podmiotu. Korzystając z kryteriów oceny wpływu określonych w sekcji 3.2 dla atrybutów bezpieczeństwa i rodzajów potencjalnych strat określonych w sekcji 3.1.2, jednostka organizacyjna odpowiedzialna za określenie wpływu musi przypisać zidentyfikowanym typom informacji związanym z celem działania oraz informacjom w zakresie zarządzania i wsparcia poziomy wpływu i związaną z tym kategoryzację bezpieczeństwa dla każdego systemu informatycznego.

4.2.1. KRYTERIA KATEGORYZACJI WEDŁUG NSC 199

W przypadku, gdy typ informacji przetwarzany przez system informacyjny nie jest sklasyfikowany w niniejszych wytycznych, konieczne będzie wstępne określenie wpływu na podstawie kryteriów kategoryzacji NSC 199 (cytowanych w tabeli 7).

Podmioty mogą przypisywać kategorie bezpieczeństwa do typów informacji i systemów informatycznych, wybierając i dostosowując odpowiednie wartości z tabeli 7 pod kątem potencjalnego wpływu naruszenia atrybutów poufności, integralności i dostępności. Osoby odpowiedzialne za wybór poziomu wpływu i późniejszą kategoryzację bezpieczeństwa powinny stosować kryteria określone w tabeli 7 do każdego rodzaju informacji otrzymywanej, przetwarzanej, przechowywanej i / lub generowanej przez każdy system, za który są odpowiedzialne. Kategoryzacja bezpieczeństwa będzie na ogół ustalana na podstawie najbardziej wrażliwych lub krytycznych informacji otrzymywanych, przetwarzanych, przechowywanych i / lub generowanych przez przeglądany system.

Tabela 7. Kategoryzacja informacji i systemów informatycznych w podmiotach publicznych

ATRYBUT BEZPIECZEŃSTWA	POTENCJALNY WPŁYW		
	NISKI	UMIARKOWANY	WYSOKI
Poufność Zapewnienie stosowania zatwierdzonych ograniczeń w zakresie ujawniania i dostępu do informacji, w tym środków ochrony prywatności i informacji osobistych.	Można oczekiwać **ograniczonego** negatywnego wpływu nieuprawnionego ujawnienia informacji na działalność organizacji, jej zasoby lub osoby fizyczne.	Można oczekiwać **poważnego** negatywnego wpływu nieuprawnionego ujawnienia informacji na działalność organizacji, jej zasoby lub osoby fizyczne.	Można oczekiwać **drastycznie lub katastrofalnie** negatywnego wpływu nieuprawnionego ujawnienia informacji na działalność organizacji, jej zasoby lub osoby fizyczne.

ATRYBUT BEZPIECZEŃSTWA	POTENCJALNY WPŁYW		
	NISKI	**UMIARKOWANY**	**WYSOKI**
Integralność Ochrona przed niewłaściwą modyfikacją lub zniszczeniem informacji, w tym zapewnienie niezaprzeczalności i autentyczności informacji.	Można oczekiwać **ograniczonego** negatywnego wpływu nieuprawnionej modyfikacji lub zniszczenia informacji na działalność organizacji, jej zasoby lub osoby fizyczne.	Można oczekiwać **poważnego** negatywnego wpływu nieuprawnionej modyfikacji lub zniszczenia informacji na działalność organizacji, jej zasoby lub osoby fizyczne.	Można oczekiwać **drastycznie lub katastrofalnie** negatywnego wpływu nieuprawnionej modyfikacji lub zniszczenia informacji na działalność organizacji, jej zasoby lub osoby fizyczne.
Dostępność Zapewnienie terminowego i niezawodnego dostępu i możliwości wykorzystania informacji.	Można oczekiwać **ograniczonego** negatywnego wpływu zaburzenia dostępu lub możliwości wykorzystania informacji na działalność organizacji, jej zasoby lub osoby fizyczne.	Można oczekiwać **poważnego** negatywnego wpływu zaburzenia dostępu lub możliwości wykorzystania informacji na działalność organizacji, jej zasoby lub osoby fizyczne.	Można oczekiwać **drastycznie lub katastrofalnie** negatywnego wpływu zaburzenia dostępu lub możliwości wykorzystania informacji na działalność organizacji, jej zasoby lub osoby fizyczne.

4.2.2. WSPÓLNE CZYNNIKI WPŁYWAJĄCE NA WYBÓR POZIOMÓW WPŁYWU

W przypadku, gdy podmiot określa poziomy wpływu na bezpieczeństwo i kategoryzację bezpieczeństwa na podstawie lokalnego zastosowania kryteriów NSC 199, zaleca się rozważenie następujących czynników w odniesieniu do wpływu na bezpieczeństwo dla każdego rodzaju informacji.

4.2.2.1. CZYNNIKI WPŁYWAJĄCE NA POUFNOŚĆ

Wykorzystując kryteria potencjalnego wpływu zakłócenia/ incydentu według NSC 199, podsumowane w tabeli 7, każdy rodzaj zidentyfikowanej informacji należy ocenić pod kątem poufności w odniesieniu do poziomu wpływu związanego z nieuprawnionym ujawnieniem (i) każdego znanego wariantu informacji należącego do typu oraz (ii) każdego zastosowania informacji w przeglądanym systemie. Odpowiedzi na następujące pytania pomogą w procesie oceny:

- W jaki sposób atakujący może wykorzystać nieuprawnione ujawnienie informacji, aby wyrządzić ograniczoną / poważną / drastyczną lub katastrofalną szkodę działaniom podmiotowi, jego majątkowi lub osobom?
- W jaki sposób atakujący może wykorzystać nieuprawnione ujawnienie informacji, aby przejąć kontrolę nad aktywami podmiotu, co może skutkować nieuprawnioną modyfikacją informacji, zniszczeniem informacji lub odmową usług systemowych, co z kolei skutkowałoby ograniczoną / poważną / drastyczną lub katastrofalną szkodą dla działalności podmiotu, jego aktywów czy osób fizycznych?
- Czy nieupoważnione ujawnienie / rozpowszechnianie elementów tego typu informacji naruszałoby prawo powszechne lub wewnętrze przepisy podmiotu?

4.2.2.2. CZYNNIKI WPŁYWAJĄCE NA INTEGRALNOŚĆ

Wykorzystując kryteria potencjalnego wpływu zakłócenia/ incydentu według NSC 199, podsumowane w tabeli 7, każdy typ informacji powinien być oceniany pod kątem integralności w odniesieniu do poziomu wpływu związanego z nieuprawnioną modyfikacją lub zniszczeniem (i) każdego znanego wariantu informacji należącego do typu oraz (ii) każdego zastosowania informacji w przeglądanym systemie. Odpowiedzi na następujące pytania pomogą w procesie oceny:

- W jaki sposób atakujący może wykorzystać nieautoryzowaną modyfikację lub zniszczenie informacji w celu wyrządzenia ograniczonej / poważnej / drastycznej lub katastrofalnej szkody działaniom podmiotu, jego majątkowi lub osobom?

- Czy nieautoryzowana modyfikacja / zniszczenie elementów typu informacji naruszałaby prawo powszechne lub wewnętrze przepisy podmiotu?

Nieautoryzowana modyfikacja lub zniszczenie informacji może przybierać różne formy. Zmiany mogą być subtelne i trudne do wykrycia lub mogą wystąpić na dużą skalę. Można skonstruować niezwykle szeroki zakres scenariuszy modyfikacji informacji i jej prawdopodobnych konsekwencji. Kilka przykładów obejmuje fałszowanie lub modyfikowanie informacji w celu:

- Zmniejszenia zaufania publicznego do podmiotu;
- Uzyskania nieprzysługujących korzyści finansowych;
- Stworzenia zamieszania lub wywołania kontrowersji poprzez oszukańcze ogłoszenie nieprawdziwej procedury;
- Zainicjowania zamieszania lub wywołania kontrowersji poprzez ogłoszenie fałszywej polityki;
- Wpływu na decyzje personelu;
- Ingerowania w pracę organów ścigania lub procesy sądowe lub manipulowania nimi;
- Wpływu na ustawodawstwo;
- Uzyskania nieautoryzowanego dostępu do informacji, a w konsekwencji naruszenia poufności.

W większości przypadków najpoważniejsze skutki naruszenia integralności mają miejsce, gdy podejmowane są działania oparte na zmodyfikowanych informacjach lub zmodyfikowane informacje są rozpowszechniane wśród innych organizacji lub społeczeństwa.

Niewykryta utrata integralności może być katastrofalna dla wielu rodzajów informacji. Konsekwencje naruszenia integralności mogą być bezpośrednie (np. zmiana zapisu finansowego, wpisu medycznego lub zmiana wpisu w rejestrze karnym) lub pośrednie (np. ułatwienie nieuprawnionego dostępu do poufnych lub prywatnych informacji lub odmowa dostępu do informacji lub usług systemu informacyjnego). Złośliwe wykorzystanie dostępu

do informacji i systemów informatycznych może wyrządzić ogromną szkodę celowi działania podmiotu i może spowodować wykorzystanie systemu podmiotu jako proxy dla ataków na inne systemy.

W niektórych przypadkach można oczekiwać, że konsekwencje nieuprawnionej modyfikacji lub zniszczenia informacji będą ograniczone i nie zagrożą celowi działania podmiotu lub zaufania publicznego do niego. W innych przypadkach kompromitacja w zakresie rzetelności może spowodować zagrożenie życia ludzkiego lub inne poważne konsekwencje. Wpływ może być szczególnie dotkliwy w przypadku informacji z krytycznym uwarunkowaniem czasowym (np. skierowanie zespołu ratunkowego pod niewłaściwy adres).

4.2.2.3. CZYNNIKI WPŁYWAJĄCE NA DOSTĘPNOŚĆ

Wykorzystując kryteria potencjalnego wpływu zakłócenia/ incydentu według NSC 199, podsumowane w tabeli 7, każdy typ informacji należy ocenić pod kątem dostępności w odniesieniu do poziomu wpływu związanego z zakłóceniem dostępu do informacji lub ich wykorzystywaniem (i) każdego znanego wariantu informacji należącego do typu oraz (ii) każdego zastosowania informacji w przeglądanym systemie. Odpowiedzi na następujące pytania pomogą w procesie oceny:

- W jaki sposób atakujący może wykorzystać zakłócenia w dostępie do informacji lub ich wykorzystywanie, aby wyrządzić ograniczoną / poważną / drastyczną lub katastrofalną szkodę działaniom podmiotu, jego majątkowi lub osobom?
- Czy zakłócenie dostępu lub wykorzystanie elementów tego typu informacji naruszałoby prawo powszechne lub wewnętrze przepisy podmiotu?

W przypadku wielu typów informacji i systemów informatycznych poziom wpływu na dostępność zależy od tego, jak długo informacje lub system pozostają niedostępne. Niewykryta utrata dostępności może mieć katastrofalne skutki dla wielu rodzajów informacji. Na przykład trwała utrata dostępu do informacji w zakresie budżetu, planowania awaryjnego, ciągłości operacji, odzyskiwania usług, windykacji, zarządzania podatkami, zarządzania personelem, zarządzania płacami, zarządzania bezpieczeństwem, zarządzania

logistycznego lub bazy danych z informacjami księgowymi byłyby katastrofalna dla prawie każdego podmiotu. Całkowita rekonstrukcja takich baz danych byłaby czasochłonna i kosztowna.

W większości przypadków negatywne skutki ograniczenia dostępności przez krótki czas będą nieznaczne dla funkcji podmiotu i zaufania publicznego do niego. Jednak w przypadku informacji o znaczeniu krytycznym, istnieje mniejsze prawdopodobieństwo, że dostępność zostanie przywrócona zanim dojdzie do poważnych szkód dla aktywów podmiotu, jego operacji lub jego personelu albo dla dobra publicznego. W takich przypadkach udokumentowane zalecenia dotyczące poziomu wpływu na dostępność powinny wskazywać, że informacja jest krytyczna czasowo i stanowi to podstawę do sklasyfikowania systemu, jako krytyczny.

4.2.3. PRZYKŁADY WYBORU POZIOMÓW WPŁYWU NA PODSTAWIE NSC 199

Poniżej przedstawiono przykłady określania poziomu wpływu incydentu / zakłócenia według NSC 199:

Przykład 1: Organizacja zarządza informacjami publicznymi na swoim serwerze internetowym ustala, że nie ma potencjalnego wpływu incydentu / zakłócenia w wyniku utraty poufności (tj. wymogi dotyczące poufności nie mają zastosowania), istnieje umiarkowany potencjalny wpływ z powodu utraty integralności i umiarkowany potencjalny wpływu z powodu utraty dostępność. Wynikową kategorię bezpieczeństwa tego typu informacji wyraża się, jako:

$$\text{Kategoria Bezpieczeństwa}_{\textit{informacje publiczne}} = \max\{(\text{poufność, nie dotyczy}), (\text{integralność, umiarkowany}), (\text{dostępność, umiarkowany})\} = \text{umiarkowany}.$$

Przykład 2: Organ ścigania zarządzający wyjątkowo wrażliwymi informacjami dochodzeniowymi stwierdza, że potencjalny wpływ utraty poufności jest wysoki, potencjalny wpływ utraty integralności jest umiarkowany, a potencjalny wpływ utraty dostępności jest umiarkowany. Wynikową kategorię bezpieczeństwa dla tego rodzaju informacji wyraża się, jako:

Kategoria Bezpieczeństwa $_{informacje\ dochodzenia}$ = max {(poufność, wysoki), (integralność, umiarkowany), (dostępność, umiarkowany)} = wysoki.

Przykład 3: Organizacja finansowa zarządzając rutynowymi informacjami administracyjnymi (niezwiązanymi z danymi osobowymi) stwierdza, że potencjalny wpływ utraty poufności jest niewielki, potencjalny wpływ utraty integralności jest niewielki oraz potencjalny wpływ utraty dostępności jest niewielki. Wynikową kategorię bezpieczeństwa tego typu informacji wyraża się, jako:

Kategoria Bezpieczeństwa $_{informacje\ administracyjna}$ = max {(poufność, niski), (integralność, niski), (dostępność, niski)} = niski.

Ogólnie rzecz biorąc, ocena wpływu na atrybuty bezpieczeństwa jest niezależna od mechanizmów stosowanych w celu złagodzenia skutków kompromitacji (tak jakby ich nie było lub całkowicie by zawiodły).

4.3. KROK 3: PRZEGLĄD WSTĘPNYCH POZIOMÓW WPŁYWU I DOSTOSOWANIE POZIOMU WPŁYWU DO KONKRETNEJ SYTUACJI

W kroku 3 podmioty powinny przejrzeć i dostosować wstępne poziomy wpływu na atrybuty bezpieczeństwa dla każdego rodzaju informacji i określić ostateczną wartość tego poziomu. Aby to osiągnąć, podmioty powinny: (i) dokonać przeglądu stosowności wstępnie przyjętych poziomów wpływu na podstawie organizacji, środowiska, celu działania, wykorzystania i udostępniania danych; (ii) w razie potrzeby dostosowywać poziomy wpływu na atrybuty bezpieczeństwa przy użyciu specjalnych czynników zawartych w Części II, załączniki A i B; oraz (iii) udokumentować wszystkie korekty poziomów wpływu i podać uzasadnienie tych korekt.

Gdy poziomy wpływu kategoryzacji bezpieczeństwa zalecane w sekcji 4.2 lub Części II, dodatki A i B zostaną przyjęte jako wstępne poziomy wpływu na bezpieczeństwo, podmiot powinien dokonać przeglądu adekwatności wstępnie przyjętych poziomów wpływu w kontekście organizacji, środowiska, celu działania, wykorzystania i udostępnianie danych związane z przeglądanym systemem informatycznym. Przegląd ten powinien obejmować

znaczenie celu działania podmiotu, wpływ na cykl życia i aktualność, informacje dotyczące konfiguracji i zasad bezpieczeństwa; specjalne wymagania dotyczące obsługi, itp. Czynniki NSC 199 przedstawione w sekcji 4.2.2 niniejszego dokumentu powinny być wykorzystane, jako podstawa do decyzji dotyczących korekty lub akceptacji wstępnych poziomów wpływu. W trakcie przeglądu poziomy wpływu w zakresie poufności, integralności i dostępności mogą być korygowane wielokrotnie. Po zakończeniu procesu przeglądu i dostosowywania można sfinalizować mapowanie poziomów oddziaływania według rodzaju informacji.

Wpływ ujawnienia określonego rodzaju informacji może być odmienny w różnych podmiotach lub w różnych kontekstach operacyjnych. Ponadto wpływ rodzaju informacji może być różny w danej fazie cyklu życia. Na przykład informacje o umowie, które mają umiarkowany poziom wpływu na poufność w okresie obowiązywania umowy, mogą mieć niski poziom wpływu po zakończeniu umowy. Informacje o polityce mogą mieć umiarkowany poziom wpływu na poufność i integralność podczas procesu opracowywania polityki, niski poziom poufności i umiarkowany poziom wpływu na integralność, gdy polityka jest wdrażana, oraz niski poziom wpływu na poufność i integralność, gdy polityka nie jest już używana.

Na poziomy wpływu związane z informacjami w zakresie zarządzania i wsparcia, wspólnymi dla wielu podmiotów, silnie wpływają informacje związane z celem działania podmiotu, z którymi są one powiązane. Oznacza to, że wspólne informacje podmiotów dotyczące zarządzania i wsparcia używane wraz z bardzo wrażliwymi lub krytycznymi typami informacji związanymi z celem działania mogą mieć wyższy poziom wpływu, niż te same wspólne informacje używane z mniej krytycznymi typami informacji związanymi z celem działania.

Systemy informatyczne przetwarzają wiele rodzajów informacji. Nie wszystkie typy informacji wymagają takiego samego poziomu bezpieczeństwa. Kompromitacja niektórych rodzajów informacji zagrozi bardziej funkcjonalności podmiotu niż kompromitacja innych typów informacji. Poziomy wpływu na bezpieczeństwo systemu należy oceniać w kontekście celu działania podmiotu i funkcji systemu, z uwzględnieniem agregacji typów informacji.

Informacje o konfiguracji i egzekwowaniu zasad bezpieczeństwa powinny zostać przejrzane i dostosowane, biorąc pod uwagę to, jakie informacje są przetwarzane w systemie. Informacje o konfiguracji i polityce bezpieczeństwa obejmują pliki haseł, reguły dostępu do sieci, inne ustawienia konfiguracji sprzętu i oprogramowania oraz dokumentację wpływającą na dostęp do danych, programów i / lub procesów systemu informatycznego. Dla tego zestawu informacji i procesów będzie miał zastosowanie co najmniej niski poziom wpływu na poufność i integralność, ze względu na możliwość uszkodzenia, niewłaściwego wykorzystania lub nadużycia informacji i procesów systemowych (nie można pominąć tych atrybutów w analizie).

Czynnikiem charakterystycznym dla zachowania poufności są informacje podlegające specjalnemu postępowaniu (np. Informacje podlegające przepisom o ochronie danych osobowych). Bez względu na inne względy, pewien minimalny poziom wpływu na poufność musi być przypisany do każdego systemu informatycznego, który przechowuje, przetwarza lub generuje takie informacje. Przykładami takich informacji są informacje stanowiące tajemnicę przedsiębiorcy, dane osobowe, tajemnice skarbowe, informacje niejawne i inne informacje podlegające ochronie ustawowej.

4.4. KROK 4: PRZYPISANIE KATEGORII BEZPIECZEŃSTWA SYSTEMU

Po wybraniu, sprawdzeniu i dostosowaniu poziomów wpływu na bezpieczeństwo, w zależności od atrybutów bezpieczeństwa każdego rodzaju informacji przetwarzanego przez system informatyczny, konieczne jest przypisanie kategorii bezpieczeństwa systemu na podstawie agregacji typów informacji. Działania w kroku 4 obejmują: (i) przegląd zidentyfikowanych kategoryzacji bezpieczeństwa dla agregacji typów informacji; (ii) określenie kategoryzacji bezpieczeństwa systemu, identyfikując poziom wpływu dla każdego z atrybutów bezpieczeństwa (poufność, integralność, dostępność) na podstawie agregacji rodzajów informacji; (iii) w razie potrzeby dostosowanie poziomu wpływu dla każdego z atrybutów bezpieczeństwa systemu, stosując czynniki omówione w sekcji 4.4.2; (iv) przypisanie ogólnego poziomu wpływu na system informatyczny na podstawie najwyższego poziomu wpływu na atrybuty bezpieczeństwa systemu; oraz

(v) udokumentowanie wszystkich ustaleń i decyzji dotyczących kategoryzacji bezpieczeństwa.

4.4.1. PROCES KATEGORYZACJI BEZPIECZEŃSTWA SYSTEMU ZGODNIE Z NSC 199

NSC 199 stanowi, że określenie kategorii bezpieczeństwa systemu informatycznego wymaga dodatkowej analizy i musi wziąć pod uwagę kategorie bezpieczeństwa wszystkich typów informacji rezydujących w systemie informatycznym. W przypadku systemu informatycznego, potencjalne poziomy wpływu na bezpieczeństwo przypisane każdemu z odpowiednich atrybutów bezpieczeństwa (poufność, integralność, dostępność) są najwyższym poziomem dla każdego z tych atrybutów, który został określony dla typów informacji znajdujących się w systemie informatycznym.

Systemy informatyczne składają się zarówno z programów komputerowych, jak i informacji. Programy wykonywane w ramach systemu informatycznego (tj. procesy systemowe) ułatwiają przetwarzanie, przechowywanie i przekazywanie informacji oraz są niezbędne dla organizacji do wykonywania jej podstawowych funkcji i operacji biznesowych. Funkcje przetwarzania systemowego również wymagają ochrony i mogą podlegać kategoryzacji bezpieczeństwa. Jednakże, w celu uproszczenia, przyjmuje się, że kategoryzacja bezpieczeństwa wszystkich typów informacji związanych z systemem informatycznym zapewnia kategoryzację dla całego systemu informatycznego - tym samym eliminując potrzebę rozważenia procesów systemowych w ramach kategoryzacji bezpieczeństwa systemu informatycznego. Wynika to z:

- zasadniczego wymogu ochrony integralności, dostępności, a w przypadku istotnych informacji, takich jak hasła i klucze szyfrujące, poufności funkcji systemowych oraz informacji na poziomie wysokim;
- silnej współzależności między poufnością, integralnością i dostępnością.

Z tego powodu NSC 199 zauważa, że o ile wartość (tzn. poziom) *„niemająca zastosowania - ND”* może dotyczyć jakiegoś atrybutu bezpieczeństwa dla określonych typów informacji przetwarzanych przez systemy, to wartość ta nie może być przypisana do żadnego atrybutu

bezpieczeństwa systemu informatycznego. Istnieje minimalny wstępny wpływ (niski) odnoszący się do naruszenia poufności, integralności i dostępności systemu informatycznego. Jest to niezbędne do zapewnienia ochrony funkcji przetwarzania na poziomie systemu oraz informacji krytycznych dla funkcjonowania systemu informacyjnego.

Uogólniony format wyrażania kategorii bezpieczeństwa, czyli SC, systemu informatycznego jest następujący:

$SC_{\text{System informacyjny}}$ = {(poufność, wpływ), (integralność, wpływ), (dostępność, wpływ)},

gdzie dopuszczalne wartości dla potencjalnego oddziaływania są NISKI, UMIARKOWANY lub WYSOKI.

Poniższe przykłady ilustrują proces kategoryzacji bezpieczeństwa systemu informatycznego opisany w NSC 199.

PRZYKŁAD SYSTEMU 1: System informatyczny stosowany w organizacji przy dużych zamówieniach zawiera zarówno wrażliwe informacje o kontraktach w fazie przed zamówieniem, jak i rutynowe informacje administracyjne. Stwierdza to kierownictwo w organizacji zamawiającej: (i) w przypadku newralgicznych informacji o umowie potencjalny wpływ utraty poufności jest umiarkowany, potencjalny wpływ utraty integralności jest umiarkowany, a potencjalny wpływ utraty dostępności jest niski; oraz (ii) w przypadku rutynowych informacji administracyjnych (informacji niezwiązanych z prywatnością) potencjalny wpływ utraty poufności jest niski, potencjalny wpływ utraty integralności jest niski, a potencjalny wpływ utraty dostępności jest niski. Wynikające z tego kategorie bezpieczeństwa, czyli SC, tych rodzajów informacji są wyrażone, jako:

$SC_{\text{Informacje o umowie}}$ = {(poufność, UMIARKOWANY), (integralność, UMIARKOWANY), (dostępność, NISKI)} = UMIARKOWANY,

oraz

$SC_{\text{informacje administracyjne}}$ = {(poufność, NISKI), (integralność, NISKI), (dostępność, NISKI)} = NISKI.

Wynikająca z tego kategoria bezpieczeństwa systemu informatycznego jest wyrażona, jako:

$SC_{\text{System zamówień}}$ = {(poufność, UMIARKOWANY), (integralność, UMIARKOWANY), (dostępność, NISKI)} = UMIARKOWANY,

reprezentująca najwyższą potencjalną wartość oddziaływania na każdy z atrybutów bezpieczeństwa spośród typów informacji znajdujących się w systemie zamówień.

PRZYKŁAD SYSTEMU 2: Elektrownia wykorzystuje system SCADA (sterowanie i pozyskiwanie danych) sterujący dystrybucją energii elektrycznej dla dużej instalacji wojskowej. System SCADA zawiera zarówno dane z czujników w czasie rzeczywistym, jak i rutynowe informacje administracyjne. Kierownictwo elektrowni stwierdza: (i) w przypadku danych z czujników pozyskiwanych przez system SCADA żadnego potencjalnego wpływu nie ma utrata poufności, wysoki potencjalny wpływu ma utrata integralności oraz Wysoki potencjalny wpływ ma utraty dostępności; oraz (ii) w przypadku informacji administracyjnych przetwarzanych przez system, istnieje niski potencjalny wpływ utraty poufności, niski potencjalny wpływ utrata integralności oraz niski potencjalny wpływ utrata dostępności. Wynikające z tego kategorie bezpieczeństwa, czyli SC, tych rodzajów informacji są wyrażone, jako:

$SC_{\text{Informacje z czujników}}$ = {(poufność, ND), (integralność, WYSOKI), (dostępność, WYSOKI)} = WYSOKI,

oraz

$SC_{\text{informacje administracyjne}}$ = {(poufność, NISKI), (integralność, NISKI), (dostępność, NISKI)} = NISKI.

Wynikająca z tego kategoria bezpieczeństwa systemu informatycznego jest wyrażona, jako:

$SC_{\text{System SCADA}}$ = {(poufność, NISKI), (integralność, WYSOKI), (dostępność, WYSOKI)} = WYSOKI,

reprezentująca najwyższą potencjalną wartość oddziaływania na każdy z atrybutów bezpieczeństwa spośród typów informacji znajdujących się w systemie SCADA. Kierownictwo elektrowni decyduje się na zwiększenie potencjalnego wpływu utraty poufności z niskiej do umiarkowanej, odzwierciedlając bardziej realistyczny obraz potencjalnego wpływu na system informatyczny w przypadku naruszenia bezpieczeństwa z powodu nieuprawnionego

ujawnienia informacji na poziomie systemu lub funkcji przetwarzania. Końcowa kategoria bezpieczeństwa systemu informatycznego jest wyrażona, jako:

$SC_{System\ SCADA}$ = {(poufność, UMIARKOWY), (integralność, WYSOKI), (dostępność, WYSOKI)} = WYSOKI

4.4.2. WYTYCZNE DOTYCZĄCE KATEGORYZACJI SYSTEMÓW

W niektórych przypadkach poziom wpływu na kategorię bezpieczeństwa systemu będzie wyższy niż jakikolwiek obiektywny poziom wpływu na bezpieczeństwo dla jakiegokolwiek typu informacji przetwarzanych przez system.

Podstawowymi czynnikami, które najczęściej podnoszą poziom kategorii bezpieczeństwa systemu ponad poziom wpływu na typy informacji występujących w systemie, są agregacja i krytyczna funkcjonalność systemu. Ponadto w procesie przypisywania skutków konieczne może być uwzględnienie zmian w zakresie wrażliwości/krytyczności w odniesieniu do czasu. Niektóre informacje tracą swoją wrażliwość w czasie (np. prognozy ekonomiczne po ich opublikowaniu). Inne informacje są szczególnie krytyczne w pewnym momencie (np. dane pogodowe w strefie podejścia w terminalu podczas operacji lądowania statku powietrznego). W tej części przedstawiono pewne ogólne wytyczne dotyczące sposobu w jaki agregacja, krytyczne funkcje i inne czynniki systemowe mogą wpływać na kategoryzację bezpieczeństwa systemu.

Wskazówka dotycząca implementacji

Personel podmiotu powinien być świadomy, że istnieje kilka czynników, które należy uwzględnić podczas agregacji rodzajów informacji systemowych. Rozważając te czynniki, można stwierdzić, że wcześniej nieprzewidziane obawy mogą mieć wpływ na poziom poufności, integralności i/lub dostępności na poziomie systemu. Czynniki te obejmują agregowanie danych, krytyczną funkcjonalność systemu, okoliczności łagodzące i inne czynniki systemowe.

Aby skutecznie zrealizować ten krok w podejmowanie decyzji dotyczących oceny skutków na poziomie systemu konieczne może być zaangażowanie różnych zainteresowanych stron (np. kierownictwa, personelu operacyjnego lub ekspertów ds. bezpieczeństwa).
W poniższych sekcjach przedstawiono czynniki, które należy uwzględnić przy dostosowywaniu poziomów wpływu na atrybuty bezpieczeństwa systemu.

4.4.2.1. AGREGACJA

Niektóre informacje mogą mieć małą lub żadną wrażliwość w izolacji, ale mogą być bardzo wrażliwe w agregacji. W niektórych przypadkach agregacja dużych ilości jednego rodzaju informacji może ujawnić wrażliwe wzorce i plany lub ułatwić dostęp do wrażliwych lub krytycznych systemów. W innych przypadkach agregacja informacji kilku różnych i pozornie nieszkodliwych rodzajów może mieć podobne skutki. Ogólnie rzecz biorąc, wrażliwość danego elementu danych będzie prawdopodobnie większa w kontekście z innymi niż w izolacji (np. powiązanie numeru rachunku z tożsamością osoby fizycznej lub instytucji). Szybko rośnie dostępność i rutynowe wykorzystanie operacyjne zaawansowanych narzędzi wnioskowania na podstawie agregowania danych. Jeżeli przegląd ujawni zwiększoną wrażliwość lub krytyczność związaną z agregatami informacji, wówczas poziomy wpływu na atrybuty bezpieczeństwa systemu może wymagać dostosowania do wyższego poziomu niż wskazany przez poziomy wpływu na bezpieczeństwo związane z każdym indywidualnym rodzajem informacji. Można tego dokonać poprzez włączenie oświadczenia wyjaśniającego zagregowany wpływ na atrybuty bezpieczeństwa, jak również zmianę poziomów wpływu na bezpieczeństwo.

4.4.2.2. KRYTYCZNA FUNKCJONALNOŚĆ SYSTEMU

Kompromitacja niektórych rodzajów informacji może mieć niewielkie oddziaływanie w kontekście podstawowej funkcji systemu, ale może mieć znacznie większe znaczenie, gdy jest postrzegana w kontekście potencjalnego oddziaływania tej kompromitacji na inne systemy:

- do których dany system jest podłączony,
- które są zależne od informacji z danego systemu.

W przypadku systemu, który przetwarza jedynie informacje o niewielkim wpływie na bezpieczeństwo, można początkowo uznać, że ma on jedynie niewielkie znaczenie dla bezpieczeństwa. Jeżeli jednak dostęp do tego systemu może skutkować jakąś formą dostępu do innych systemów (np. poprzez sieć), należy rozważyć wrażliwość i krytyczność wszystkich systemów, do których może prowadzić taki pośredni dostęp. Podobnie, niektóre informacje mogą mieć na ogół niską wrażliwość lub krytyczność atrybutów bezpieczeństwa. Informacje te mogą być jednak wykorzystywane przez inne systemy w celu umożliwienia realizacji niezwykle wrażliwych lub krytycznych funkcji (np. wykorzystanie przez kontrolę ruchu lotniczego informacji o pogodzie lub wykorzystanie komercyjnych informacji o lotach do identyfikacji wojskowych systemów transportu bojowego). Utrata integralności danych, ich dostępności, kontekstu czasowego lub innego kontekstu może mieć wtedy skutki katastrofalne.

4.4.2.3. UWZGLĘDNIENIE SKUTKÓW WYNIKAJĄCYCH Z INNYCH OKOLICZNOŚCI NIŻ KATEGORYZACJA INFORMACJI

Niniejsza publikacja koncentruje się na kategoryzacji systemu informatycznego na podstawie przetwarzanych w nim rodzajów informacji i związanych z nimi skutków dla bezpieczeństwa. Są okoliczności, kiedy poziom wpływu atrybuty bezpieczeństwa systemu powinien zostać podniesiony na podstawie innych przyczyn niż informacje. Na przykład system informacyjny zapewnia obsługę krytycznego procesu lub zapewnia wsparcie w dziedzinie bezpieczeństwa, jest dostępny dla ogółu społeczeństwa, wspiera inne systemy zależne od jego działania lub wymagałby znacznych nakładów w przypadku ewentualnej wymiany. Przykłady te, biorąc pod uwagę konkretną sytuację, mogą uzasadnić zwiększenie przez właściciela systemu ogólnego poziomu wpływu na bezpieczeństwo systemu.

Konieczność podniesienia poziomu wpływu w oparciu o przewidywanie powyższych skutków może być bardziej widoczne poprzez porównanie pierwotnej kategoryzacji bezpieczeństwa z analizą wpływu na działalność. Jeśli system został skategoryzowany na podstawie NSC 199 jako posiadający umiarkowanym poziom wpływu, ale właściciel systemu stwierdził, że musi on wznowić działanie w ciągu 4-8 godzin od zakłócenia, niezależnie od wyżej przypisanego

poziomu wpływu na bezpieczeństwo zagregowanej dostępności informacji, wówczas istnieje wyłączenie ogólnej zasady, które może spowodować zastosowanie wyższej kategoryzacji systemu. Aby uzyskać pełną adekwatność do konkretnych okoliczności, podmioty muszą odpowiednio dostosować poziom wpływu na bezpieczeństwo dostępności systemu informatycznego.

4.4.2.4. INNE CZYNNIKI

Integralność informacji publicznej

Większość podmiotów publicznych prowadzi strony internetowe, które są publicznie dostępne. Zdecydowana większość tych publicznych stron internetowych pozwala na interakcję między podmiotem, a odbiorcami. W niektórych przypadkach strona zawiera jedynie informacje. W innych przypadkach za pośrednictwem strony internetowej można składać formularze w zakresie usług publicznych. W niektórych przypadkach strona internetowa jest środkiem przekazu dla transakcji biznesowych. Nieautoryzowana modyfikacja lub zniszczenie informacji mających wpływ na komunikację zewnętrzną (np. strony internetowe, poczta elektroniczna) może mieć negatywny wpływ na działalność lub zaufanie publiczne do podmiotu. W większości przypadków szkoda może zostać naprawiona w stosunkowo krótkim czasie, a szkoda jest ograniczona (poziom wpływu jest niski). W innych przypadkach (np. bardzo dużych transakcji oszukańczych lub modyfikacji strony internetowej należącej do podmiotu odpowiedzialnego za bezpieczeństwo publiczne), szkoda może mieć poważny wpływ na funkcjonowanie podmiotu lub zaufanie publiczne do niego. W takich przypadkach wpływ na integralność związany z nieuprawnioną modyfikacją lub zniszczeniem publicznej strony internetowej byłby co najmniej ***umiarkowany***.

Katastrofalna utrata dostępności systemu

Fizyczne lub logiczne zniszczenie głównych aktywów może skutkować bardzo dużymi wydatkami na ich odtworzenie lub długimi okresami czasu na ich odzyskanie. Stała utrata lub niedostępność funkcji systemu informatycznego może poważnie utrudnić działalność podmiotu, a w przypadku gdy w grę wchodzą bezpośrednie usługi na rzecz społeczeństwa,

może mieć poważny negatywny wpływ na zaufanie publiczne do podmiotów publicznych. Szczególnie w przypadku dużych systemów, kryteria NSC 199 sugerują, że katastroficzna utrata dostępności systemu może skutkować ***wysokim*** poziomem wpływu na dostępność. To, czy poziom wpływu dostępności systemu powinien być ***wysoki*** (a następnie ***wysoki*** poziom wpływu na bezpieczeństwo systemu), zależy raczej od innych czynników, takich jak koszty i krytyczność systemu, niż od poziomu wpływu na bezpieczeństwo typów informacji przetwarzanych przez system.

Duże systemy wspomagające i łączące

Duże lub złożone systemy informatyczne składające się z wielu podsystemów często wymagają dodatkowych rozważań dotyczących przydzielania kategorii bezpieczeństwa. Poniżej zostaną przedstawione wytyczne dotyczące stosowania i powiązania wyników kategoryzacji bezpieczeństwa poszczególnych systemów z podmiotu, dużymi infrastrukturami wsparcia (takimi jak ogólne systemy wsparcia technicznego, aplikacje hurtowni danych, duże magazyny danych, farmy serwerów i repozytoria informacji) oraz systemami, w których występują połączenia międzysystemowe.

Po określeniu kategorii bezpieczeństwa dla poszczególnych systemów informatycznych wchodzących w interakcję z dużymi systemami infrastruktury, informatycy i personel ochrony są w posiadaniu cennych informacji, które mogą teraz zapewnić przedsiębiorstwu szeroką perspektywę spojrzenia na bezpieczeństwo. Jednym z istotnych działań jest wprowadzenie ogólnej kategoryzacji bezpieczeństwa dla infrastruktur sieciowych wspomagających podmiot. Ponieważ sieci, podobnie jak inne ogólne systemy wspomagające, nie są z natury "własne", albowiem ich działanie nie wynika bezpośrednio z typów informacji związanych z zadaniami podmiotu lub funkcjami administracyjnymi albo funkcjami wspierającymi, kategoryzacja infrastruktury będzie wynikała z agregacji kategorii bezpieczeństwa poszczególnych systemów informatycznych. Innymi słowy, kategoryzacja bezpieczeństwa infrastruktury wynika z najwyższego wskaźnika wpływu obsługiwanych systemów informatycznych i opiera się na typach informacji przetwarzanych, przesyłanych lub przechowywanych w sieci lub ogólnym systemie wsparcia. Łącznie, ocena zagrożeń

w skali całego podmiotu i ocena bezpieczeństwa, uzyskana w wyniku agregacji, pozwoli podmiotowi spojrzeć na jej profil ryzyka z całościowego i zrównoważonego punktu widzenia. Ponadto, analiza ta zapewni właściwe stosowanie zabezpieczeń wspólnych wspierających wiele systemów informatycznych, a ochrona zapewniana przez te zabezpieczenia jest dziedziczona przez poszczególne systemy.

Infrastruktura krytyczna i zasoby usług kluczowych

W przypadku gdy zadania obsługiwane przez system informatyczny lub informacje przetwarzane przez ten system wpływają na bezpieczeństwo infrastruktury krytycznej lub zasobów usług kluczowych, szkoda wynikająca z kompromitacji informacji lub systemu informatycznego wymaga szczególnej uwagi. W takim przypadku wpływ na bezpieczeństwo może obejmować znaczne zmniejszenie skuteczności mechanizmów ochrony fizycznej lub cyberbezpieczeństwa, lub ułatwienie ataku terrorystycznego na infrastrukturę krytyczną i usługi kluczowe. W związku z tym należy starannie określić kategoryzację bezpieczeństwa systemu, jeżeli utrata poufności, integralności lub dostępności będzie miała negatywny wpływ na infrastrukturę krytyczną lub usługi kluczowe.

Sprawy dotyczące bezpieczeństwa infrastruktury krytycznej reguluje *ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*, a sprawy dotyczące bezpieczeństwa usług kluczowych *ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*.

Dane osobowe

Kwestie ochrony danych osobowych w podmiotach publicznych regulują przepisy *rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych*

Ponieważ większość przepisów dotyczących ochrony danych osobowych koncentruje się na dostępie, wykorzystywaniu, ujawnianiu lub udostępnianiu informacji, czynnik ochrony

danych osobowych traktowany jest w niniejszych wytycznych, jako odnoszący się do wpływu na poufność. Nie należy jednak zapominać, że ochronie podlegają także pozostałe atrybuty bezpieczeństwa. Ustalając poziomy wpływu na poufność dla każdego rodzaju informacji, podmioty muszą wziąć pod uwagę konsekwencje nieautoryzowanego ujawnienia informacji o danych osobowych (w odniesieniu do prawa powszechnego).

Podmioty są zobowiązane do przeprowadzenia Oceny Wpływu na Prywatność (*ang. Privacy Impact Assessment – PIA*) lub inaczej Ocenę Wpływu na Ochronę Danych Osobowych (*ang. Data Protection Impact Assessment – DPIA*) przed opracowaniem systemów informatycznych, które zawierają informacje umożliwiające identyfikację osób lub przed zebraniem informacji umożliwiających identyfikację osób drogą elektroniczną. Wpływ naruszeń ochrony danych osobowych powinien uwzględniać wszelkie negatywne skutki, jakich doświadczają osoby fizyczne lub organizacje w wyniku utraty poufności danych osobowych. Przykłady niepożądanych skutków, jakich doświadczają osoby fizyczne, mogą obejmować szantaż, kradzież tożsamości, dyskryminację lub emocjonalny niepokój danej osoby. Przykłady negatywnych skutków, jakich doświadczają organizacje, mogą obejmować obciążenia administracyjne, straty finansowe, utratę reputacji i zaufania publicznego oraz kary związane z naruszeniem odpowiednich przepisów.

Należy dokonać przeglądu kategoryzacji, aby upewnić się, że negatywne skutki utraty poufności danych osobowych zostały odpowiednio uwzględnione w ustaleniach wpływu. Poziom wpływu na poufność powinien zasadniczo mieścić się na poziomie ***umiarkowany***.

Tajemnice przedsiębiorcy

Przepisy *ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji* wyraźnie zabraniają nieuprawnionego ujawnienia tajemnic przedsiębiorcy. Systemom przechowującym, komunikującym się lub przetwarzającym tajemnice przedsiębiorcy zwykle przypisuje się co najmniej ***umiarkowany*** poziom wpływu na poufność.

4.4.3. CAŁKOWITY WPŁYW ZAKŁÓCENIA / INCYDENTU NA SYSTEMU INFORMATYCZNY

Ponieważ wartości oddziaływania (tj. poziomy) dotyczące poufności, integralności i dostępności nie zawsze są takie same dla wszystkich atrybutów bezpieczeństwa danego systemu informacyjnego, do określenia ogólnego poziomu oddziaływania incydentu / zakłócenia na system informatyczny stosuje się koncepcję "najwyższego znacznika ". Poziom wpływu na bezpieczeństwo systemu informatycznego będzie zasadniczo najwyższym poziomem wpływu na atrybuty bezpieczeństwa (poufność, integralność i dostępność) związane z zagregowanymi typami informacji w systemie. Zatem system o niskim wpływie definiuje się jako system informatyczny, w którym wszystkie trzy atrybuty bezpieczeństwa mają niskie oddziaływanie incydentu / zakłócenia. System o umiarkowanym wpływie to system informatyczny, w którym co najmniej jeden z atrybutów bezpieczeństwa ma umiarkowany wpływ incydentu / zakłócenia, a żaden z atrybutów bezpieczeństwa nie posiada większego poziomu wpływu niż umiarkowany. I wreszcie, system o wysokim wpływie to system informatyczny, w którym co najmniej jeden z atrybutów posiada poziom wpływu określony jako wysoki.

4.5. DOKUMENTOWANIE PROCESU KATEGORYZACJI BEZPIECZEŃSTWA

Niezbędne w procesie kategoryzacji bezpieczeństwa jest udokumentowanie badań, kluczowych decyzji i zatwierdzeń oraz wykazanie uzasadnienia kategoryzacji bezpieczeństwa systemu informatycznego. Informacje te mają kluczowe znaczenie dla cyklu życia bezpieczeństwa i będą musiały zostać uwzględnione w planie bezpieczeństwa systemu informatycznego.

Rysunek 3 przedstawia przykład szczegółowych informacji, które należy zebrać.

<table>
<tr><td colspan="4">Nazwa Systemu Informatycznego: System SCADA [Identyfikator stosowany w podmiocie]</td></tr>
<tr><td colspan="4">Biznes i misja wspierana: System SCADA (kontrola nadzorcza i pozyskiwanie danych) zapewnia kontrolę w czasie rzeczywistym i informacje wspierające w dużej elektrowni. Elektrownia zapewnia krytyczną dystrybucję energii elektrycznej do instalacji wojskowej.</td></tr>
<tr><td colspan="4">Typy Informacji</td></tr>
<tr><td>[B.7.1] Źródła Energii</td><td colspan="3">Dane z czujników monitorujących dostępność energii dla instalacji wojskowej oraz jej żołnierzy i organów dowodzenia. Funkcja ta obejmuje kontrolę dystrybucji i przekazywania mocy. Zdalne sterowanie SCADA może podejmować takie działania jak inicjowanie niezbędnych czynności przełączania w celu złagodzenia stanu przeciążenia mocy. Wpływ na te informacje i system SCADA może mieć wpływ na infrastrukturę krytyczną instalacji.</td></tr>
<tr><td>[A.2.8.12] Informacje ogólne</td><td colspan="3">System informatyczny SCADA przetwarza rutynowe informacje administracyjne.</td></tr>
<tr><td>Krok 1</td><td colspan="3">Krok 2 [wstępny] / Krok 3a [dostosowanie]</td></tr>
<tr><td rowspan="2">Identyfikacja typów informacji</td><td>Wpływ na poufność</td><td>Wpływ na integralność</td><td>Wpływ na dostępność</td></tr>
<tr><td colspan="3">Krok 3b- Uzasadnienie dostosowania skutków</td></tr>
<tr><td rowspan="2">Źródła Energii</td><td>Niski / Umiarkowany</td><td>Niski / Wysoki</td><td>Niski / Wysoki</td></tr>
<tr><td>Ujawnienie informacji z czujników może mieć poważny wpływ</td><td>Mogą wystąpić poważne konsekwencje w</td><td>Ze względu na utratę dostępności może nastąpić poważny</td></tr>
</table>

	na misję, jeżeli przeciwnikowi zostaną przekazane wskazania i ostrzeżenia dotyczące potencjału elektrowni.	przypadku, gdy niekorzystna modyfikacja informacji skutkuje nieprawidłowym sterowaniem systemu elektroenergetycznego lub działaniami kontrolnymi.	wpływ powodujący niezdolność realizacji zadań, co może mieć ogólne katastrofalne skutki dla infrastruktury krytycznej obiektu i może doprowadzić do utraty życia ludzkiego.
Informacje ogólne	Niski	Niski	Niski
	Brak zmian	Brak zmian	Brak zmian
Step 4 Kategoryzacja Systemu:	**Umiarkowany**	**Wysoki**	**Wysoki**
	Ogólny wpływ na system informatyczny: Wysoki		

Rysunek 3. Gromadzenie informacji dotyczących bezpieczeństwa w ramach kategoryzacji

Ponadto podmioty mogą rozważyć ulepszenie swoich planów bezpieczeństwa systemu (*ang. System Security Plan – SSP*) o inne analizy, decyzje, zadania lub zatwierdzenia, które wykorzystano w procesie kategoryzacji. Przykładowo mogą one obejmować:

- Obszar działalności podmiotu (krok 1 w tabeli 1);
- Kwestie legislacyjne mające wpływ na przypisanie lub dostosowanie wpływu informacji (sekcja 4.1.3);
- Wskazania wynikające krytycznego znaczenia czasowego w uzasadnieniu przypisywania poziomów wpływu na dostępność (sekcja 4.2.2.3);

- Uzasadnienie przypisywania informacji do ogólnego typu informacji (sekcja 4.1.2, Wskazówka dotycząca wdrażania);
- Wyniki przeglądów adekwatności tymczasowych poziomów wpływu na atrybuty bezpieczeństwa informacji (sekcja 4.3);
- Wyniki rozważenia potencjalnego wpływu na inne organizacje i rozważenia z przepisów ustawy o krajowym systemie cyberbezpieczeństwa i ustawy o zarządzaniu kryzysowym;
- Wyniki przeglądu zidentyfikowanych kategoryzacji bezpieczeństwa dla agregatu typów informacji (krok 4 w tabeli 1);
- Wpływ różnych czynników i okoliczności (np. Agregacja danych, krytyczna funkcjonalność systemu, dane osobowe, tajemnice przedsiębiorcy, infrastruktura krytyczna, agregacja, krytyczna funkcjonalność systemu, okoliczności łagodzące) na kategorię systemu (sekcja 4.4.2)
- Czy i dlaczego podmiot ustalił, że poziom wpływu systemu musi być wyższy niż którykolwiek z poziomów typów informacji przetwarzanych przez system (sekcja 4.4)
- Zatwierdzenia wszystkich ustaleń lub decyzji (krok 4 w tabeli 1)

4.6. WYKORZYSTANIE INFORMACJI O KATEGORYZACJI

Wyniki kategoryzacji bezpieczeństwa systemu mogą i powinny być wykorzystywane lub udostępniane odpowiednim pracownikom podmiotu w celu wspierania działań podmiotu, w tym:

- Analizę wpływu na działalność (BIA): Personel podmiotu powinien rozważyć wykorzystanie kategoryzacji bezpieczeństwa systemów informatycznych i informacji przy analizie BIA Wzajemne czerpanie informacji umożliwi właściwą ocenę wymagań bezpieczeństwa dla systemu informatycznego. Sprzeczne informacje i nietypowe warunki wynikające z każdej z tych analiz, takie jak na przykład określenie wpływu incydentu na dostępność jako niski, przy jednoczesnym wymogu w BIA polegającym

na trzygodzinnym czasie odzyskiwania, powinny spowodować ponowną ocenę zarówno analizy wpływu incydentu, jak i analizy BIA.

- Planowanie kapitału i kontrola inwestycji (CPIC) i architektura korporacyjna (EA): Podobnie jak nie należy dokonywać żadnych inwestycji IT bez architektury zatwierdzonej przez osoby odpowiedzialne za realizację zadań podmiotu, tak kategoryzacja bezpieczeństwa, która rozpoczyna cykl życia bezpieczeństwa, jest z działalnością umożliwiającą właściwe decyzje dotyczące nowych inwestycji, a także decyzje dotyczące migracji i aktualizacji. W szczególności kategoryzacja zabezpieczeń może stanowić solidną podstawę uzasadnienia niektórych wydatków kapitałowych, ale także może zapewnić wkład analityczny w celu uniknięcia niepotrzebnych inwestycji.

- Projektowanie systemu: Zrozumienie i zaprojektowanie architektury systemu z uwzględnieniem różnych poziomów wrażliwości informacji może pomóc w osiągnięciu podmiotowi korzyści dzięki efektowi skali dzięki wspólnym strefom i usługom bezpieczeństwa. Na przykład system informatyczny zawierający informacje o danych osobowych może znajdować się w jednej strefie bezpieczeństwa z innymi systemami informatycznymi zawierającymi podobnie wrażliwe informacje. W innym przypadku każda strefa może mieć różne poziomy bezpieczeństwa. Przykładowo, bardziej krytyczne strefy mogą wymagać uwierzytelnienia 3-czynnikowego, podczas gdy strefa ogólnodostępna może wymagać jedynie prostej kontroli dostępu. Tego rodzaju podejście wymaga dokładnego zrozumienia informacji podmiotu i typów danych uzyskanych w procesie kategoryzacji bezpieczeństwa.

- Planowanie na wypadek awarii i odzyskiwania po awarii: Personel ds. Planowania na wypadek awarii i odzyskiwania po awarii powinien dokonać przeglądu systemów informatycznych, które mają wiele rodzajów danych o różnych poziomach wpływu i rozważyć grupowanie aplikacji o podobnych poziomach wpływu na system informacyjny z odpowiednio chronioną infrastrukturą. Zapewnia to skuteczne stosowanie prawidłowych zabezpieczeń na wypadek awarii i ochrony przed

katastrofami oraz pozwala uniknąć nadmiernej ochrony systemów informatycznych o mniejszym wpływie.

- Umowy dotyczące wymiany informacji i wzajemnych połączeń systemowych: Podczas oceny połączeń pomiędzy systemami różnych podmiotów personel należy wykorzystać zarówno zagregowane, jak i indywidualne informacje o kategoryzacji bezpieczeństwa. Na przykład wiedza o tym, że informacje przetwarzane w systemie informacyjnym o dużym wpływie płyną do systemu informacyjnego o średnim wpływie innego podmiotu, powinna spowodować, że oba podmioty jednolicie ocenią informacje dotyczące kategoryzacji bezpieczeństwa, wdrożone lub wynikające z nich zabezpieczenia oraz ryzyko związane z połączenia systemów. Wyniki tej oceny mogą uzasadniać potrzebę dodatkowych zabezpieczeń w postaci umowy o gwarantowanym poziomie usług, aktualizacji systemów informatycznych, dodatkowych zabezpieczeniach ograniczających ryzyko lub alternatywnych sposobów udostępniania wymaganych informacji.

ZAŁĄCZNIK A REFERENCJE

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA	
NSC 199	Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199
NSC 200	Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych – na podstawie FIPS 200
NSC 800-53	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 800-53 MAP	Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 Patrz: SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)
NSC 800-60	Wytyczne w zakresie określania kategorii bezpieczeństwa informacji I kategorii bezpieczeństwa systemu informatycznego – na podstawie NIST SP 800-60

STANDARDS, AND GUIDELINES	
FIPS 199	*Standards for Security Categorization of Federal Information and Information Systems*, February 2004
FIPS 200	*Minimum Security Requirements for Federal Information and Information Systems*, March 2006
NIST SP 800-18	*Guide for Developing Security Plans for Federal Information Systems*, February 2006
NIST SP 800-30	*Risk Management Guide for Information Technology Systems*, July 2002
NIST SP 800-34	*Contingency Planning Guide for Information Technology Systems*, June 2002
NIST SP 800-37	*Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004
NIST SP 800-39	*Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011
NIST SP 800-53	*Security and Privacy Controls for Information Systems and Organizations*, September 2020
NIST SP 800-53A	*Guide for Assessing the Security Controls in Federal Information Systems*, December 2014
NIST SP 800-59	*Guideline for Identifying an Information System as a National Security System*, August 2003
NIST SP 800-64	*Security Considerations in the Information System Development Life Cycle*, June 2004.