NSC NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA	Narodowy Standard Cyberbezpieczeństwa		
Nazwa standardu	Symbol	Wersja	Data wydania
Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne	**NSC 800-30**	1.0	15/02/2022

PRZEWODNIK DOTYCZĄCY POSTĘPOWANIA W ZAKRESIE SZACOWANIA RYZYKA W PODMIOTACH REALIZUJĄCYCH ZADANIA PUBLICZNE

PEŁNOMOCNIK RZĄDU DS. CYBERBEZPIECZEŃSTWA
Warszawa 2022

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 800-18, Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych – na podstawie NIST SP 800- 18;

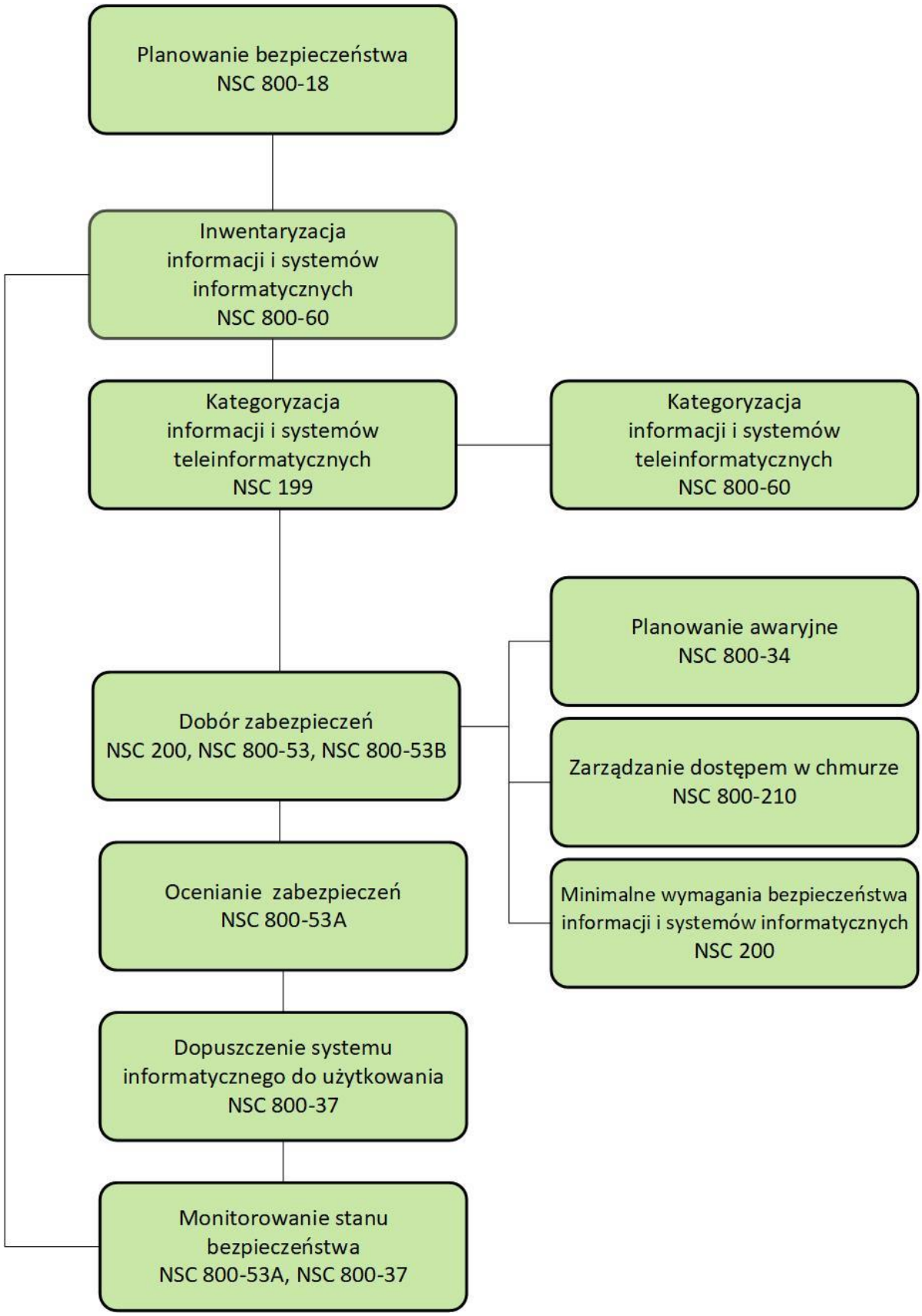
[1] Wymienione są podstawowe dokumenty. Każdy z nich może się odwoływać w rozdziale *Referencje* do szeregu powiązanych publikacji, które składają się na całościowy proces osiągania cyberbezpieczeństwa.

[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 800-39, Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informatycznego – na podstawie NIST SP 800-39;
- NSC 800-53, Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji – na podstawie NIST SP 800-53;
- NSC 800-53A, Ocena środków bezpieczeństwa i ochrony prywatności systemów informatycznych oraz organizacji. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A;
- NSC 800-53B, Zabezpieczenia bazowe systemów informatycznych oraz organizacji – na podstawie NIST SP 800-53B;
- NSC 800-60, Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego – na podstawie NIST SP 800-60;
- NSC 800-61, Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego – na podstawie NIST SP 800-61;
- NSC 800-210, Ogólne wytyczne dotyczące kontroli dostępu do systemów chmury obliczeniowej – na podstawie NIST SP 800-210.

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

Cykl zarządzania bezpieczeństwem bazujący na publikacjach NIST wykorzystuje następujące dokumenty:


Planowanie bezpieczeństwa
NSC 800-18
Inwentaryzacja informacji i systemów informatycznych
NSC 800-60
Kategoryzacja informacji i systemów teleinformatycznych
NSC 199
Kategoryzacja informacji i systemów teleinformatycznych
NSC 800-60
Dobór zabezpieczeń
NSC 200, NSC 800-53, NSC 800-53B
Planowanie awaryjne
NSC 800-34
Zarządzanie dostępem w chmurze
NSC 800-210
Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych
NSC 200
Ocenianie 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. Cyberbezpiecze ństwa.

Niniejsza publikacja, ***Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne***, opracowana została za zgodą National Institute of Science and Technology (NIST) na podstawie specjalnej publikacji NIST SP 800-30 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

Spis ilustracji

Spis tabel

ROZDZIAŁ 1 WPROWADZENIE

W celu realizacji celów działania i funkcji biznesowych, podmioty[3] w sektorze publicznym i prywatnym są uzależnione od technologii[4] i systemów informatycznych[5]. Systemy informatyczne mogą obejmować bardzo zróżnicowane instalacje, od sieci biurowych, systemów finansowych i kadrowych po bardzo wyspecjalizowane systemy (np. systemy sterowania przemysłowego/procesowego, systemy broni, systemy telekomunikacyjne i systemy kontroli środowiska). Z uwagi na występujące podatności systemy informatyczne są narażone na skutki poważnych zagrożeń, które mogą mieć negatywny wpływ na działalność organizacji i jej aktywa, osoby fizyczne, inne organizacje i społeczeństwo poprzez naruszenie atrybutów bezpieczeństwa w postaci poufności, integralności lub dostępności informacji przetwarzanych, przechowywanych lub przekazywanych przez te systemy. Zagrożenia dla systemów informatycznych mogą obejmować ataki celowe, zakłócenia środowiskowe, błędy ludzkie/maszynowe oraz awarie strukturalne i mogą prowadzić do szkód dla bezpieczeństwa narodowego i gospodarczego Polski. Dlatego konieczne jest, aby liderzy i menedżerowie wszystkich szczebli rozumieli swoje obowiązki i byli odpowiedzialni za zarządzanie ryzykiem związanym z bezpieczeństwem informacji, czyli ryzykiem związanym z funkcjonowaniem i korzystaniem z systemów informatycznych, które wspierają cel i funkcje biznesowe ich podmiotów.

Szacowanie ryzyka jest jednym z podstawowych elementów procesu zarządzania ryzykiem w podmiocie, opisanym w publikacji NSC 800-39. Szacowanie ryzyka wynikającego z funkcjonowania i korzystania z systemów informatycznych, jest wykorzystywane do jego identyfikacji, oceny i ustalania priorytetów ryzyka związanego z działalnością organizacji (tj. celem, funkcjami, wizerunkiem i reputacją), jej zasobami, osobami, innymi organizacjami i społeczeństwem. Celem szacowania ryzyka jest informowanie decydentów i wspieranie

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

[4] Organizacje zarządzają również technologią informacyjną w ramach wspólnej infrastruktury, zbioru wspólnych usług oraz zestawu zabezpieczeń wspólnych.

[5] Określony zestaw zasobów utworzonych w celu gromadzenia, przetwarzania, konserwacji, użytkowania, udostępniania, rozpowszechniania lub usuwania informacji.

reakcji na ryzyko poprzez identyfikację: (i) istotnych zagrożeń dla podmiotu lub zagrożeń skierowanych przez podmiot przeciwko innym podmiotom; (ii) słabych punktów zarówno wewnętrznych, jak i zewnętrznych w stosunku do organizacji; (iii) wpływu (tj. szkody) na organizacje, który może wystąpić, biorąc pod uwagę możliwość wystąpienia zagrożeń wykorzystujących słabe punkty; oraz (iv) prawdopodobieństwa wystąpienia szkody. Końcowym wynikiem jest określenie poziomu ryzyka (tj. zazwyczaj funkcji stopnia szkodliwości (straty) i prawdopodobieństwa wystąpienia straty). Szacowanie ryzyka można przeprowadzić na wszystkich trzech poziomach w hierarchii zarządzania ryzykiem, w tym na poziomie 1 (poziom organizacji), 2 (poziom procesu celu/podmiotu) i 3 (poziom systemu informatycznego). Na poziomie 1 i 2 organizacje wykorzystują szacowanie ryzyka do oceny, na przykład, ryzyka związanego z bezpieczeństwem informacji systemowych, z zarządzaniem organizacją i jej działalnością, procesami biznesowymi, architekturą korporacyjną lub finansowaniem programów bezpieczeństwa informacji. Na poziomie 3 organizacje wykorzystują szacowanie ryzyka do skuteczniejszego wspierania wdrażania Ram Zarządzania Ryzykiem (*ang. Risk Management Framework – RMF)*[6] tj. kategoryzacji bezpieczeństwa; wyboru, wdrażania i oceny zabezpieczeń systemu informatycznego i zabezpieczeń wspólnych oraz monitorowania zabezpieczeń[7].

1.1. Cel i zastosowanie

Celem publikacji NSC 800-30 jest dostarczenie wskazówek dotyczących przeprowadzania szacowania ryzyka systemów informatycznych podmiotów realizujących zadania publiczne, które zostały rozszerzone w dokumencie NSC 800-39. Szacowanie ryzyka, przeprowadzane na wszystkich trzech poziomach w hierarchii zarządzania ryzykiem, stanowi część ogólnego procesu zarządzania ryzykiem, dostarczając kierownikom wyższego szczebla informacji niezbędnych do określenia odpowiednich kierunków działań w odpowiedzi na zidentyfikowane ryzyka. W szczególności niniejszy dokument zawiera wskazówki dotyczące

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

[7] Ramy Zarządzania Ryzykiem opisane są w publikacji NSC 800-37.

przeprowadzania każdego z etapów procesu szacowania ryzyka (tj. przygotowania do szacowania, przeprowadzenia szacowania, przekazania wyników szacowania oraz utrzymania szacowania) oraz sposobu, w jaki szacowanie ryzyka i inne procesy zarządzania ryzykiem w podmiocie uzupełniają się i wzajemnie się wspomagają. Publikacja NSC 800-30 zawiera również wytyczne dla organizacji dotyczące identyfikacji konkretnych czynników ryzyka, które należy na bieżąco monitorować tak, aby podmioty mogły określić, czy ryzyko wzrosło do niedopuszczalnego poziomu (tj. czy przekroczyło poziom tolerancji ryzyka organizacyjnego) i aby można było podjąć różne działania w celu jego obniżenia.

Wytyczne zawarte w niniejszej publikacji powinny mieć zastosowanie do wszystkich systemów informatycznych podmiotów realizujących zadania publiczne innych niż systemy podlegające regulacji wynikających z ustawy o ochronie informacji niejawnych.

1.2. Grupa docelowa

Niniejsza publikacja ma na celu służyć zróżnicowanej grupie specjalistów w zakresie zarządzania ryzykiem[8], w tym:

- osobom pełniącym funkcje nadzorcze w zakresie zarządzania ryzykiem (np. ministrowie, kierownicy urzędów, dyrektorzy generalni, dyrektorzy komórek organizacyjnych urzędów, funkcje wykonawcze ds. ryzyka (*ang. risk executive (function) -RE*), kierownicy jednostek organizacyjnych (*ang. head of agencies - HA*);
- osobom odpowiedzialnym za realizację celów organizacyjnych/funkcji biznesowych (np. właściciele misji lub procesów biznesowych (*ang. mission* or *business owner - BO*), właściciele informacji/władający informacją (*ang. Information owner* or *steward – IO/S)*, osoby autoryzujące (*ang. authorizing officias – AO*);
- osobom odpowiedzialnym za nabywanie produktów, usług lub systemów informatycznych (np. pracownicy ds. zamówień publicznych);

[8] Definicje stanowisk i ról – patrz: NSC 800-37; NSC 800-39; NSC 7298.

- osobom odpowiedzialnym za projektowanie, rozwój i wdrażanie systemów informatycznych/techniki bezpieczeństwa (np. kierownicy programów, architekci korporacyjni, architekci bezpieczeństwa informacji, inżynierowie systemów informatycznych/techniki bezpieczeństwa, integratorzy systemów informatycznych);
- osobom mającym nadzór nad bezpieczeństwem informacji, wykonującym obowiązki zarządcze i operacyjne (np. *chief information officer – CIO, senior information security oficer – SISO*[9], właściciele systemów informatycznych, dostawcy zabezpieczeń wspólnych);
- osobom odpowiedzialnym za bezpieczeństwo informacji/ocenę ryzyka i monitorowanie (np. osoby oceniające system, pentesterzy, osoby oceniające zabezpieczenia, osoby oceniające ryzyko, niezależni weryfikatorzy/walidatorzy, kontrolerzy państwowi, audytorzy).

1.3. Publikacje powiązane

Pojęcia i zasady związane z procesami i podejściami do oceny ryzyka zawartymi w niniejszej publikacji są podobne i spójne z procesami i podejściami opisanymi w normach Międzynarodowej Organizacji Normalizacyjnej (ISO)[10] i Międzynarodowej Komisji Elektrotechnicznej (IEC)[11]. Rozszerzenie koncepcji i zasad tych międzynarodowych standardów na podmioty realizujące zadania publiczne i ich wykonawców oraz promowanie ponownego wykorzystywania wyników szacowania ryzyka, zmniejsza obciążenie organizacji, które muszą spełniać normy ISO/IEC.

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

[10] Patrz: https://www.iso.org/home.html

[11] Patrz: https://www.iso.org/organization/70.html

Powiązania:

- NSC 800-39, Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informatycznego[12];
- NSC 800-37, Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu;
- NSC 800-53, Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji;
- NSC 800-53A, Ocenianie środków bezpieczeństwa i ochrony prywatności w systemach informatycznych podmiotów publicznych.

1.4. Struktura publikacji

Publikacja jest zorganizowana w następujący sposób:

- Rozdział pierwszy: (i) wprowadzenie; (ii) cel i zastosowanie; (iii) grupa docelowa; (iv) publikacje związane.
- Rozdział drugi opisuje: (i) proces zarządzania ryzykiem oraz sposób, w jaki szacowanie ryzyka stanowią integralną część tego procesu; (ii) podstawową terminologię stosowaną przy przeprowadzaniu szacowania ryzyka; oraz (iii) sposób, w jaki szacowanie ryzyka może być stosowane na wszystkich szczeblach zarządzania ryzykiem w organizacji (tj. na poziomie organizacji, na poziomie celu/procesu biznesowego oraz na poziomie systemu informatycznego).
- W rozdziale trzecim opisano proces szacowania ryzyka dla bezpieczeństwa informacji, w tym: (i) ogólny zarys procesu szacowania ryzyka; (ii) działania niezbędne do przygotowania się do szacowania ryzyka; (iii) działania niezbędne do przeprowadzenia szacowania ryzyka; (iv) działania niezbędne do przekazywania wyników szacowania

[12] NSC 800-39 jest kontynuacją NSC 800-30, stanowiąc podstawowe źródło wytycznych dotyczących zarządzania ryzykiem w zakresie bezpieczeństwa informacji.

ryzyka i wymiany informacji na temat ryzyka w całej organizacji; oraz (v) działania niezbędne do utrzymania wyników szacowania ryzyka.

- Załączniki zawierają dodatkowe informacje dotyczące szacowania ryzyka, w tym: (i) referencje; (ii) słownik; (iii) akronimy; (iv) źródła zagrożeń; (v) zdarzenia zagrożenia; (vi) podatności i predyspozycje; (vii) prawdopodobieństwo wystąpienia zdarzenia zagrożenia; (viii) wpływ na organizację; (ix) określenie ryzyka; (x) informowanie o reakcji na ryzyko; (xi) podstawowe informacje do sprawozdań z szacowania ryzyka; oraz (xii) podsumowanie zadań związanych z szacowaniem ryzyka.

Słownik terminów i wyjaśnienie akronimów stanowi odrębną publikację NSC 7298.

ROZDZIAŁ 2 PODSTAWOWE POJĘCIA ZWIĄZANE Z SZACOWANIEM RYZYKA

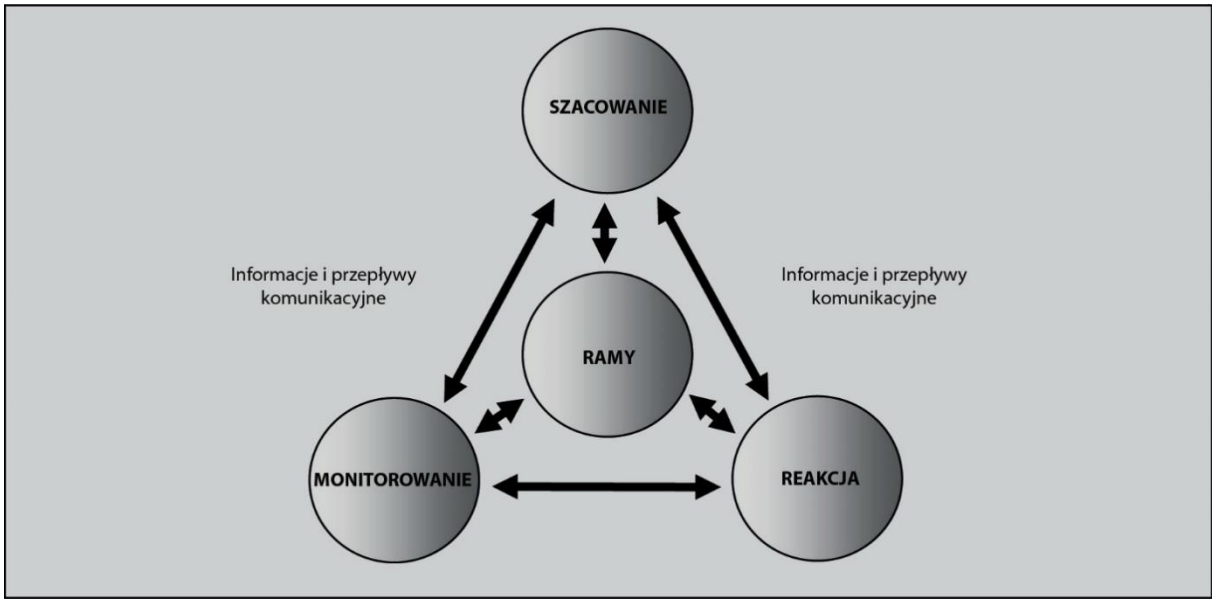
W niniejszym rozdziale opisano podstawowe pojęcia związane z szacowaniem ryzyka dla bezpieczeństwa informacji w podmiocie, w tym: (i) ogólny zarys procesu zarządzania ryzykiem oraz roli, jaką odgrywa w tym procesie szacowanie ryzyka; (ii) podstawowe pojęcia stosowane przy przeprowadzaniu szacowania ryzyka; oraz (iii) sposób, w jaki szacowanie ryzyka może być stosowane na wszystkich szczeblach zarządzania ryzykiem w podmiocie[13].

2.1. Proces zarządzania ryzykiem

Szacowanie ryzyka jest kluczowym elementem całościowego, obejmującego całą organizację procesu zarządzania ryzykiem, określonego w publikacji NSC 800-39, Zarządzanie ryzykiem związanym z bezpieczeństwem informacji. Organizacja, cel i przegląd systemu informatycznego. Procesy zarządzania ryzykiem obejmują: (i) ustanowienie kontekstu ryzyka; (ii) szacowanie ryzyka; (iii) postępowanie z ryzykiem; oraz (iv) monitorowanie ryzyka. Rysunek 1 ilustruje cztery etapy procesu zarządzania ryzykiem – w tym etap szacowania ryzyka oraz przepływy informacji i komunikacji niezbędne do skutecznego funkcjonowania procesu[14].

[13] NSC 800-39 zawiera wytyczne dotyczące trzech poziomów w hierarchii zarządzania ryzykiem, w tym poziomu 1 (organizacja), poziomu 2 (cel/proces biznesowy) i poziomu 3 (system informatyczny).

[14] Wiele wyników uzyskanych na etapie określania ryzyka stanowi istotny wkład w fazę oceny ryzyka i związany z nią proces oceny ryzyka. Należą do nich na przykład: strategia zarządzania ryzykiem, tolerancja ryzyka organizacyjnego, metodologia oceny ryzyka, założenia, ograniczenia oraz priorytety celów/zadań biznesowych.



Rysunek 1. Proces zarządzania ryzykiem.

Pierwszy komponent zarządzania ryzykiem dotyczy sposobu, w jaki organizacje określają *ramy ryzyka* lub ustanawiają kontekst ryzyka - czyli opisują środowisko, w którym podejmowane są decyzje oparte na ryzyku. Celem tego komponentu jest stworzenie *strategii zarządzania ryzykiem*, która odnosi się do tego, jak organizacje zamierzają oceniać ryzyko, reagować na ryzyko i monitorować ryzyko, czyniąc jasnym i przejrzystym postrzeganie ryzyka, które organizacje rutynowo wykorzystują przy podejmowaniu decyzji inwestycyjnych i operacyjnych. Strategia zarządzania ryzykiem stanowi podstawę zarządzania ryzykiem i wyznacza w podmiocie granice dla decyzji opartych na ryzyku[15].

Drugi komponent zarządzania ryzykiem dotyczy sposobu, w jaki podmioty szacują ryzyko w kontekście ram ryzyka organizacyjnego. Celem komponentu szacowania ryzyka jest identyfikacja: (i) zagrożeń dla danego podmiotu (tj. jego operacji, aktywów lub osób) lub zagrożeń skierowanych za pośrednictwem danego podmiotu przeciwko innym podmiotom

[15] W przypadku braku jednoznacznej lub formalnej strategii zarządzania ryzykiem organizacyjnym, można wykorzystać zasoby organizacyjne (np. narzędzia, repozytoria danych) i odniesienia (np. przykładowe raporty z oceny ryzyka), aby rozeznać te aspekty podejścia organizacji do zarządzania ryzykiem, które mają wpływ na ocenę ryzyka.

lub społeczeństwu; (ii) podatności wewnętrznych i zewnętrznych w stosunku do podmiotu [16]; (iii) straty/szkody (tj. niekorzystnego wpływu), która może zajść ze względu na możliwość wystąpienia zagrożeń wykorzystujących podatności; oraz (iv) prawdopodobieństwa wystąpienia straty/szkody. Efektem końcowym jest określenie ryzyka (zazwyczaj jest to funkcja stopnia szkodliwości i prawdopodobieństwa wystąpienia straty/szkody).

Trzeci element zarządzania ryzykiem dotyczy sposobu, w jaki podmioty reagują na ryzyko po jego określeniu na podstawie wyników szacowania ryzyka. Celem komponentu reakcji na ryzyko, zwanego też postępowaniem z ryzykiem, jest zapewnienie spójnej, obejmującej cały podmiot reakcji na ryzyko, zgodnie z ramami ryzyka organizacyjnego przez: (i) opracowanie alternatywnych sposobów reagowania na ryzyko; (ii) ocenę alternatywnych sposobów działania; (iii) określenie odpowiednich sposobów działania zgodnych z przyjętą w podmiocie tolerancją ryzyka; oraz (iv) wdrożenie reakcji na ryzyko w oparciu o wybrane sposoby działania.

Czwarty element zarządzania ryzykiem dotyczy sposobu, w jaki podmioty monitorują ryzyko w czasie. Celem komponentu monitorowania ryzyka jest: (i) określenie bieżącej skuteczności reakcji na ryzyko (zgodnie z ramami ryzyka przyjętymi w podmiocie); (ii) określenie zmian wpływających na ryzyko w systemach informatycznych organizacji i środowiskach, w których systemy te działają[17] oraz (iii) sprawdzenie, czy planowane reakcje na ryzyko są wdrażane i czy spełnione są wymagania dotyczące bezpieczeństwa informacji wynikające z celu/misji działania podmiotu/funkcji biznesowych, przepisów prawa, zasad, norm i wytycznych.

[16] Podatności organizacyjne nie ograniczają się do systemów informatycznych, ale mogą obejmować na przykład podatności w strukturach zarządzania, zadaniach/procesach biznesowych, architekturze korporacyjnej, architekturze bezpieczeństwa informacji, obiektach, sprzęcie, procesach cyklu życia systemu, działaniach w ramach łańcucha dostaw i wśród zewnętrznych dostawców usług.

[17] Środowiska operacyjne obejmują, ale nie ograniczają się do: przestrzeni zagrożeń; podatności; misji/funkcji biznesowych; procesów misji/biznesu; architektur bezpieczeństwa korporacyjnego i informacyjnego; technologii informacyjnych; personelu; obiektów; relacji w łańcuchu dostaw; zarządzania/kultury organizacyjnej; procesów zamówień publicznych/nabywania; polityk / procedur organizacyjnych; założeń organizacyjnych, ograniczeń, tolerancji ryzyka i priorytetów/kompromisów).

2.2. Szacowanie ryzyka

Niniejsza publikacja koncentruje się na elemencie szacowania ryzyka w zarządzaniu ryzykiem, zapewniając podmiotom stopniowy proces tego szacowania: (i) jak przygotować się do szacowania ryzyka; (ii) jak przeprowadzić szacowanie ryzyka; (iii) jak przekazać wyniki szacowania ryzyka kluczowemu personelowi podmiotu; oraz (iv) jak utrzymać szacowanie ryzyka w czasie. Szacowanie ryzyka nie jest jednorazowym działaniem, które dostarcza decydentom stałych i ostatecznych informacji w celu ukierunkowania i poinformowania ich o zagrożeniach dla bezpieczeństwa informacji. Organizacje powinny przeprowadzać szacowanie ryzyka na bieżąco przez cały cykl życia systemu i na wszystkich szczeblach hierarchii zarządzania ryzykiem – z częstotliwością szacowania ryzyka i zasobami stosowanymi podczas tych szacowań, proporcjonalnie do wyraźnie określonego celu i zakresu.

Szacowanie ryzyka dotyczy potencjalnego negatywnego wpływu na działalność i aktywa podmiotu, osoby fizyczne, inne podmioty oraz interesy gospodarcze i bezpieczeństwo narodowe, wynikającego z działania i korzystania z systemów informatycznych oraz informacji przetwarzanych[18] przez te systemy. Podmioty realizujące zadania publiczne przeprowadzają szacowanie ryzyka w celu określenia ryzyka wspólnego dla głównych celów/funkcji biznesowych podmiotu, procesów biznesowych, segmentów misyjnych/biznesowych, wspólnej infrastruktury/usług wspierających lub systemów informatycznych.

Szacowanie ryzyka może stanowić wsparcie dla wielu różnych decyzji i działań opartych na ryzyku, podejmowanych przez personel organizacyjny na wszystkich trzech poziomach hierarchii zarządzania ryzykiem, w tym m.in:

- opracowanie architektury bezpieczeństwa informacji;

[18] Wszelkie operacje wykonywane w odniesieniu do informacji i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie.

- określenie wymogów dotyczących połączeń międzysystemowych dla systemów informatycznych (w tym systemów wspierających procesy biznesowe i wspólną infrastrukturę/usługi wsparcia);
- projektowanie rozwiązań w zakresie bezpieczeństwa dla systemów informatycznych i środowisk pracy, w tym dobór zabezpieczeń, produktów informatycznych, łańcucha dostaw, dostawców i wykonawców;
- autoryzację (lub odmowę autoryzacji) do korzystania z systemów informatycznych lub do stosowania zabezpieczeń odziedziczonych przez te systemy (tj. zabezpieczeń wspólnych);
- modyfikację celów/funkcji biznesowych i/lub procesów biznesowych na stałe lub na określony czas (np. do czasu usunięcia nowo odkrytego zagrożenia lub podatności na zagrożenia, do czasu zastąpienia zabezpieczenia kompensacyjnego/tymczasowego);
- wdrażanie rozwiązań w zakresie bezpieczeństwa (np. czy określone produkty technologii informatycznej lub konfiguracje tych produktów spełniają ustalone wymagania);
- obsługę i konserwację rozwiązań zabezpieczających (np. strategie i programy ciągłego monitorowania, bieżące autoryzacje).

Ponieważ cele działania podmiotów i funkcje biznesowe, wspierające misje/procesy biznesowe, systemy informatyczne, zagrożenia i środowiska działania zmieniają się w czasie, zasadność i użyteczność każdego szacowania ryzyka jest ograniczona w czasie.

2.3. Kluczowe pojęcia dotyczące ryzyka

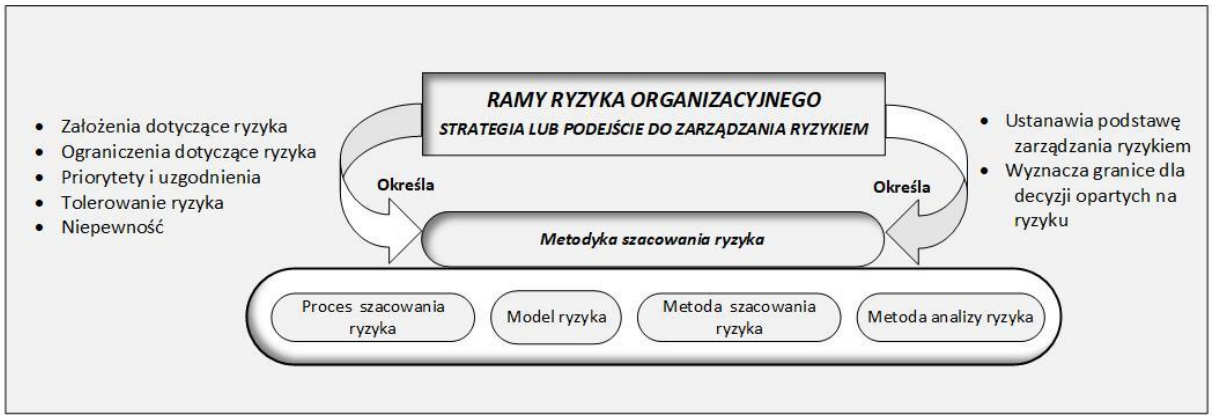
Ryzyko jest miarą stopnia, w jakim podmiot jest zagrożony potencjalną okolicznością lub zdarzeniem i zazwyczaj jest funkcją: (i) niekorzystne skutki, które wystąpiłyby w przypadku zaistnienia danej okoliczności lub zdarzenia; oraz (ii) prawdopodobieństwo ich wystąpienia. Zagrożenia dla bezpieczeństwa informacji to zagrożenia, które wynikają z utraty poufności, integralności lub dostępności informacji lub dostępności systemów informatycznych i odzwierciedlają potencjalny negatywny wpływ na działalność podmiotu (tj. cel, funkcje, wizerunek lub reputację), zasoby organizacyjne, osoby, inne organizacje i społeczeństwo. Szacowanie ryzyka jest procesem identyfikacji, oceny i ustalania priorytetów ryzyka

związanego z bezpieczeństwem informacji. Szacowanie ryzyka wymaga starannej analizy informacji o zagrożeniach i podatnościach na zagrożenia w celu określenia stopnia, w jakim okoliczności lub zdarzenia mogą mieć negatywny wpływ na podmiot oraz prawdopodobieństwa wystąpienia takich okoliczności lub zdarzeń.

Metodyka szacowania ryzyka zwykle obejmuje: (i) proces szacowania ryzyka (opisany w rozdziale trzecim); (ii) model konkretnego znanego ryzyka, definiujący kluczowe terminy i możliwe do oceny czynniki ryzyka oraz ich związki; (iii) metodę szacowania (np. ilościową, jakościową lub pół-jakościową), określającą zakres wartości, jakie czynniki ryzyka mogą przyjąć podczas szacowania ryzyka oraz sposób identyfikowania/analizy kombinacji czynników ryzyka, tak aby wartości tych czynników można było funkcjonalnie połączyć w celu dokonania szacowania; oraz (iv) metodę analizy (np. zorientowaną na zagrożenie, zorientowaną na wpływ na aktywa lub zorientowaną na podatność na zagrożenia), opisujące sposób identyfikacji/analizy kombinacji czynników ryzyka w celu zapewnienia odpowiedniego pokrycia przestrzeni problemowej na stałym poziomie szczegółowości. Metodyki szacowania ryzyka są definiowane przez podmiot i stanowią element celów zarządzania ryzykiem opracowanej na etapie definiowania ryzyka w procesie zarządzania ryzykiem[19].

Rysunek 2 ilustruje podstawowe komponenty w ramach ryzyka organizacyjnego oraz relacje pomiędzy tymi komponentami.

[19] Metodyka szacowania ryzyka jest w dużej mierze uzależniona od strategii zarządzania ryzykiem w organizacji. Metodyka szacowania ryzyka może być jednak dostosowana do każdej oceny ryzyka w oparciu o cel i zakres oceny oraz specyficzne czynniki, które organizacje decydują się wprowadzić w odniesieniu do procesu oceny ryzyka, modelu ryzyka, podejścia do oceny i analizy.



Rysunek 2. Związek pomiędzy komponentami tworzącymi ramy zarządzania ryzykiem.

Podmioty mogą korzystać z jednej metodyki szacowania ryzyka lub mogą stosować wiele metodyk, przy czym wybór konkretnej metodyki zależy na przykład od tego, czy jest ona odpowiednia do: (i) ram czasowych dla planowania inwestycji lub zmian polityki planowania; (ii) złożoność/dojrzałość celu organizacji/procesów biznesowych (w podziale na segmenty architektury korporacyjnej); (iii) fazy w cyklu życia systemów informatycznych; lub (iv) krytyczność/wrażliwość[20] systemów informatycznych wspierających podstawowe cele podmiotu/funkcje biznesowe. Dzięki jednoznacznemu określeniu modelu ryzyka, podejścia do oceny i zastosowanej metody analizy oraz wymaganiu, jako części procesu oceny, uzasadnienia dla ocenianych wartości czynników ryzyka, organizacje mogą zwiększyć odtwarzalność i powtarzalność ocen ryzyka[21].

2.3.1. Modele ryzyka

Modele ryzyka określają czynniki ryzyka, które mają być oceniane oraz relacje pomiędzy tymi czynnikami[22]. Czynniki ryzyka są cechami wykorzystywanymi w modelach ryzyka, jako dane

[20] Publikacja NSC 800-60 omawia kwestie związane z krytycznością i wrażliwością informacji w odniesieniu do kategoryzacji bezpieczeństwa.

[21] Odtwarzalność odnosi się do zdolności różnych ekspertów do uzyskania takich samych wyników na podstawie tych samych danych. Powtarzalność odnosi się do zdolności do powtórzenia oceny w przyszłości, w sposób, który jest spójny, a więc porównywalny z wcześniejszymi ocenami - umożliwiając organizacji identyfikację zachodzących trendów.

[22] Dokumentacja modelu ryzyka obejmuje: (i) identyfikację czynników ryzyka (definicje, opisy, skale wartości); oraz (ii) identyfikację relacji pomiędzy tymi czynnikami ryzyka (zarówno relacji pojęciowych, przedstawionych w sposób opisowy, jaki algorytmów łączenia wartości). Model ryzyka przedstawiony w tym rozdziale (i opisany w załącznikach D-I) nie określa algorytmów łączenia wartości.

wejściowe do określenia poziomów ryzyka w szacowaniu ryzyka. Czynniki ryzyka są również szeroko stosowane w komunikatach o ryzyku, aby podkreślić, co silnie wpływa na poziom ryzyka w konkretnych sytuacjach, okolicznościach lub kontekstach. Typowe czynniki ryzyka obejmują zagrożenie, podatność (wrażliwość), wpływ, prawdopodobieństwo i stan predyspozycji. Czynniki ryzyka mogą być rozłożone na bardziej szczegółowe charakterystyki (np. zagrożenia zdekomponowane na źródła zagrożeń i zdarzenia zagrożeń)[23]. Definicje te są ważne dla podmiotu, aby udokumentować je przed przeprowadzeniem szacowania ryzyka, ponieważ działania w procesie szacowania opierają się na dobrze zdefiniowanych atrybutach zagrożeń, podatnościach, skutkach i innych czynnikach ryzyka w celu skutecznego określenia ryzyka i jego poziomu.

Zagrożenia:

Zagrożenie jest to każda okoliczność lub zdarzenie, które może mieć negatywny wpływ na działalność organizacji i aktywa, osoby fizyczne, inne organizacje lub społeczeństwo poprzez system informatyczny za pośrednictwem nieautoryzowanego dostępu, zniszczenia, ujawnienia lub modyfikacji informacji lub odmowy świadczenia usług[24]. Źródło zagrożenia jest scharakteryzowane, jako: (i) zamiar i metoda ukierunkowane na wykorzystanie słabych punktów (podatności); lub (ii) sytuacja i metoda, które mogą przypadkowo wykorzystać słabe punkty. Ogólnie rzecz biorąc, rodzaje źródeł zagrożeń obejmują: (i) wrogie cyberataki lub ataki fizyczne; (ii) błędy ludzkie polegające na zaniechaniu lub działaniu; (iii) awarie strukturalne zasobów kontrolowanych przez organizację (np. sprzętu komputerowego, oprogramowania, kontroli środowiska); oraz (iv) klęski żywiołowe i katastrofy spowodowane przez człowieka, wypadki i awarie będące poza kontrolą organizacji. Opracowano różne

[23] Czynnik ryzyka może mieć jedną cechę podlegającą ocenie (np. dotkliwość skutków) lub wiele cech, z których niektóre mogą być możliwe do oceny, a niektóre mogą nie być możliwe do oceny. Cechy, które nie są możliwe do oceny, zazwyczaj pomagają określić, jakie cechy niższego poziomu są istotne. Na przykład źródło zagrożenia charakteryzuje typ zagrożenia (przy użyciu taksonomii typów zagrożeń, które są raczej cechami symbolicznymi niż możliwymi do oceny). Typ zagrożenia określa, które z bardziej szczegółowych charakterystyk są istotne (np. źródło zagrożenia typu adwersarz ma powiązane charakterystyki zdolności, zamiaru i ukierunkowania, które są cechami podlegającymi bezpośredniej ocenie).

[24] Organizacje mogą wybrać określenie zdarzeń zagrożenia, jako: (i) pojedyncze zdarzenia, działania lub okoliczności; lub (ii) zestawy i/lub sekwencje powiązanych działań, czynności i/lub okoliczności.

taksonomie źródeł zagrożeń[25]. Niektóre taksonomie źródeł zagrożeń wykorzystują, jako zasadę organizacyjną rodzaj negatywnego wpływu. Wiele źródeł zagrożeń może zainicjować lub spowodować to samo zdarzenie zagrożenia, np. serwer rezerwowy może zostać zablokowany w wyniku ataku typu *denial-of-service*, celowego złośliwego działania administratora systemu, błędu administracyjnego, awarii sprzętu lub awarii zasilania.

Modele ryzyka różnią się stopniem szczegółowości i złożoności, z jakim identyfikowane są zdarzenia zagrożeń. W przypadku, gdy zdarzenia zagrożenia są identyfikowane z dużą specyficznością, można modelować, opracowywać i analizować *scenariusze zagrożeń*[26]. Zdarzenia zagrożenia dla cyberataków lub ataków fizycznych charakteryzują się taktyką, technikami i procedurami (TTP) stosowanymi przez przeciwników. Zrozumienie zdarzeń zagrożeń opartych na zachowaniach przeciwników daje podmiotom wgląd w możliwości związane z określonymi źródłami zagrożeń. Ponadto, posiadanie większej wiedzy na temat tego, kto przeprowadza ataki, daje podmiotom lepsze zrozumienie tego, co przeciwnicy chcą zyskać dzięki atakom. Znajomość intencji i aspektów potencjalnego ataku pomaga podmiotom zawęzić zestaw najbardziej istotnych do rozważenia zdarzeń zagrożeń.

Przesunięcie zagrożenia (*ang. Threat shifting)* jest reakcją przeciwników na dostrzegane przez niego zabezpieczenia lub środki zaradcze, w której przeciwnik zmienia niektóre cechy charakterystyczne swojego zamiaru w celu uniknięcia lub pokonania tych zabezpieczeń/środków zaradczych. Przesunięcie zagrożenia może wystąpić w jednej lub kilku domenach, w tym: (i) domenie czasowej (np. opóźnienie ataku lub nielegalne wejście w celu przeprowadzenia dodatkowego rozpoznania); (ii) domenie docelowej (np. wybór innego celu, który nie jest równie dobrze chroniony); (iii) domenie zasobów (np. dodanie zasobów do ataku w celu zmniejszenia niepewności jego powodzenia lub w celu przezwyciężenia środków ochronnych lub zaradczych); lub (iv) domenie dotyczącej planowania ataku/metody ataku (np. zmiana środka użytego do ataku lub ścieżki ataku). Przemieszczanie się zagrożeń

[25] Załącznik D zawiera przykładową taksonomię źródeł zagrożeń i związanych z nimi cech zagrożenia.

[26] *Scenariusz zagrożenia* jest zbiorem dyskretnych zdarzeń zagrożenia, przypisanych do konkretnego źródła zagrożenia lub wielu źródeł zagrożenia, uporządkowanych w czasie, które skutkują niekorzystnymi skutkami.

jest naturalną konsekwencją dynamicznego zestawu interakcji pomiędzy źródłami zagrożeń i rodzajami docelowych zasobów organizacyjnych. W przypadku bardziej wyrafinowanych źródeł zagrożeń ma on również tendencję do wychodzenia na ścieżkę najmniejszego oporu w celu wykorzystania poszczególnych słabych punktów, a odpowiedzi nie zawsze są przewidywalne. Oprócz wdrożonych zabezpieczeń lub środków zaradczych oraz wpływu udanego wykorzystania podatności organizacyjnej, kolejnym czynnikiem wpływającym na przesunięcie zagrożenia jest korzyść dla atakującego. Korzyść postrzegana po stronie atakującego może również wpływać na to, jak bardzo i kiedy następuje zmiana zagrożenia.

Podatności i warunki predyspozycji na zagrożenia:

Podatność to słaby punkt w systemie informatycznym, procedurach bezpieczeństwa systemu, zabezpieczeniach wewnętrznych lub implementacji, który może zostać wykorzystany przez źródło zagrożenia[27]. Ważne jest jednak również, aby uwzględnić możliwość zaistnienia słabych punktów, które mogą pojawić się w sposób naturalny w miarę upływu czasu, jak ewoluują cele organizacyjne/funkcje biznesowe, zmieniają się środowiska działania, mnożą się nowe technologie i pojawiają nowe zagrożenia. W kontekście takiej zmiany istniejące zabezpieczenia w zakresie ochrony mogą stać się nieodpowiednie i mogą wymagać ponownej oceny ich skuteczności. Tendencja do potencjalnej degradacji skuteczności zabezpieczeń w miarę upływu czasu wzmacnia potrzebę utrzymania szacowania ryzyka w całym cyklu życia systemu, a także znaczenie programów ciągłego monitorowania tej skuteczności, w celu uzyskania ciągłej świadomości sytuacyjnej w zakresie bezpieczeństwa organizacji.

Podatności nie są identyfikowane wyłącznie w ramach systemów informatycznych. Patrząc na systemy informatyczne w szerszym kontekście, można znaleźć słabe punkty w strukturach zarządzania podmiotem (np. brak skutecznych celów zarządzania ryzykiem i odpowiedniego kształtowania ryzyka, słaba komunikacja wewnątrz podmiotu, niespójne decyzje dotyczące

[27] Waga podatności jest oceną względnej ważności jej zniwelowania/usunięcia. Waga może być określona przez zakres potencjalnego negatywnego wpływu, jeśli taka luka zostanie wykorzystana przez źródło zagrożenia. W związku z tym, waga podatności, ogólnie rzecz biorąc, zależy od kontekstu.

względnych priorytetów celów/funkcji biznesowych lub niewłaściwe dostosowanie architektury podmiotu do wspierania działalności misyjnej/biznesowej). Podatności występują również w relacjach zewnętrznych (np. zależność od poszczególnych źródeł energii, łańcuchów dostaw, technologii informatycznych i dostawców usług telekomunikacyjnych), procesach misyjnych/biznesowych (np. słabo zdefiniowane procesy lub procesy nieświadome ryzyka) oraz w architekturach bezpieczeństwa podmiotu/informacji (np. złe decyzje architektoniczne skutkujące brakiem różnorodności lub odporności w systemach informatycznych podmiotu)[28].

Ogólnie rzecz biorąc, ryzyko materializuje się w wyniku szeregu zdarzeń zagrażających bezpieczeństwu informacji, z których każde wykorzystuje jedną lub więcej podatności. Podmioty definiują scenariusze zagrożeń, aby opisać, w jaki sposób zdarzenia spowodowane przez źródło zagrożenia mogą przyczynić się do powstania lub spowodowania szkody. Opracowanie scenariuszy zagrożeń jest analitycznie użyteczne, ponieważ niektóre podatności mogą nie być narażone na eksploatację, chyba, że przyczyniają się do wykorzystania innych podatności. Dlatego też analiza, która pokazuje, w jaki sposób zbiór podatności, rozpatrywanych łącznie, może być wykorzystany przez jedno lub więcej zdarzeń zagrożenia, jest bardziej przydatna niż analiza poszczególnych podatności. Ponadto scenariusz zagrożenia opowiada pewną historię, a tym samym jest przydatny do informowania o ryzyku, jak również do przeprowadzenia analizy.

Oprócz podatności opisanych powyżej, organizacje biorą również pod uwagę warunki predysponujące. Warunki predysponujące to warunki istniejące w organizacji, misji lub procesie biznesowym, architekturze korporacyjnej, systemie informatycznym lub środowisku operacyjnym, które wpływają na (tj. zwiększają lub zmniejszają) prawdopodobieństwo, że zdarzenia związane z zagrożeniem, po ich zainicjowaniu, spowodują negatywne skutki dla

[28] NSC 800-39 zawiera wytyczne dotyczące podatności na wszystkich trzech poziomach w hierarchii zarządzania ryzykiem oraz potencjalnych negatywnych skutków, jakie mogą wystąpić, jeśli zagrożenia wykorzystają takie podatności.

operacji i aktywów organizacji, osób, innych organizacji lub Państwa[29]. Warunki predysponujące obejmują, na przykład, lokalizację obiektu w regionie zagrożonym huraganami lub powodziami (zwiększające prawdopodobieństwo narażenia na huragany lub powodzie) lub autonomiczny system informatyczny pozbawiony łączności z siecią zewnętrzną (zmniejszające prawdopodobieństwo narażenia na cyberatak sieciowy). Podatności wynikające z warunków predysponujących, których nie da się łatwo naprawić, mogą obejmować na przykład luki w planach awaryjnych, stosowanie przestarzałych technologii lub słabości/braki w mechanizmach tworzenia kopii zapasowych i awaryjnych systemów informatycznych. Podatności (w tym te przypisane do warunków predysponujących) są częścią ogólnego stanu bezpieczeństwa organizacyjnych systemów informatycznych i środowisk operacyjnych, które mogą wpływać na prawdopodobieństwo wystąpienia zdarzenia powodującego zagrożenie.

Prawdopodobieństwo:

Prawdopodobieństwo wystąpienia określonego zdarzenia jest ważonym czynnikiem ryzyka opartym na analizie prawdopodobieństwa, że dane zagrożenie jest w stanie wykorzystać daną podatność (lub zespół podatności). Czynnik prawdopodobieństwa ryzyka łączy w sobie oszacowanie prawdopodobieństwa zainicjowania zdarzenia zagrożenia z oszacowaniem prawdopodobieństwa oddziaływania (tj. prawdopodobieństwa, że zdarzenie zagrożenia doprowadzi do negatywnych skutków). W przypadku zagrożeń o charakterze intencyjnym ocena ich wystąpienia opiera się zazwyczaj na ocenie prawdopodobieństwa ich wystąpienia i obejmuje: (i) zamiar przeciwnika; (ii) zdolność przeciwnika; oraz (iii) ukierunkowanie przeciwnika. W przypadku zdarzeń innych niż intencyjne, prawdopodobieństwo ich wystąpienia jest szacowane na podstawie dowodów historycznych, danych empirycznych lub innych czynników. Należy pamiętać, że prawdopodobieństwo, iż zdarzenie zagrażające zostanie zainicjowane lub wystąpi, ocenia się w odniesieniu do konkretnych ram czasowych

[29] Koncepcja warunku predysponującego jest również związana z pojęciem podatności lub ekspozycji. Organizacje nie są podatne na ryzyko (lub narażone na ryzyko), jeśli zagrożenie nie może wykorzystać podatności do wywołania negatywnych skutków. Na przykład, organizacje, które nie korzystają z systemów zarządzania bazami danych, nie są podatne na zagrożenia związane z wstrzykiwaniem kodu SQL, a zatem nie są narażone na takie ryzyko.

(np. kolejnych sześciu miesięcy, następnego roku lub okresu do osiągnięcia określonego etapu rozwoju systemu). Jeżeli zdarzenie zagrażające jest prawie pewne, iż zostanie zainicjowane lub wystąpi w (określonych lub domniemanych) ramach czasowych, ocena ryzyka może uwzględniać szacunkową częstotliwość zdarzenia. Prawdopodobieństwo wystąpienia zagrożenia może być również oparte na stanie organizacji (w tym na przykład na jej podstawowych procesach biznesowych, architekturze korporacyjnej, architekturze bezpieczeństwa informacji, systemach informatycznych i środowiskach, w których te systemy działają) – biorąc pod uwagę warunki predyspozycji oraz obecność i skuteczność wdrożonych zabezpieczeń w celu ochrony przed nieautoryzowanym/niepożądanym zachowaniem, wykrywanie i ograniczanie szkód lub utrzymanie lub przywrócenie zdolności biznesowych. Prawdopodobieństwo wystąpienia oddziaływania uwzględnia prawdopodobieństwo (lub możliwość), że zdarzenie zagrażające wywrze negatywny wpływ, niezależnie od skali szkody, jakiej można się spodziewać.

Podmioty zazwyczaj stosują trzyetapowy proces w celu określenia ogólnego prawdopodobieństwa wystąpienia zdarzeń zagrażających. Po pierwsze, podmioty oceniają prawdopodobieństwo, że zdarzenia zagrażające zostaną zainicjowane (w przypadku zdarzeń mających charakter intencyjny) lub wystąpią (w przypadku zdarzeń niemających charakteru intencyjnego). Po drugie, podmioty oceniają prawdopodobieństwo, że zdarzenia zagrożenia po jego rozpoczęciu lub wystąpieniu spowodują niekorzystne skutki lub szkody dla działalności podmiotu i jego aktywów, osób, innych organizacji lub społeczeństwa. Wreszcie, podmioty oceniają ogólne prawdopodobieństwo, jako połączenie prawdopodobieństwa inicjacji/wystąpienia i prawdopodobieństwa wystąpienia negatywnego wpływu.

Parowanie zagrożeń i podatności na zagrożenia (tj. ustalenie relacji jeden do jednego pomiędzy zagrożeniami i podatnościami) może być niepożądane przy ocenie prawdopodobieństwa na poziomie celu/funkcji biznesowej, a w wielu przypadkach może być problematyczne nawet na poziomie systemu informatycznego ze względu na potencjalnie dużą liczbę zagrożeń i podatności na zagrożenia. Podejście to zazwyczaj wpływa na poziom szczegółowości w identyfikacji zdarzeń i podatności, a nie pozwala podmiotom na efektywne wykorzystanie informacji o zagrożeniach lub identyfikację zagrożeń na poziomie

szczegółowości, który jest istotny. W zależności od poziomu szczegółowości specyfikacji zagrożenia, dane zdarzenie zagrożenia może wykorzystywać wiele luk w zabezpieczeniach. Oceniając prawdopodobieństwo, podmioty badają podatności, które mogą być wykorzystywane przez zdarzenia zagrażające, a także podatność celów/funkcji biznesowych na zdarzenia, w odniesieniu do których nie istnieją zabezpieczenia lub wykonalne wdrożenia zabezpieczeń (np. ze względu na zależności funkcjonalne, w szczególności zależności zewnętrzne). W niektórych sytuacjach najskuteczniejszym sposobem zmniejszenia ryzyka związanego z bezpieczeństwem informacji jest przeprojektowanie procesów biznesowych tak, aby w przypadku zagrożenia systemów informatycznych istniały realne warunki pracy. Wykorzystanie opisanej powyżej koncepcji scenariuszy zagrożeń może pomóc podmiotom przezwyciężyć niektóre z ograniczeń związanych z łączeniem w pary zagrożeń i podatności na zagrożenia.

Wpływ:

Poziom wpływu zdarzenia zagrożenia to wielkość szkody, jakiej można się spodziewać w wyniku nieautoryzowanego ujawnienia informacji, nieautoryzowanej modyfikacji informacji, nieautoryzowanego zniszczenia informacji lub utraty informacji, lub utraty dostępności systemu informatycznego. Szkody takie mogą być odczuwane przez różne grupy interesariuszy, w tym na przykład kierowników urzędów, właścicieli celu, właścicieli informacji/struktur, właścicieli celu/procesów biznesowych, właścicieli systemów informatycznych lub osoby/grupy w sektorze publicznym lub prywatnym polegające w zakresie swoich interesów na danym podmiocie publicznym, osoby mające interes prawny w działaniach organizacji, aktywach lub osoby fizyczne, w tym inne organizacje współpracujące z organizacją lub społeczeństwo[30]. Podmioty powinny jasno określić: (i) proces stosowany przy dokonywaniu oznaczeń wpływu; (ii) założenia związane

[30] Termin aktywa organizacyjne może mieć bardzo szeroki zakres zastosowania i obejmować na przykład programy o dużym wpływie, fizyczne instalacje, krytyczne dla misji systemy informatyczne, personel, sprzęt lub logicznie powiązaną grupę systemów. W szerszym ujęciu, aktywa organizacyjne reprezentują wszelkie zasoby lub zestaw zasobów, które organizacja uznaje za wartościowe, w tym aktywa niematerialne, takie jak wizerunek lub reputacja.

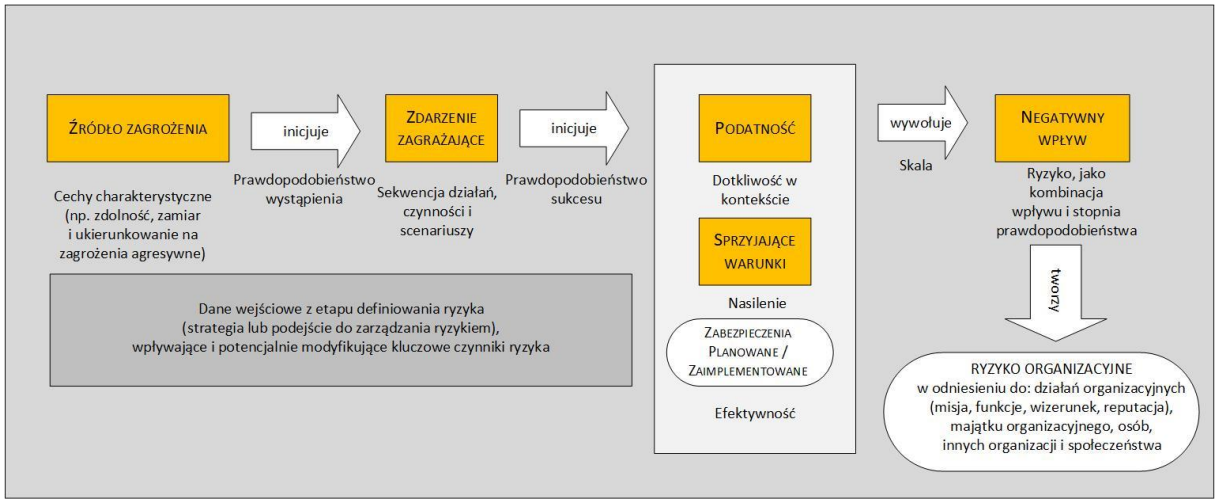
z oznaczeniami wpływu; (iii) źródła i metody uzyskiwania informacji o wpływie; oraz (iv) uzasadnienie wniosków wyciągniętych w odniesieniu do oznaczeń wpływu.

Podmioty powinny wyraźnie określić, w jaki sposób ustalone priorytety i wartości kierują identyfikacją aktywów o wysokiej wartości i potencjalnych negatywnych skutkach dla interesariuszy podmiotu. Jeśli takie informacje nie zostaną określone, priorytety i wartości związane z określeniem celów źródeł zagrożeń i związanych z nimi skutków organizacyjnych można zazwyczaj wyprowadzić z planowania strategicznego i polityki. Na przykład, poziomy kategoryzacji bezpieczeństwa wskazują na organizacyjne skutki narażenia na ujawnienie różnych rodzajów informacji. Oceny wpływu na prywatność i poziomy krytyczności (jeśli są zdefiniowane jako część planowania awaryjnego lub analizy wpływu celu/biznesu) wskazują na niekorzystne dla podmiotu skutki zniszczenia, kompromitacji lub utraty odpowiedzialności za zasoby informacyjne.

Plany strategiczne i polityka podkreślają lub implikują również względne priorytety w zakresie natychmiastowego lub bliskiego osiągnięcia celu/realizacji funkcji biznesowych oraz długoterminowej rentowności organizacyjnej (która może zostać osłabiona przez utratę reputacji lub sankcje wynikające z narażenia na ujawnienie informacji wrażliwych). Podmioty mogą również wziąć pod uwagę zakres skutków zdarzeń zagrożenia, w tym względną wielkość zespołu zasobów, których ono dotyczy, przy ostatecznym ustalaniu skutków. Założenia dotyczące tolerancji ryzyka mogą stanowić, że zdarzenia zagrażające oddziaływaniem poniżej określonej wartości nie dają podstaw do dalszej analizy.

Ryzyko:

Rysunek 3 ilustruje przykład modelu ryzyka uwzględniającego kluczowe czynniki ryzyka omówione powyżej oraz relacje pomiędzy tymi czynnikami. Każdy z tych czynników ryzyka jest wykorzystywany w procesie oceny ryzyka w rozdziale trzecim.



Rysunek 3. Ogólny model ryzyka z kluczowymi czynnikami ryzyka.

Jak wspomniano powyżej, ryzyko jest funkcją prawdopodobieństwa wystąpienia zagrożenia i potencjalnego negatywnego wpływu w przypadku wystąpienia zdarzenia. Definicja ta uwzględnia wiele rodzajów negatywnych skutków na wszystkich poziomach hierarchii zarządzania ryzykiem opisanych w publikacji NSC 800-39 (np. uszczerbek na wizerunku lub reputacji organizacji lub strata finansowa na poziomie 1; niezdolność do pomyślnej realizacji określonej celu/procesu biznesowego na poziomie 2; lub zasoby wydane w odpowiedzi na incydent z systemem informatycznym na poziomie 3). Uwzględnia również zależności między skutkami (np. utrata obecnej lub przyszłej skuteczności celu podmiotu ze względu na utratę atrybutów bezpieczeństwa informacji lub utratę dostępności systemu. Taka szeroka definicja pozwala również na przedstawienie ryzyka, jako pojedynczej wartości lub jako wektora (tzn. wielu wartości), w którym różne rodzaje oddziaływań są oceniane osobno. Dla celów informowania o ryzyku, ryzyko jest na ogół pogrupowane zgodnie z rodzajami negatywnych skutków (i ewentualnie ramami czasowymi, w których skutki te mogą być odczuwalne).

Agregacja:

Podmioty mogą stosować agregację ryzyka w celu przekształcenia kilku pojedynczych lub niższych poziomów ryzyka w ryzyko bardziej ogólne lub wyższe. Podmioty mogą również wykorzystywać agregację ryzyka do efektywnego zarządzania zakresem i skalą ocen ryzyka dotyczących wielu systemów informatycznych i wielu procesów biznesowych o określonych

relacjach i zależnościach pomiędzy tymi systemami i procesami. Agregacja ryzyka, prowadzona głównie na poziomie 1 i 2, a sporadycznie na poziomie 3, ocenia ogólne ryzyko dla operacji podmiotu, aktywów i osób, biorąc pod uwagę zestaw pojedynczych ryzyk. Ogólnie rzecz biorąc, w przypadku pojedynczego ryzyka (np. ryzyka związanego z pojedynczym systemem informatycznym wspierającym dobrze zdefiniowany proces biznesowy), w najgorszym przypadku wpływ ustanawia górną granicę ogólnego ryzyka dla operacji organizacyjnych, aktywów i osób[31]. Jedną z kwestii związanych z agregacją ryzyka jest to, że ta górna granica ryzyka może nie mieć zastosowania. Na przykład, korzystne dla podmiotu może być dokonanie oceny ryzyka na poziomie całego podmiotu, w sytuacji gdy wiele ryzyk materializuje się jednocześnie lub gdy to samo ryzyko materializuje się wielokrotnie na przestrzeni czasu. W takich sytuacjach istnieje możliwość, że wysokość ponoszonego ogólnego ryzyka przekracza możliwości ryzyka podmiotu, a tym samym ogólny wpływ na działania i aktywa podmiotu (tj. wpływ na cel/działalność) wykracza poza to, co zostało pierwotnie ocenione dla każdego konkretnego ryzyka.

Przy sumowaniu ryzyka podmioty biorą pod uwagę relacje pomiędzy różnymi pojedynczymi rodzajami ryzyka. Na przykład, może istnieć związek przyczynowo - skutkowy polegający na tym, że jeżeli jedno z ryzyk się zmaterializuje, to mniej lub bardziej prawdopodobne jest zmaterializowanie się innego. Jeżeli istnieje bezpośrednia lub odwrotna zależność pomiędzy pojedynczymi rodzajami ryzyka, wówczas ryzyka te mogą być powiązane (w sensie jakościowym) lub skorelowane (w sensie ilościowym) w sposób pozytywny lub negatywny. Sprzężenie lub korelacja ryzyka (tj. znalezienie związków między ryzykami, które zwiększają lub zmniejszają prawdopodobieństwo zmaterializowania się konkretnego ryzyka) mogą być dokonywane na poziomach 1, 2 lub 3.

Niepewność:

[31] Kategoryzacje bezpieczeństwa przeprowadzone zgodnie z publikacją NSC 199 stanowią przykłady analiz wpływu w przypadku najgorszego scenariusza (z wykorzystaniem koncepcji najwyższej wartości - *ang. high water mark*). Tego rodzaju analiza wpływu stanowi górną granicę ryzyka w przypadku zastosowania jej do konkretnych sytuacji w organizacji.

Niepewność jest nieodłącznym elementem oceny ryzyka, ze względu na takie czynniki jak (i) ograniczenia dotyczące stopnia, w jakim sytuacje z przyszłości będą przypominać sytuacje z przeszłości; (ii) niedoskonałą lub niepełną znajomość zagrożenia (np. cechy charakterystyczne przeciwników, w tym ich taktyka, techniki i procedury); (iii) nieujawnione podatności technologii lub produktów; oraz (iv) nierozpoznane zależności, które mogą prowadzić do nieprzewidzianych skutków. Niepewność, co do wartości konkretnych czynników ryzyka może być również spowodowana krokiem w rozwoju Ram Zarządzania Ryzykiem (RMF) lub fazą cyklu życia systemu, na której dokonuje się szacowania ryzyka. Na przykład we wczesnych fazach cyklu życia systemu obecność i skuteczność zabezpieczeń może być nieznana, podczas gdy w późniejszych fazach cyklu życia koszt oceny skuteczności kontroli może przewyższać korzyści w postaci pełniejszej informacji przy podejmowaniu decyzji. Wreszcie, niepewność może wynikać z niepełnej wiedzy na temat ryzyka związanego z innymi systemami informatycznymi, procesami biznesowymi, usługami, wspólną infrastrukturą lub innymi podmiotami. Stopień niepewności w wynikach oceny ryzyka, z tych różnych powodów, może być przekazany w formie wyników (np. poprzez wyrażenie wyników w sposób jakościowy, poprzez podanie zakresów wartości, a nie pojedynczych wartości dla zidentyfikowanych zagrożeń, lub poprzez zastosowanie wizualnych reprezentacji regionów rozmytych, a nie punktów).

2.3.2. Podejście do szacowania

Ryzyko i jego przyczyny mogą być szacowane na różne sposoby, w tym ilościowo, jakościowo lub w sposób mieszany. Każde podejście do szacowania ryzyka rozważane przez podmiot ma zalety i wady. Preferowane podejście (lub specyficzny dla danej sytuacji zestaw podejść) może zostać wybrany w oparciu o kulturę organizacyjną, a w szczególności postawy wobec koncepcji niepewności i komunikacji ryzyka. W ocenach ilościowych stosuje się zazwyczaj zestaw metod, zasad lub reguł szacowania ryzyka opartych na wykorzystaniu liczb – przy czym znaczenia i proporcjonalność wartości są utrzymywane wewnątrz i na zewnątrz kontekstu oceny. Ten rodzaj oceny najskuteczniej wspiera analizy kosztów i korzyści alternatywnych rozwiązań w zakresie ryzyka lub kierunków działań. Jednakże znaczenie wyników ilościowych może nie zawsze być jasne i może wymagać interpretacji i wyjaśnienia

– w szczególności w celu wyjaśnienia założeń i ograniczeń dotyczących wykorzystania wyników. Na przykład, organizacje mogą zazwyczaj pytać, czy liczby lub wyniki uzyskane w ramach szacowania ryzyka są wiarygodne lub czy różnice w uzyskanych wartościach są znaczące lub nieistotne. Dodatkowo, rygor kwantyfikacji jest znacznie zmniejszony, gdy subiektywne oznaczenia są zawarte w ramach oceny ilościowej lub gdy znacząca niepewność dotyczy wyznaczania wartości. Korzyści płynące z ocen ilościowych (pod względem rygoru, powtarzalności i odtwarzalności wyników oceny) mogą w niektórych przypadkach zostać zniwelowane przez koszty (pod względem czasu i wysiłku ekspertów oraz ewentualnego wykorzystania i użycia narzędzi niezbędnych do przeprowadzenia takiej oceny).

W przeciwieństwie do ocen ilościowych, w ocenach jakościowych stosuje się zazwyczaj zestaw metod, zasad lub reguł oceny ryzyka w oparciu o nienumeryczne kategorie lub poziomy (np. bardzo niskie, niskie, umiarkowane, wysokie, bardzo wysokie). Ten rodzaj oceny wspiera przekazywanie wyników oceny ryzyka decydentom. Zakres wartości w ocenach jakościowych jest jednak w większości przypadków stosunkowo niewielki, co utrudnia względne ustalenie priorytetów lub porównanie w ramach zestawu zgłoszonych zagrożeń. Ponadto, o ile każda z tych wartości nie jest bardzo wyraźnie określona lub nie jest scharakteryzowana za pomocą konkretnych przykładów, różni eksperci, opierając się na swoich indywidualnych doświadczeniach, mogą uzyskać znacząco różne wyniki oceny. Powtarzalność i odtwarzalność ocen jakościowych zwiększa adnotacje o ocenianych wartościach (np. wartość ta jest wysoka z następujących powodów) oraz wykorzystanie tabel lub innych dobrze zdefiniowanych funkcji do łączenia wartości jakościowych.

Wreszcie, w ocenach mieszanych stosuje się zazwyczaj zestaw metod, zasad lub reguł oceny ryzyka, w których wykorzystuje się przedziały wartości, skale lub liczby reprezentatywne, których wartości i znaczenia nie są zachowane w innych kontekstach. Ten rodzaj oceny może przynieść korzyści w postaci oceny ilościowej i jakościowej. Przedziały wartości (np. 0-15, 16-35, 36-70, 71-85, 86-100) lub skale (np. 1-10) z łatwością przekładają się na terminy jakościowe, które wspomagają informowanie decydentów o ryzyku (np. wynik można zinterpretować, jako bardzo wysoki), a jednocześnie umożliwiają względne porównanie wartości w różnych przedziałach wartości lub nawet w obrębie tego samego przedziału (np.

różnica między zagrożeniami ocenionymi odpowiednio na 70 i 71 jest stosunkowo nieistotna, natomiast różnica między zagrożeniami ocenionymi na 36 i 70 jest stosunkowo istotna). Rola eksperta w przypisywaniu wartości jest bardziej oczywista niż w przypadku podejścia czysto ilościowego. Ponadto, jeżeli skale lub przedziały wartości zapewniają dostateczną ziarnistość, lepsze wsparcie stanowi względna priorytetyzacja wyników niż w przypadku podejścia czysto jakościowego. Podobnie jak w podejściu ilościowym, rygor jest znacznie zmniejszony, gdy subiektywne ustalenia są zawarte w ocenach lub gdy znaczna niepewność dotyczy ustalenia wartości. Podobnie jak w przypadku nienumerycznych kategorii lub poziomów stosowanych w dobrze uzasadnionym podejściu jakościowym, każdy przedział lub zakres wartości musi być jasno zdefiniowany lub scharakteryzowany za pomocą istotnych przykładów.

Niezależnie od rodzaju wybranej skali wartości, szacowania wyraźnie wskazują na element czasowy czynników ryzyka. Na przykład, podmioty mogą powiązać konkretny okres czasu z oceną prawdopodobieństwa wystąpienia i oceną powagi oddziaływania.

2.3.3. Podejście analityczne

Podejścia analityczne różnią się pod względem orientacji lub punktu wyjścia szacowania ryzyka, poziomu szczegółowości szacowania oraz sposobu traktowania zagrożeń wynikających z podobnych scenariuszy zagrożeń. Podejście analityczne może być: (i) zorientowane na zagrożenie; (ii) zorientowane na aktywa/skutki; lub (iii) zorientowane na podatność na zagrożenia[32]. Podejście zorientowane na zagrożenie rozpoczyna się od identyfikacji źródeł zagrożeń i zdarzeń powodujących zagrożenie i koncentruje się na opracowywaniu scenariuszy zagrożeń; podatność na zagrożenia identyfikuje się w kontekście zagrożeń, a w przypadku zagrożeń o charakterze agresywnym skutki identyfikuje się w oparciu o intencje przeciwnika. Podejście ukierunkowane na aktywa/skutki rozpoczyna się od identyfikacji skutków lub konsekwencji obaw i krytyczności aktywów, w miarę możliwości z wykorzystaniem wyników celu lub analiz wpływu na działalność (*ang. Business Impact*

[32] Organizacje mają dużą swobodę w wyborze konkretnego podejścia do analizy. Na wybór konkretnego podejścia wpływają różne względy organizacyjne (np. jakość i ilość dostępnych informacji dotyczących zagrożeń, podatności oraz skutków/aktywów; konkretny kierunek, który ma dla organizacji najwyższy priorytet; dostępność narzędzi analitycznych kładących nacisk na określone kierunki; lub kombinacja powyższych).

Analysis – BIA)[33] oraz identyfikacji zdarzeń zagrażających, które mogą prowadzić do powstania skutków lub konsekwencji lub źródeł zagrożeń mogących prowadzić do wystąpienia tych skutków lub konsekwencji. Podejście zorientowane na podatności zaczyna się od zestawu predysponujących warunków lub możliwych do wykorzystania słabości/niedoskonałości w systemach informatycznych organizacji lub środowiskach, w których systemy te działają i identyfikuje zdarzenia zagrożeń, które mogłyby wykorzystać te podatności wraz z ewentualnymi konsekwencjami wykorzystania podatności. Każde podejście analityczne uwzględnia te same czynniki ryzyka, a zatem obejmuje ten sam zestaw działań związanych z szacowaniem ryzyka, choć w różnej kolejności. Różnice w punkcie wyjścia szacowania ryzyka mogą potencjalnie wpływać na wyniki, powodując, że niektóre rodzaje ryzyka nie zostaną zidentyfikowane. Dlatego też identyfikacja ryzyka z drugiej orientacji (np. uzupełnienie podejścia opartego na analizie zagrożeń o podejście oparte na analizie aktywów/skutków) może poprawić rygor i skuteczność analizy.

Oprócz ukierunkowania podejścia analitycznego, podmioty mogą stosować bardziej rygorystyczne techniki analizy (np. analizy oparte na wykresach), aby zapewnić efektywny sposób rozliczania relacji międzyludzkich: (i) źródła zagrożeń i zdarzenia zagrożeń (tj. jedno zdarzenie zagrożenia może być spowodowane przez wiele źródeł zagrożeń, a jedno źródło zagrożenia może spowodować wiele zdarzeń zagrożenia); (ii) zdarzenia zagrożenia i podatności (tj. jedno zdarzenie zagrożenia może wykorzystać wiele podatności, a jedna podatność może być wykorzystana przez wiele zdarzeń zagrożenia); oraz (iii) zdarzenia zagrożenia i wpływy/aktywa (tj. jedno zdarzenie powodujące zagrożenie może mieć wpływ na wiele aktywów lub mieć wielorakie skutki, a pojedynczy składnik aktywów może zostać

[33] Analiza wpływu na działalność określa aktywa o wysokiej wartości oraz niekorzystne skutki w zakresie utraty integralności lub dostępności. Publikacja NSC 800-34 zawiera wytyczne dotyczące BIA na poziomie systemu informatycznego w hierarchii zarządzania ryzykiem.

dotknięty przez wiele zdarzeń powodujących zagrożenie [34]. Rygorystyczne podejścia analityczne umożliwiają również ustalenie, czy w ramach czasowych, dla których szacuje się ryzyko, może wystąpić określony niekorzystny wpływ (lub może dojść do uszkodzenia konkretnego składnika aktywów) co najwyżej raz, a może nawet wielokrotnie, w zależności od charakteru wpływu i sposobu, w jaki podmioty (w tym procesy misyjne/biznesowe lub systemy informatyczne) poradzą sobie z tym niekorzystnym wpływem.

2.3.4. Wpływ kultury organizacyjnej na szacowanie ryzyka

Podmioty mogą różnić się pod względem modeli ryzyka, podejść do oceny i analiz, które preferują z różnych powodów. Na przykład, kwestie kulturowe [35] mogą predysponować organizacje do stosowania modeli ryzyka, które zakładają stałą wartość jednego lub kilku możliwych czynników ryzyka, tak, że niektóre czynniki obecne w modelach innych organizacji nie są reprezentowane. Kultura może również predysponować podmioty do stosowania modeli ryzyka, które wymagają szczegółowych analiz wykorzystujących oceny ilościowe (np. w kontekście bezpieczeństwa jądrowego). Alternatywnie, podmioty mogą preferować metody oceny jakościowej lub mieszanej. Oprócz różnic pomiędzy podmiotami, różnice mogą występować również wewnątrz podmiotu. Na przykład, podmioty mogą stosować modele wstępnego lub wysokiego ryzyka na wczesnym etapie cyklu życia systemu, aby wybrać zabezpieczenia, a następnie bardziej szczegółowe modele szacowania ryzyka dla danej celu lub funkcji biznesowej. Ramy ryzyka organizacyjnego [36] określają, jakie modele

[34] Na przykład, techniki analizy oparte na grafach (np. funkcjonalna analiza zależności sieciowych, analiza drzewa ataku dla zagrożeń adwersarza, analiza drzewa błędu dla innych rodzajów zagrożeń) zapewniają sposoby wykorzystania określonych zdarzeń zagrożenia do generowania scenariuszy zagrożeń. Techniki analizy oparte na grafach mogą również zapewnić sposoby uwzględniania sytuacji, w których jedno zdarzenie może zmienić prawdopodobieństwo wystąpienia innego zdarzenia. W szczególności analizy ataków i drzew błędów mogą generować wiele scenariuszy zagrożeń, które są prawie takie same, w celu określenia poziomów ryzyka. Dzięki zautomatyzowanemu modelowaniu i symulacji można wygenerować dużą liczbę scenariuszy zagrożeń (np. drzewa ataków/awarii, przejścia przez sieci zależności funkcjonalnych). Dlatego też techniki analizy grafów zawierają sposoby ograniczenia analizy do zdefiniowania rozsądnego podzbioru wszystkich możliwych scenariuszy zagrożeń.

[35] Publikacja NSC 800-39 opisuje, w jaki sposób kultura organizacyjna wpływa na zarządzanie ryzykiem.

[36] NSC 800-39 definiuje ramy ryzyka organizacji, jako zbiór założeń, ograniczeń, tolerancji ryzyka, priorytetów i wyłączeń, które leżą u podstaw strategii zarządzania ryzykiem organizacji - tworząc solidną podstawę do zarządzania ryzykiem i ograniczając jej decyzje oparte na ryzyku.

ryzyka, podejścia do szacowania i podejścia do analizy należy stosować w różnych okolicznościach.

KORZYSTANIE Z MODELI RYZYKA

Pojedynczy model ryzyka (składający się ze stałego zestawu czynników, stałej skali oceny dla każdego czynnika oraz stałego algorytmu łączenia czynników) nie może zaspokoić zróżnicowanych potrzeb podmiotów sektora publicznego i prywatnego, które opierają się na NSC 800-30. Na przykład, podczas gdy niektóre podmioty mogą zwracać uwagę na zagrożenia o charakterze agresywnym i dostarczać szczegółowych informacji o takich zagrożeniach, inne mogą zamiast tego skupić się na zagrożeniach o charakterze innym niż agresywne, dostarczając bardziej szczegółowych informacji o tych rodzajach zagrożeń, a mniej szczegółowych o zagrożeniach o charakterze agresywnym. Dlatego też modele ryzyka opracowane przez podmioty o różnych założeniach dotyczących zagrożeń będą obejmowały różne czynniki, jak również różne poziomy szczegółowości.

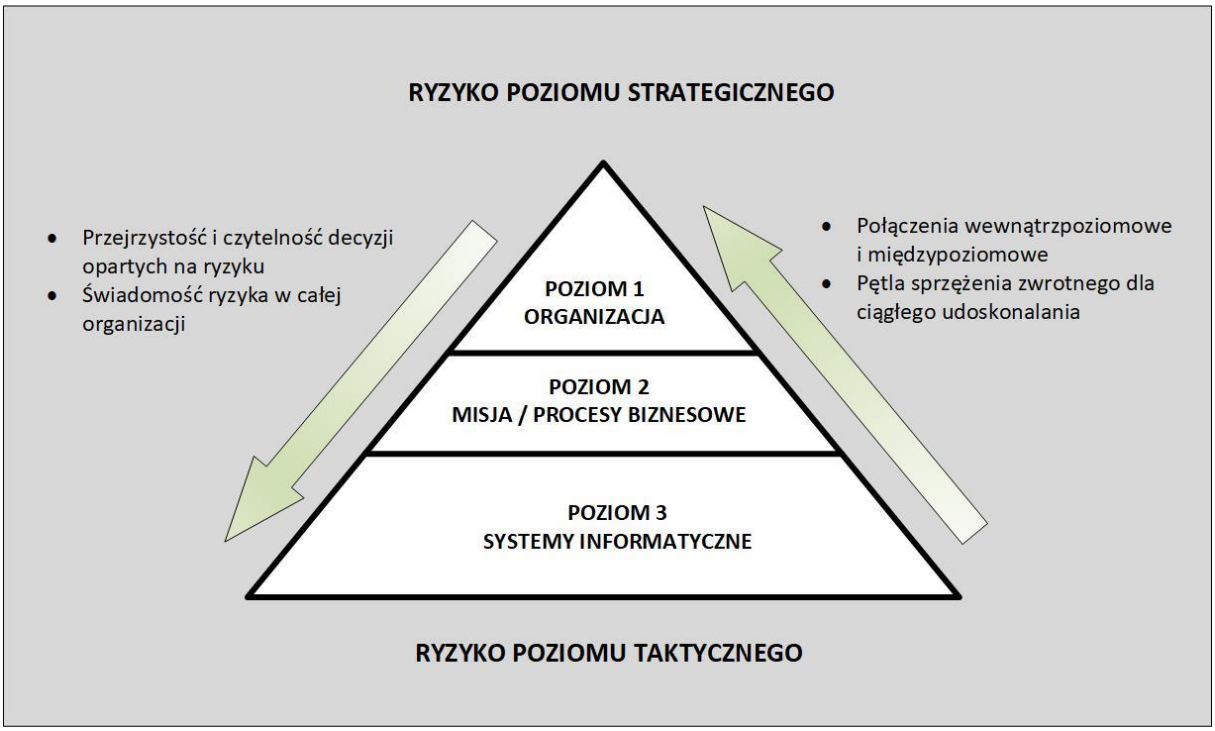
Podobnie, w ramach jednego podmiotu lub wspólnoty interesów, różne skale oceny mogą być odpowiednie dla różnych celów/funkcji biznesowych, różnych kategorii systemów informatycznych lub dla systemów na różnych etapach cyklu życia systemu. Na przykład podczas wstępnej oceny ryzyka przeprowadzanej podczas pierwszego rozważania systemu informatycznego dostępne informacje o zagrożeniach i podatnościach mogą być niespecyficzne i wysoce niepewne. Dla takich szacunków ryzyka właściwa może być ocena jakościowa, wykorzystująca tylko kilka czynników. Natomiast szacowanie ryzyka oparte na ocenie zabezpieczeń może być znacznie bardziej szczegółowe, a szacunki mogą być dokonywane z większą wiarygodnością. Dla takich ocen bardziej odpowiednie może być szacowanie mieszane przy użyciu skali wartości 0-100.

Oczekiwaniem zawartym w NSC 800-39 i 800-30 jest to, aby każdy podmiot lub społeczeństwo zdefiniowało model ryzyka odpowiadający ich postrzeganiu ryzyka (tj. formuły, które odzwierciedlają poglądy podmiotu lub społeczności na temat tego, które czynniki ryzyka muszą być brane pod uwagę, które czynniki mogą być łączone, które

czynniki muszą być dalej dekomponowane oraz w jaki sposób oceniane wartości powinny być łączone algorytmicznie). W publikacji NSC 800-30 określono czynniki ryzyka, które są powszechne w szerokim spektrum modeli ryzyka. Ponadto, dzięki zdefiniowaniu wielu ujednoliconych skali wartości, niniejsza publikacja stanowi podstawę spójnego podejścia do szacowania ryzyka w zakresie bezpieczeństwa informacji w całym cyklu życia systemu, bez zmuszania do dokonywania ocen na wczesnym etapie cyklu życia, które byłyby bardziej szczegółowe, niż można to uzasadnić dostępnymi informacjami.

2.4. Stosowanie szacowania ryzyka

Jak stwierdzono wcześniej, szacowanie ryzyka może być przeprowadzane na wszystkich trzech poziomach hierarchii zarządzania ryzykiem – na poziomie organizacji, na poziomie procesów biznesowych i na poziomie systemu informatycznego. Rysunek 4 ilustruje hierarchię zarządzania ryzykiem zdefiniowaną w publikacji NSC 800-39, która przedstawia wiele perspektyw ryzyka od poziomu strategicznego do taktycznego. Tradycyjne szacowania ryzyka zasadniczo koncentrują się na poziomie 3 (tj. na poziomie systemu informatycznego) i w rezultacie zazwyczaj pomijają inne istotne czynniki ryzyka, które mogą być lepiej ocenione na poziomie 1 lub 2 (np. narażenie podstawowej funkcji wykonywanej w ramach celu podmiotu na niekorzystne zagrożenie oparte na wzajemnych połączeniach systemów informatycznych).



Rysunek 4. Hierarchia zarządzania ryzykiem.

Szacowania ryzyka wspierają decyzje dotyczące reakcji na ryzyko na różnych szczeblach hierarchii zarządzania ryzykiem. Na poziomie 1 ocena ryzyka może mieć wpływ na przykład na: (i) programy, polityki, procedury i wytyczne w zakresie bezpieczeństwa informacji w skali całego podmiotu; (ii) rodzaje odpowiednich reakcji na ryzyko (tj. akceptacja ryzyka, unikanie, łagodzenie, dzielenie się lub przekazywanie); (iii) decyzje inwestycyjne dotyczące technologii/systemów informatycznych; (iv) zamówienia; (v) minimalne zabezpieczenia w skali całego podmiotu; (vi) zgodność z architekturą przedsiębiorstwa/systemów bezpieczeństwa; oraz (vii) strategie monitorowania i bieżące zezwolenia na użycie systemów informatycznych oraz zabezpieczenia wspólne. Na poziomie 2 szacowanie ryzyka może mieć wpływ na przykład na: (i) decyzje dotyczące projektowania architektury korporacyjnej/architektury bezpieczeństwa; (ii) wybór zabezpieczeń wspólnych; (iii) wybór dostawców, usług i wykonawców w celu wsparcia celu organizacji/funkcji biznesowych; (iv) opracowanie procesów biznesowych świadomych ryzyka; oraz (v) interpretację polityki bezpieczeństwa informacji w odniesieniu do systemów informatycznych podmiotu

i środowisk, w których te systemy działają. Wreszcie – na poziomie 3 – szacowanie ryzyka może mieć wpływ na przykład na: (i) decyzje projektowe (w tym wybór, dostosowanie i uzupełnienie zabezpieczeń oraz wybór produktów informatycznych dla systemów informatycznych podmiotu); (ii) decyzje wykonawcze (w tym stwierdzenie, czy określone produkty informatyczne lub konfiguracje produktów spełniają wymogi zabezpieczeń); oraz (iii) decyzje operacyjne (w tym wymagany poziom monitorowania, częstotliwość wydawania bieżących zezwoleń na użycie systemów informatycznych oraz decyzje dotyczące utrzymania systemu).

Szacowania ryzyka mogą również informować o innych działaniach w zakresie zarządzania ryzykiem na trzech poziomach, które nie są związane z bezpieczeństwem. Na przykład na poziomie 1 szacowanie ryzyka może dostarczyć użytecznych danych wejściowych do: (i) określanie ryzyka operacyjnego (w tym ciągłości działania w przypadku celu organizacyjnych i funkcji biznesowych); (ii) określania ryzyka organizacyjnego (w tym ryzyka finansowego, ryzyka braku zgodności, ryzyka regulacyjnego, ryzyka utraty reputacji i skumulowanego ryzyka nabycia w przypadku projektów na dużą skalę); oraz (iii) określania ryzyka wielokrotnego wpływu (w tym ryzyka związanego z łańcuchem dostaw i ryzyka związanego z działalnością partnerską). Na poziomie 2 szacowanie ryzyka może dostarczyć tych samych użytecznych informacji na temat ryzyka operacyjnego, organizacyjnego i wielorakiego wpływu, charakterystycznego dla procesów biznesowych. Na poziomie 3 szacowanie ryzyka może informować o kosztach, harmonogramie i ryzyku związanym z systemami informatycznymi, przy czym eksperci ds. bezpieczeństwa informacji koordynują swoje działania z kierownikami programów, właścicielami systemów informatycznych i organami zatwierdzającymi. Ten rodzaj koordynacji jest niezbędny w podmiotach w celu wyeliminowania silosów lub działań wyspowych, które generują mniej niż optymalne lub nieefektywne rozwiązania informatyczne i zabezpieczające, co wpływa na zdolność podmiotu do wykonywania przydzielonych zadań/funkcji biznesowych z maksymalną wydajnością i opłacalnością.

Należy zauważyć, że ryzyko związane z bezpieczeństwem informacji przyczynia się do powstawania ryzyka braku bezpieczeństwa na każdym poziomie. W związku z tym wyniki

szacowania ryzyka na danym poziomie służą, jako dane wejściowe do działań w zakresie zarządzania ryzykiem niezwiązanym z bezpieczeństwem na tym poziomie i są z nimi powiązane[37]. Ponadto wyniki oceny ryzyka na niższych poziomach służą jako dane wejściowe do oceny ryzyka na wyższych poziomach. Ryzyko może pojawić się w różnych skalach czasowych (np. ujawnienie informacji o bieżących operacjach organizacyjnych może natychmiast zagrozić skuteczności tych operacji, natomiast ujawnienie informacji o planowaniu strategicznym może zagrozić przyszłym możliwościom operacyjnym). Decyzje dotyczące reakcji na ryzyko mogą również obowiązywać w różnych przedziałach czasowych (np. zmiany w polityce organizacyjnej lub celów inwestycyjnej mogą czasami wymagać lat, podczas gdy zmiany konfiguracyjne w poszczególnych systemach mogą być często wprowadzane natychmiast). Ogólnie rzecz biorąc, proces zarządzania ryzykiem przebiega wolniej na poziomach 1 i 2 niż na poziomie 3. Wynika to ze sposobu, w jaki podmioty zazwyczaj reagują na ryzyko, które potencjalnie może mieć wpływ na szeroko zakrojone działania organizacyjne i aktywa – gdzie takie reakcje na ryzyko mogą wymagać rozwiązania problemów systemowych lub instytucjonalnych. Jednakże niektóre decyzje poziomu 1 (np. nowo odkryte zagrożenia lub słabe punkty wymagające wdrożenia w całej organizacji mandatu do ich ograniczenia) mogą wymagać natychmiastowego działania.

2.4.1. Szacowanie ryzyka na poziomie organizacyjnym

Na poziomie 1 szacowania ryzyka wspierają strategie organizacyjne, polityki, wytyczne i procesy zarządzania ryzykiem. Szacowania ryzyka przeprowadzane na poziomie 1 koncentrują się na operacjach organizacyjnych, aktywach i indywidualnych, kompleksowych ocenach w różnych obszarach działalności biznesowej. Na przykład, oceny ryzyka poziomu 1 mogą dotyczyć: (i) szczególnego rodzaju zagrożeń skierowanych do podmiotu, które mogą różnić się od zagrożeń występujących w innych podmiotach oraz sposób, w jaki zagrożenia te wpływają na decyzje dotyczące polityki; (ii) podatności lub braki systemowe wykryte w wielu systemach informatycznych podmiotu, które mogą być wykorzystywane przez przeciwników;

[37] W szczególności, wyniki oceny ryzyka wspierają zarządzanie ryzykiem inwestycyjnym. Publikacja specjalna NIST SP 800-65 zawiera wytyczne dotyczące włączania bezpieczeństwa informacji do procesu planowania inwestycyjnego i kontroli inwestycji kapitałowych (*ang. Capital Planning and Investment Control - CPIC*).

(iii) potencjalnego niekorzystnego wpływ na podmiot wynikającego z utraty lub narażenia na szwank informacji o podmiocie (umyślnie lub nieumyślnie); oraz (iv) wykorzystanie nowych technologii informatycznych i obliczeniowych, takich jak technologie mobilne i chmura obliczeniowa oraz potencjalnego wpływu na zdolność podmiotu do skutecznego wykonywania swoich celu/działań biznesowych przy wykorzystaniu tych technologii. Szacowanie ryzyka w całym podmiocie może opierać się wyłącznie na założeniach, ograniczeniach, tolerancjach ryzyka, priorytetach i kompromisach ustalonych na etapie określania ryzyka (tj. wynikających głównie z działań poziomu 1). Bardziej realistyczne i znaczące szacowanie ryzyka opiera się jednak na szacunkach przeprowadzonych w odniesieniu do wielu obszarów celu/przedsiębiorstw (tj. pochodzących głównie z działań poziomu 2). Zdolność organizacji do efektywnego wykorzystania szacowania ryzyka na poziomie 2 jako wkładu do oceny ryzyka na poziomie 1 jest kształtowana przez takie czynniki jak (i) podobieństwo celu/funkcji organizacyjnych i procesów misyjnych/biznesowych; oraz (ii) stopień autonomii jednostek organizacyjnych lub ich części składowych w stosunku do organizacji macierzystych. W zdecentralizowanych organizacjach lub organizacjach o różnych celach/funkcjach biznesowych i/lub środowiskach działania, może być konieczna specjalistyczna analiza w celu normalizacji wyników szacowania ryzyka poziomu 2. Wreszcie, szacowanie ryzyka na poziomie 1 uwzględnia identyfikację istotnych funkcji z planów kontynuacji operacji (*ang. Continuity of Operations Plans - COOP*)[38] przygotowanych przez podmiot przy określaniu udziału ryzyka poziomu 2. Wyniki szacowania ryzyka na poziomie 1 są przekazywane komórkom organizacyjnym w celu przeprowadzenia szacowania ryzyka na poziomie 2 i poziomie 3.

2.4.2. Szacowanie ryzyka na poziomie celu/procesu biznesowego

Na poziomie 2, szacowania ryzyka wspomagają określenie wymagań dotyczących ochrony i odporności procesów biznesowych oraz przypisanie tych wymagań do architektury korporacyjnej, jako części segmentów biznesowych (które wspierają procesy biznesowe). Alokacja ta jest realizowana za pomocą architektury bezpieczeństwa informacji wbudowanej

[38] Publikacja NSC 800-34 zawiera wytyczne dotyczące planowania awaryjnego systemu informatycznego (*ang. Information System Contingency Planning - ISCP*).

w architekturę korporacyjną. Szacowania ryzyka na poziomie 2 informują również o tym, czy i w jaki sposób i kiedy należy korzystać z systemów informatycznych w określonych procesach biznesowych, w szczególności w przypadku alternatywnego przetwarzania danych dotyczących celu/przedsiębiorstwa w obliczu zagrożonych systemów informatycznych. Zarządzanie ryzykiem i związane z tym działania w zakresie oceny ryzyka na poziomie 2 są ściśle związane z opracowywaniem planów zachowania ciągłości działania (*ang. Business Continuity Plan – BCP*). Szacowanie ryzyka na poziomie 2 koncentruje się na segmentach branżowych, które zazwyczaj obejmują wiele systemów informatycznych, o różnym stopniu krytyczności lub wrażliwości w odniesieniu do podstawowych branż/funkcji biznesowych [39]. Szacowanie ryzyka na poziomie 2 może również koncentrować się na architekturze bezpieczeństwa informacji, jako krytycznym elemencie architektury korporacyjnej, aby pomóc podmiotom w wyborze wspólnych elementów zabezpieczeń odziedziczonych przez systemy informatyczne organizacji na poziomie 3. Wyniki szacowania ryzyka opracowane na poziomie 2 są przekazywane i udostępniane komórkom organizacyjnym na poziomie 3, aby pomóc w informowaniu i kierowaniu procesem wprowadzania zabezpieczeń w systemach informatycznych i środowiskach, w których te systemy działają. Szacowanie ryzyka na poziomie 2 dostarcza również oceny bezpieczeństwa i pozycji ryzyka procesów biznesowych, które stanowią podstawę oceny ryzyka organizacyjnego na poziomie 1. W związku z tym wyniki oceny ryzyka na poziomie 2 są rutynowo przekazywane jednostkom organizacyjnym na poziomie 1 i 3.

2.4.3. Szacowanie ryzyka na poziomie systemu informatycznego

Poziom 2 hierarchii zarządzania ryzykiem i cykl życia systemu określają cel i zakres działań związanych z szacowaniem ryzyka na poziomie 3. Podczas gdy wstępne szacowanie ryzyka (tj. szacowanie ryzyka wykonywane po raz pierwszy, a nie uaktualnianie wcześniejszych szacowań ryzyka) mogą być wykonywane na dowolnym etapie cyklu życia systemu,

[39] Krytyczność systemów informatycznych dla misji organizacji/funkcji biznesowych może być określona w Analizach Wpływu na Działalność (*ang. Business Impact Analyses - BIA*).

w idealnym przypadku szacowania te powinny być wykonywane w fazie początkowej [40]. Szacowania takie informują o reakcji na ryzyko, umożliwiając właścicielom systemów informatycznych/zarządzającym programami, wraz z właścicielami procesów biznesowych, podjęcie ostatecznych decyzji o koniecznych zabezpieczeniach w oparciu o kategoryzację bezpieczeństwa i środowisko działania. Szacowania ryzyka przeprowadzane są również w późniejszych fazach cyklu życia systemu, aktualizując wyniki szacowania ryzyka z wcześniejszych faz. Wyniki szacowania ryzyka systemów informatycznych w fazie powykonawczej lub w odniesieniu do już wdrożonych systemów informatycznych zazwyczaj zawierają opisy podatności w systemach, ocenę ryzyka związanego z każdą z podatności (tym samym aktualizację oceny dotkliwości podatności) oraz działania naprawcze, które mogą być podjęte w celu ograniczenia ryzyka. Wyniki szacowania ryzyka obejmują również ocenę ogólnego ryzyka dla podmiotu oraz informacji zawartych w systemach informatycznych. Wyniki szacowania ryzyka na poziomie 3 są przekazywane komórkom organizacyjnym zajmującym się szacowaniem ryzyka na poziomie 1 i poziomie 2.

Działania związane z szacowaniem ryzyka mogą być zintegrowane z krokami zawartymi w Ramach Zarządzania Ryzykiem (RMF), określonych w NSC 800-37 „*Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu*". RMF, w ramach podejścia opartego na cyklu życia systemu, działa przede wszystkim na poziomie 3, z pewnym zastosowaniem na poziomie 1 i 2, na przykład w zakresie wyboru zabezpieczeń wspólnych. Szacowania ryzyka mogą być dostosowane do każdego etapu w ramach RMF, co znajduje odzwierciedlenie w celu i zakresie ocen opisanych w sekcji 3.1. Szacowania ryzyka mogą również pomóc w określeniu rodzaju ocen bezpieczeństwa przeprowadzanych na różnych etapach cyklu życia systemu, częstotliwości takich szacunków, poziomu rygoryzmu stosowanego podczas szacowania, stosowanych metod szacowania oraz rodzajów/liczby ocenianych obiektów. Korzyści

[40] Specjalna publikacja NIST SP 800-64 zawiera wytyczne dotyczące zagadnień bezpieczeństwa w cyklu życia systemu.

z szacowania ryzyka przeprowadzanego w ramach RMF mogą być realizowane zarówno na podstawie szacunków wstępnych, jak i szacunków zaktualizowanych, jak opisano poniżej.

Krok 1 RMF – Kategoryzacja

Podmioty powinny wykorzystywać wstępne szacowanie ryzyka do podejmowania decyzji w zakresie kategoryzacji bezpieczeństwa zgodnych ze strategią zarządzania ryzykiem przedstawioną przez organ wykonawczy (zarząd, kierownictwo) oraz jako etap przygotowawczy do selekcji zabezpieczeń. Przeprowadzenie wstępnego szacowania ryzyka pozwala na zebranie dostępnych informacji o źródłach zagrożeń, zdarzeniach zagrożeń, podatnościach i uwarunkowaniach predysponujących do wykorzystania tych informacji w celu dokonania kategoryzacji informacji i systemów informatycznych w oparciu o znane i potencjalne zagrożenia i podatności w systemach informatycznych organizacji i środowiskach, w których te systemy funkcjonują[41]. Decyzje dotyczące kategoryzacji bezpieczeństwa wpływają na wybór wstępnych zabezpieczeniach bazowych. Służą one, jako punkt wyjścia do organizacyjnego dostosowania i uzupełnienia działań opisanych w kroku 2 RMF - Wybór.

Krok 2 RMF – Wybór

Organizacje powinny wykorzystywać szacowania ryzyka do informowania i kierowania wyborem zabezpieczeń dla systemów informatycznych podmiotu i środowiska jego pracy. Po dokonaniu wstępnego wyboru poziomu bazowego zabezpieczenia w oparciu o proces kategoryzacji bezpieczeństwa, wyniki szacowania ryzyka są pomocne dla podmiotu w: (i) zastosowaniu odpowiednich wytycznych w celu dostosowania zabezpieczeń w oparciu o konkretne wymagania wynikające z realizowanych zadań, założenia, ograniczenia, priorytety, kompromisy lub inne warunki określone przez podmiot; oraz (ii) uzupełnieniu zabezpieczeń w oparciu o konkretne i wiarygodne informacje o zagrożeniach[42]. Dane

[41] Nawet, jeśli wstępna ocena ryzyka jest przeprowadzana przed utworzeniem systemu informatycznego, podatności mogą występować w określonych technologiach, które będą wykorzystywane w systemie, w zabezpieczeniach wspólnych, które będą dziedziczone przez system, lub w środowisku, w którym system będzie funkcjonował.

[42] Dodatkowe informacje zostaną włączone do procesu dostosowywania w publikacji NSC 800-53.

o zagrożeniach pochodzące z szacowania ryzyka dostarczają krytycznych informacji na temat możliwości, zamiarów i celów, które mogą mieć wpływ na decyzje podmiotu dotyczące wyboru dodatkowych zabezpieczeń, w tym związanych z nimi kosztów i korzyści. Podmioty biorą również pod uwagę wyniki szacowania ryzyka przy wyborze zabezpieczeń wspólnych (*ang. Common Control*), zazwyczaj w zakresie działania z poziomu 1 i 2. Ryzyko wprowadza się, jeżeli wdrożenie zabezpieczeń wspólnych prowadzi do pojedynczego punktu awarii, ponieważ zabezpieczenie takie ma zapewniać zdolność ochrony potencjalnie dziedziczoną przez wiele systemów informatycznych. Ponieważ szacunki ryzyka są aktualizowane i udoskonalane, podmioty wykorzystują ich wyniki do modyfikowania bieżących wyborów w zakresie zabezpieczeń w oparciu o najnowsze dostępne informacje na temat zagrożeń i podatności na zagrożenia.

Krok 3 RMF – Wdrożenie

Podmioty powinny wykorzystywać wyniki szacowania ryzyka w celu określenia alternatywnych sposobów wdrażania wybranych zabezpieczeń (np. biorąc pod uwagę podatności charakterystyczne dla jednego wdrożenia zabezpieczenia w porównaniu z innym). Niektóre produkty informatyczne, komponenty systemów lub konfiguracje architektoniczne mogą być bardziej podatne na pewne rodzaje źródeł zagrożeń, podatności te są następnie uwzględniane podczas opracowywania i wdrażania zabezpieczeń. Ponadto, siła mechanizmów zabezpieczeń wybranych do wdrożenia może uwzględniać dane o zagrożeniach pochodzące z szacowania ryzyka. Indywidualne ustawienia konfiguracyjne produktów informatycznych i komponentów systemu mogą eliminować podatności zidentyfikowane podczas analizy zdarzeń zagrożeń. Wyniki szacowania ryzyka są również pomocne przy podejmowaniu decyzji dotyczących kosztów, korzyści i kompromisów w zakresie ryzyka przy korzystaniu z jednego rodzaju technologii w stosunku do innego lub sposobu skutecznego wdrażania zabezpieczeń w poszczególnych środowiskach operacyjnych (np. jeżeli muszą być zastosowane zabezpieczenia zamienne ze względu na niedostępność niektórych technologii). Ponieważ szacowania ryzyka są aktualizowane i udoskonalane, podmioty wykorzystują ich wyniki, aby pomóc w ustaleniu, czy obecne wdrożenia zabezpieczeń są nadal skuteczne, biorąc pod uwagę zmiany w przestrzeni zagrożeń.

Krok 4 RMF – Ocena

Podmioty powinny wykorzystywać wyniki ocen zabezpieczeń do informowania o ocenie ryzyka. Oceny zabezpieczeń (dokumentowane w raportach z oceny bezpieczeństwa) identyfikują podatności w systemach informatycznych podmiotu oraz w środowiskach, w których systemy te działają. Częściowe lub całkowite niepowodzenie skuteczności wdrożonych zabezpieczeń lub brak planowanych zabezpieczeń stanowi potencjalne podatności, które mogą być wykorzystane przez źródła zagrożeń. Podmioty korzystają z wyników szacowania ryzyka, aby określić powagę takich podatności, które z kolei mogą ukierunkować reakcje podmiotu na ryzyko (np. priorytetyzacja działań w zakresie reagowania na ryzyko, wyznaczenie etapów działań naprawczych).

Krok 5 RMF – Autoryzacja

Podmioty powinny wykorzystywać wyniki szacowania ryzyka w celu dostarczenia informacji związanych z ryzykiem do osób autoryzujących. Reakcje na ryzyko podejmowane przez organizacje w oparciu o szacowanie ryzyka skutkują znajomością stanu bezpieczeństwa systemów informatycznych podmiotu i ich środowisk pracy. Wyniki szacowania ryzyka dostarczają istotnych informacji umożliwiających osobom autoryzującym podjęcie decyzji w oparciu o wynik szacowania ryzyka, czy należy korzystać z tych systemów w obecnym stanie bezpieczeństwa, czy też należy podjąć działania w celu zapewnienia dodatkowych zabezpieczeń, a tym samym dalszego zmniejszenia ryzyka dla operacji i aktywów podmiotu, osób, innych organizacji lub Państwa.

Krok 6 RMF – Monitorowanie

Podmioty powinny na bieżąco aktualizować szacowanie ryzyka, wykorzystując informacje dotyczące bezpieczeństwa pochodzące z procesów ciągłego monitorowania stosowanych w podmiocie[43]. Ocena wynikająca z procesów ciągłego monitorowania obejmuje: (i) skuteczność zabezpieczeń; (ii) zmiany w systemach informatycznych i środowiskach ich

[43] Publikacja specjalna NIST SP 800-137 zawiera wytyczne dotyczące ciągłości monitorowania bezpieczeństwa informacji w systemach informatycznych i organizacjach.

działania; oraz (iii) zgodność z przepisami prawa, zasadami, standardami i wytycznymi. W miarę jak szacowania ryzyka są aktualizowane i udoskonalane, podmioty wykorzystują ich wyniki do aktualizacji celów zarządzania ryzykiem, włączając tym samym doświadczenia zdobyte w procesach zarządzania ryzykiem, poprawiając reakcje na ryzyko oraz budując solidną podstawę informacji o zagrożeniach i podatnościach dostosowanych do celu działania podmiotu.

2.4.4. Komunikacja w zakresie ryzyka i wymiana informacji

Proces szacowania ryzyka wiąże się z bieżącą komunikacją i wymianą informacji między zainteresowanymi stronami w celu zapewnienia tego, że: (i) dane wejściowe do takich szacunków są jak najdokładniejsze; (ii) wyniki szacowań pośrednich mogą być wykorzystywane na przykład do wspierania szacowania ryzyka na innych poziomach; oraz (iii) wyniki są znaczącym i użytecznym wkładem na etapie reagowania na ryzyko w procesie zarządzania ryzykiem. Sposób i forma komunikowania o ryzyku są wyrazem kultury organizacyjnej podmiotu, a także ograniczeń prawnych, regulacyjnych i umownych. Aby komunikacja o ryzyku związanym z bezpieczeństwem informacji i innych informacji związanych z ryzykiem, która powstaje w trakcie szacowania ryzyka, była skuteczna, musi ona być spójna z innymi formami komunikacji o ryzyku w podmiocie. W celu zmaksymalizowania korzyści płynących z szacowania ryzyka, podmioty powinny ustanowić zasady, procedury i mechanizmy wdrożeniowe zapewniające, że informacje uzyskane w trakcie szacowania są skutecznie przekazywane i udostępniane na wszystkich trzech poziomach zarządzania ryzykiem[44]. W celu wzmocnienia znaczenia komunikacji i wymiany informacji o ryzyku w podmiocie, tabele danych wejściowych w Załącznikach (tj. źródła zagrożeń, zdarzenia zagrożeń, podatności, warunki predysponujące, prawdopodobieństwo, wpływ i ryzyko) oraz zalecane elementy raportu z szacowania ryzyka odnoszą się do komunikacji/podziału ryzyka pomiędzy poszczególnymi poziomami.

[44] Publikacje specjalne NIST SP 800-117 i SP 800-126 zawierają wytyczne dotyczące programu" Automatyczny protokół zabezpieczeń zawartości" (ang. Security Content Automation Protocol - SCAP). Program SCAP zapewnia standardowy, spójny sposób przekazywania informacji o zagrożeniach i podatnościach.

UKIERUNKOWANE SZACOWANIE RYZYKA

Podmioty powinny korzystać z ukierunkowanych szacowań ryzyka, których zakres jest ściśle określony, w celu uzyskania odpowiedzi na konkretne pytania (np. jakie jest ryzyko związane z poleganiem na danej technologii, w jaki sposób należy zmienić wcześniejsze szacowanie ryzyka na podstawie zaistniałych zdarzeń, jakie nowe rodzaje ryzyka można zidentyfikować na podstawie wiedzy o nowo odkrytym zagrożeniu lub podatności na zagrożenia) lub w celu podjęcia konkretnych decyzji (np. jakie rodzaje ryzyka powinny być zarządzane na poziomie 1, a nie na poziomie 2 lub 3). Podmioty powinny rozważyć przeprowadzenie szacowanie ryzyka na poziomie 1 i 2, wynikającego ze zbioru wspólnych zagrożeń i podatności na zagrożenia, mających zastosowanie do szerokiego zakresu systemów informatycznych podmiotu. Szacowanie ryzyka na poziomie 1 i 2 pozwala podmiotom na zmniejszenie liczby zagrożeń i podatności na zagrożenia rozpatrywanych na poziomie poszczególnych systemów informatycznych oraz na opracowanie wspólnych reakcji na ryzyko dla takich zagrożeń w skali całego podmiotu. Podejście to może wspierać wspólny dla organizacji proces selekcji zabezpieczeń oraz zwiększać skuteczność i efektywność kosztową szacowani ryzyka w całym podmiocie.

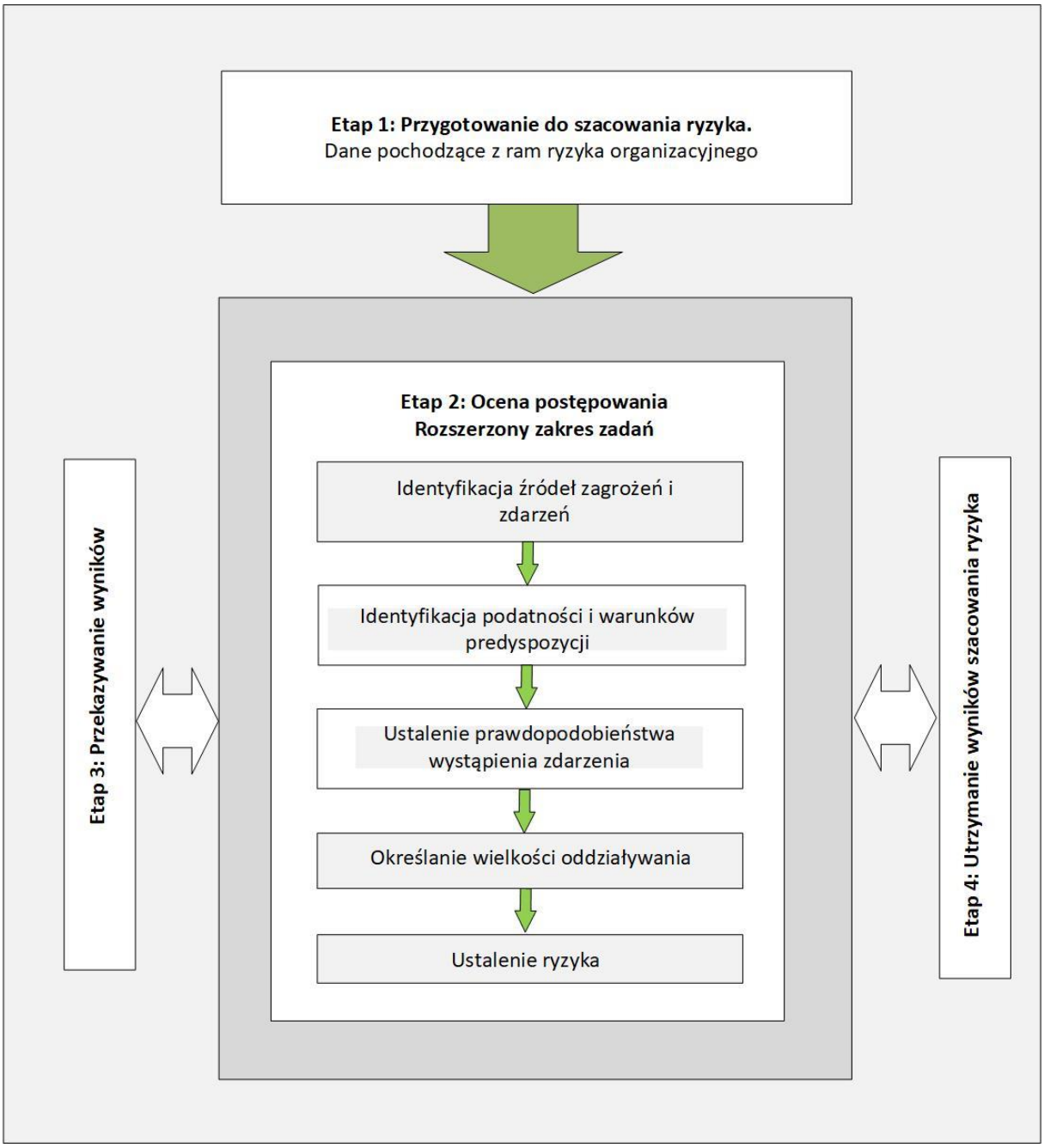
W odniesieniu do wszystkich trzech poziomów w hierarchii zarządzania ryzykiem nie ma szczególnych wymagań w tym zakresie: (i) formalności, rygoru lub poziomu szczegółowości charakteryzujących dane szacowanie ryzyka; (ii) metodologii, narzędzi i technik stosowanych do przeprowadzania takich szacowań ryzyka; lub (iii) formatu i treści wyników szacowania oraz wszelkich związanych z nimi mechanizmów sprawozdawczości. Podmioty dysponują maksymalną elastycznością w zakresie sposobu przeprowadzania szacowania ryzyka, miejsca jego przeprowadzania oraz sposobu wykorzystania jego wyników. Zachęca się organizacje do korzystania z wytycznych w sposób, który będzie najbardziej skuteczny i efektywny kosztowo i zapewni informacje niezbędne dla kierowników wyższego szczebla/wykonawców w celu ułatwienia podejmowania świadomych decyzji w zakresie zarządzania ryzykiem.

ROZDZIAŁ 3 PROCES PROWADZENIA SZACOWANIA RYZYKA W PODMIOCIE

W niniejszym rozdziale opisano proces szacowania ryzyka związanego z bezpieczeństwem informacji, w tym: (i) ogólny zarys procesu szacowania ryzyka; (ii) działania niezbędne do przygotowania do szacowania ryzyka; (iii) działania niezbędne do przeprowadzenia skutecznych szacunków ryzyka; (iv) działania niezbędne do przekazania wyników szacowania i wymiany informacji związanych z ryzykiem; oraz (v) działania niezbędne do utrzymania wyników szacowania ryzyka na bieżąco. Proces szacowania ryzyka[45] składa się z czterech etapów: (i) przygotowania się do szacowania; (ii) przeprowadzenia szacowania; (iii) przekazania wyników szacowania; oraz (iv) utrzymania efektów szacowania Każdy etap podzielony jest na szereg zadań[46]. W przypadku każdego zadania podane są wskazówki zawierają dodatkowe informacje dla podmiotów przeprowadzających szacowanie ryzyka. Tabele ryzyka i przykładowe skale oceny są wymienione w odpowiednich zadaniach i odsyłają do dodatkowych, bardziej szczegółowych informacji w Załącznikach. Rys. 5 ilustruje podstawowe kroki w procesie szacowania ryzyka i podkreśla konkretne zadania związane z jego przeprowadzaniem.

[45] Intencją opisu procesu w rozdziale trzecim jest zapewnienie wspólnego wyrażenia istotnych elementów skutecznej oceny ryzyka. Nie ma on na celu ograniczenia elastyczności organizacyjnej w przeprowadzaniu tych ocen. Możliwe jest wdrożenie innych procedur, jeśli organizacje się na to zdecydują, zgodnie z intencją opisu procesu.

[46] Czteroetapowy proces oceny ryzyka opisany w niniejszej publikacji jest zgodny z ogólnym procesem oceny ryzyka opisanym w publikacji NSC 800-39. Dodatkowe kroki i zadania wynikają z potrzeby dostarczenia bardziej szczegółowych wytycznych, które pozwolą na efektywne przeprowadzenie specyficznych działań związanych z oceną ryzyka.



Rysunek 5. Proces szacowania ryzyka.

3.1. Przygotowanie do szacowania ryzyka

Pierwszym krokiem w procesie szacowania ryzyka jest przygotowanie się do tej oceny. Celem tego etapu jest stworzenie kontekstu dla szacowania ryzyka. Kontekst ten jest ustalany i uwzględniany na podstawie wyników etapu określania ryzyka w procesie zarządzania

ryzykiem. Ramowy system zarządzania ryzykiem identyfikuje na przykład informacje organizacyjne dotyczące zasad i wymogów w zakresie przeprowadzania szacowania ryzyka, konkretnych metodyk szacowania, które należy zastosować, procedur wyboru czynników ryzyka, które należy uwzględnić, zakresu oceny, rygoru analiz, stopnia formalności oraz wymogów, które ułatwiają spójne i powtarzalne określanie ryzyka w całym podmiocie. Podmioty stosują strategię zarządzania ryzykiem w zakresie, w jakim jest to możliwe, w celu uzyskania informacji niezbędnych do przygotowania się do szacowania ryzyka.
Przygotowanie do szacowania ryzyka obejmuje następujące zadania:

- określenie celu szacowania;
- określenie zakresu szacowania;
- ustalenie założeń i ograniczeń związanych z szacowaniem;
- zidentyfikowanie źródeł informacji, które należy wykorzystać jako dane wejściowe do szacowania;
- określenie modelu ryzyka i podejścia analitycznego (tzn. podejścia do oceny i analizy), które mają być stosowane podczas szacowania.

Krok 1: Przygotowanie do szacowania ryzyka

Cel identyfikacji

Zadanie 1-1: Określić cel szacowania ryzyka w odniesieniu do informacji, które szacowanie ma dostarczyć oraz decyzji, które szacowanie ma wspierać.

Dodatkowe wskazówki: Cel szacowania ryzyka powinien być określony wystarczająco szczegółowo, aby zapewnić, że szacowanie dostarczy odpowiednich informacji i wesprze planowane decyzje. Podmioty powinny udzielić wskazówek, w jaki sposób uchwycić i przedstawić informacje uzyskane podczas szacowania ryzyka (np. przy użyciu określonego szablonu organizacyjnego). Załącznik K zawiera przykładowy szablon sprawozdania z oceny ryzyka oraz preferowany sposób przekazania informacji o ryzyku. Na poziomie 3, wsparcie szacowania ryzyka obejmuje: (i) decyzje związane z udzielaniem zezwoleń w całym cyklu życia systemu; (ii) wzajemność, w szczególności w przypadku ponownego wykorzystywania

informacji dotyczących oceny; (iii) działania związane z zarządzaniem ryzykiem na poziomie 2; oraz (iv) działania związane z programowym zarządzaniem ryzykiem w całym cyklu życia systemu. Na poziomie 2 oceny ryzyka umożliwiają organizacjom: (i) zrozumienie zależności i sposobów akceptowania, odrzucania, dzielenia się, przekazywania lub ograniczania ryzyka pomiędzy systemami informatycznymi, które wspierają procesy biznesowe podmiotu; (ii) wspieranie decyzji architektonicznych i operacyjnych w zakresie reagowania na ryzyko organizacyjne (np. ograniczanie zależności, ograniczanie łączności, wzmocnienie lub ukierunkowanie monitorowania oraz zwiększenie odporności informacji/systemów); (iii) identyfikację trendów w celu określenia proaktywnych celów reagowania na ryzyko i kierunków działań w zakresie procesów biznesowych; oraz (iv) wspieranie wzajemności, w szczególności w celu umożliwienia wymiany informacji. Na poziomie 1, oceny ryzyka: (i) stanowią wsparcie dla organu wykonawczego ds. ryzyka (funkcji); oraz (ii) służą jako kluczowy wkład w strategię zarządzania ryzykiem. Oprócz tych wspólnych celów, szacowanie ryzyka może mieć bardzo konkretny cel, polegający na udzieleniu odpowiedzi na konkretne pytanie (np. jakie są implikacje ryzyka odnoszącego się do nowo odkrytej podatności lub klasy podatności, umożliwienie nowej komunikacji, outsourcing określonej funkcji lub przyjęcie nowej technologii?) Wyniki szacowania ryzyka na wszystkich poziomach mogą być wykorzystywane przez podmioty do informowania o procesie akwizycji systemów poprzez pomoc w zapewnieniu, że wymagania dotyczące bezpieczeństwa informacji są jasno określone.

Na cel szacowania ryzyka ma wpływ to, czy jest to: (i) szacowanie wstępne; lub (ii) kolejne szacowanie zainicjowane na podstawie reakcji na ryzyko lub wynikające z etapów monitorowania w procesie zarządzania ryzykiem. W przypadku szacowania wstępnego cel może: (i) ustanowienie podstawowej oceny ryzyka; lub (ii) identyfikację zagrożeń i podatności, wpływu na działalność podmiotu i jej aktywa, osoby fizyczne, inne organizacje i społeczeństwo oraz innych czynników ryzyka, które należy śledzić w czasie, w ramach monitorowania ryzyka. W przypadku ponownego szacowania wykonywanego na etapie reagowania na ryzyko, celem może być na przykład przedstawienie analizy porównawczej alternatywnych reakcji na ryzyko lub udzielenie odpowiedzi na konkretne pytanie (zob.

omówienie docelowych szacowań ryzyka powyżej). Alternatywnie, w przypadku ponownego szacowania rozpoczętego od etapu monitorowania ryzyka, celem może być na przykład aktualizacja szacowania ryzyka na podstawie tego szacowania: (i) bieżące określanie skuteczności zabezpieczeń w systemach informatycznych organizacji lub środowiskach ich działania; (ii) zmiany w systemach informatycznych lub środowiskach ich działania (np. zmiany w sprzęcie komputerowym, oprogramowaniu sprzętowym i oprogramowaniu aplikacyjnym; zmiany w zakresie zabezpieczeń specyficznych dla danego systemu, zabezpieczeń hybrydowych lub wspólnych; zmiany w zakresie procesów biznesowych, wspólnej infrastruktury i usług wsparcia, zagrożeń, podatności lub obiektów); oraz (iii) wyniki działań w zakresie weryfikacji zgodności. Ponowne szacowanie może być również inicjowane przez podmioty w związku z wystąpieniem incydentów (np. cyberataków zagrażających informacjom lub systemom informatycznym).

Zakres Identyfikacji

Zadanie 1-2: Zidentyfikuj zakres szacowania ryzyka pod względem możliwości organizacyjnych, ram czasowych oraz względów architektonicznych/technologicznych.

Dodatkowe wskazówki: Zakres szacowania ryzyka określa, co zostanie uwzględnione podczas tego szacowania. Zakres szacowania ryzyka wpływa na zakres informacji dostępnych do podejmowania decyzji opartych na ryzyku i jest określany przez osobę wnioskującą o dokonanie szacowania oraz strategię zarządzania ryzykiem. Ustalenie zakresu szacowania ryzyka pomaga podmiotom w ich określeniu: (i) jakie poziomy są uwzględniane w ocenie; (ii) na które części podmiotu ma wpływ szacowanie i w jaki sposób wpływa on na nie; (iii) jakie decyzje są poparte wynikami szacowania; (iv) jak długo wyniki szacowania są istotne; oraz (v) co wpływa na potrzebę aktualizacji szacowania. Ustalenie zakresu szacowania ryzyka pomaga określić formę i treść raportu z szacowania ryzyka, a także informacje, którymi należy się podzielić w wyniku przeprowadzenia szacowania. Na poziomie 3 zakres szacowania ryzyka może zależeć od granic uprawnień do systemu informatycznego. W dodatku K przedstawiono przykładowy rodzaj informacji, które mogą być zawarte

w sprawozdaniu z szacowania ryzyka lub preferowanym sposobie służącym do informowania o ryzyku.

Zastosowanie organizacyjne

Zastosowanie organizacyjne opisuje, na które części organizacji ma wpływ szacowanie ryzyka i wynikające z niego decyzje oparte na ryzyku (w tym wskazuje części organizacji odpowiedzialne za realizację działań i zadań związanych z tymi decyzjami). Na przykład, szacowanie ryzyka może informować o decyzjach dotyczących systemów informatycznych wspierających konkretną funkcję organizacji lub proces biznesowy. Może to obejmować decyzje dotyczące wyboru, dostosowania lub uzupełnienia zabezpieczeń dla konkretnych systemów informatycznych lub wybór zabezpieczeń wspólnych. Alternatywnie, szacowanie ryzyka może informować o decyzjach dotyczących zestawu ściśle powiązanych funkcji lub procesów biznesowych. Zakres szacowania ryzyka może obejmować nie tylko funkcje, zadania, procesy biznesowe, wspólną infrastrukturę lub wspólne usługi, od których podmiot jest obecnie zależny, ale także te, z których podmiot może korzystać w określonych warunkach operacyjnych.

Efektywność ram czasowych

Podmioty określają, jak długo wyniki poszczególnych szacowań ryzyka mogą być wykorzystywane do uzasadnionego podejmowania decyzji opartych na ryzyku. Ramy czasowe są zazwyczaj związane z celem szacowania. Na przykład, szacowanie ryzyka mające na celu poinformowanie o decyzjach związanych z polityką Poziomu 1 musi być istotne przez dłuższy okres czasu, ponieważ w wielu podmiotach proces zarządzania zmianami polityki może być czasochłonny. Szacowanie ryzyka przeprowadzone w celu poinformowania o decyzji Poziomu 3 dotyczącej wykorzystania kompensacyjnego zabezpieczenia systemu informatycznego może być istotna jedynie do czasu kolejnego wprowadzenia do obrotu produktu informatycznego zapewniającego wymagane zdolności w zakresie bezpieczeństwa. Podmioty określają okres użytkowania wyników szacowania ryzyka oraz warunki, w jakich aktualne wyniki szacowania stają się nieskuteczne lub nieistotne. Monitorowanie ryzyka może być stosowane w celu określenia skuteczności ram czasowych szacowania ryzyka.

Oprócz wyników szacowania ryzyka, podmioty biorą pod uwagę również terminowość (tzn. zmiany istotności informacji w funkcji czasu) wszystkich rodzajów informacji/danych wykorzystywanych do szacowania ryzyka. Ma to szczególne znaczenie przy ponownym wykorzystywaniu informacji i ocenie ważności wyników szacowania.

Aspekty architektoniczne/technologiczne

Podmioty wykorzystują aspekty architektoniczne i technologiczne do wyjaśnienia zakresu szacowania ryzyka. Na przykład, na poziomie 3, zakresem szacowania ryzyka może być system informatyczny podmiotu w jego środowisku działania. Pociąga to za sobą umieszczenie systemu informatycznego w jego kontekście architektonicznym, tak aby można było uwzględnić podatności zabezpieczeń dziedzicznych. Alternatywnie, zakres szacowania może być ograniczony wyłącznie do systemu informatycznego, bez uwzględniania podatności dziedzicznych. Na poziomie 2 zakres szacowania ryzyka można zdefiniować w odniesieniu do architektury segmentu zadań (np. w tym wszystkich systemów, usług i infrastruktury, które wspierają dany cel/funkcję). W przypadku ukierunkowanego szacowania ryzyka na dowolnym poziomie, konkretne pytanie, na które należy odpowiedzieć, może ograniczyć zakres do pytań odnoszących się do konkretnej technologii.

Określanie założeń i ograniczeń

Zadanie 1-3: Określ konkretne założenia i ograniczenia, w ramach których przeprowadzana jest ocena ryzyka.

Dodatkowe wskazówki: W ramach etapu określania ram ryzyka w procesie zarządzania ryzykiem, podmioty wyraźnie określają konkretne założenia, ograniczenia, tolerancję ryzyka oraz priorytety i kompromisy stosowane w ramach podmiotu przy podejmowaniu decyzji inwestycyjnych i operacyjnych. Informacje te stanowią przewodnik i źródło informacji na temat szacowania ryzyka w organizacji. W przypadku, gdy strategia zarządzania ryzykiem w podmiocie nie może być cytowana, szacowania ryzyka identyfikują i dokumentują założenia i ograniczenia. Założenia i ograniczenia zidentyfikowane przez podmiot na etapie definiowania ryzyka i włączone jako część celów zarządzania ryzykiem w podmiocie, nie muszą być powtarzane w każdym indywidualnym szacowaniu ryzyka. Dzięki wyraźnemu

określeniu założeń i ograniczeń, model ryzyka wybrany do szacowania ryzyka staje się bardziej przejrzysty, a wyniki szacowania są powtarzalne oraz zwiększa się szansa na porównywalność wyników pomiędzy różnymi podmiotami. Podmioty identyfikują założenia w kluczowych obszarach istotnych dla szacowania ryzyka, w tym np.: (i) źródła zagrożeń; (ii) zdarzenia powodujące zagrożenie; (iii) podatności i warunki predysponujące; (iv) potencjalne skutki; (v) podejścia do oceny i analizy; oraz (vi) które zadania/funkcje biznesowe są najważniejsze. Organizacje określają również ograniczenia w kluczowych obszarach istotnych dla szacowania ryzyka, w tym np.: (i) zasoby dostępne na potrzeby szacowania; (ii) umiejętności i wiedza specjalistyczna wymagane na potrzeby szacowania; oraz (iii) względy operacyjne związane z celem/działalnością biznesową. Na przykład, założenia w danym podmiocie dotyczące sposobu oceny zagrożeń i skutków mogą być różne – od wykorzystania prognoz najgorszego przypadku do wykorzystania prognoz najlepszego przypadku lub innych elementów znajdujących się pomiędzy tymi punktami krańcowymi. Wreszcie, podmioty biorą pod uwagę niepewność w odniesieniu do przyjętych założeń lub innych informacji wykorzystanych w szacowaniu ryzyka. Niepewność założeń może mieć wpływ na tolerancję ryzyka w podmiocie. Na przykład, założenia oparte na braku konkretnych lub wiarygodnych informacji mogą zmniejszyć tolerancję podmiotu na ryzyko ze względu na niepewność wpływającą z tych założeń. W kolejnych sekcjach przedstawiono kilka reprezentatywnych przykładów obszarów, w których można zidentyfikować założenia lub ograniczenia dotyczące szacowania ryzyka.

Źródła zagrożeń

Podmioty określają, jakie rodzaje źródeł zagrożeń należy uwzględnić podczas szacowania ryzyka. Podmioty wyraźnie określają proces identyfikacji zagrożeń i wszelkie założenia związane z procesem identyfikacji zagrożeń. Jeżeli takie informacje zostaną zidentyfikowane na etapie definiowania ryzyka i włączone do celów zarządzania ryzykiem w podmiocie, nie muszą być powtarzane w każdej indywidualnym szacowaniu ryzyka. Szacowania ryzyka mogą dotyczyć wszystkich rodzajów źródeł zagrożeń, jednego szerokiego źródła zagrożeń (np. o charakterze kontradyktoryjnym) lub konkretnego źródła zagrożeń (np. zaufane osoby mające dostęp do informacji poufnych). Tabela D-2 przedstawia przykładową taksonomię

źródeł zagrożeń, które mogą być brane pod uwagę przez podmioty przy określaniu założeń do szacowania ryzyka. Założenia w podmiocie dotyczące źródeł zagrożeń są do rozważenia w ramach zadania 2-1.

Zdarzenia zagrożeń

Podmioty określają, jaki rodzaj zdarzeń zagrożeń należy uwzględnić podczas szacowania ryzyka oraz poziom szczegółowości niezbędny do opisania takich zdarzeń. Opisy zdarzeń zagrożeń mogą być wyrażone w sposób bardzo ogólny (np. phishing, rozproszona odmowa usługi), bardziej opisowy przy użyciu taktyki, technik i procedur lub w sposób bardzo szczegółowy (np. nazwy konkretnych systemów informatycznych, technologii, podmiotów ról lub lokalizacji). Ponadto, podmioty biorą pod uwagę: (i) jaki reprezentatywny zestaw zdarzeń powodujących zagrożenie może służyć jako punkt wyjścia do identyfikacji konkretnych zdarzeń powodujących zagrożenie w szacowaniu ryzyka; oraz (ii) jaki stopień potwierdzenia jest potrzebny, aby zdarzenia powodujące zagrożenie zostały uznane za istotne dla celów szacowania ryzyka. Na przykład podmioty mogą uwzględniać tylko te zdarzenia zagrożeń, które zostały zaobserwowane (wewnętrznie lub przez podmioty będące partnerami zewnętrznymi), lub wszystkie możliwe zdarzenia zagrożeń. Tabela E-2 i tabela E-3 przedstawiają reprezentatywne przykłady agresywnych i nieagresywnych zdarzeń zagrożeń na poziomie szczegółowości, które mogą być wykorzystane do szacowania ryzyka na wszystkich poziomach. Bardziej szczegółowe informacje można znaleźć w wielu źródłach (np. we wspólnym wykazie i klasyfikacji wzorów ataków [CAPEC][47]). Założenia mające miejsce w podmiocie dotyczące zdarzeń zagrażających, które należy rozważyć, oraz poziom szczegółowości podano w zadaniu 2-2.

Podatności i warunki predyspozycji

Podmioty określają rodzaje podatności, które należy uwzględnić podczas szacowania ryzyka oraz poziom szczegółowości opisów podatności. Podmioty wyraźnie określają proces wykorzystywany do identyfikacji podatności oraz wszelkie założenia związane z procesem

[47] Lista wzorów ataków publikowana przez organizację MITRE – https://capec.mitre.org/data/index.html

identyfikacji podatności. Jeśli takie informacje zostaną zidentyfikowane na etapie definiowania ryzyka i włączone do celów zarządzania ryzykiem w podmiocie, nie muszą być powtarzane w każdym indywidualnym szacowaniu ryzyka. Podatności mogą być związane z systemami informatycznymi podmiotu (np. sprzęt, oprogramowanie, firmware, zabezpieczenia wewnętrzne i procedury bezpieczeństwa) lub środowiskami, w których systemy te działają (np. zarządzanie podmiotem, relacje zewnętrzne, procesy misyjne, architektury korporacyjne, architektury bezpieczeństwa informacji). Podmioty określają również rodzaje uwarunkowań predysponujących, które należy uwzględnić podczas szacowania ryzyka, w tym np. stosowane architektury i technologie, środowiska działania i personel. Tabela F-4 zawiera reprezentatywne przykłady takich uwarunkowań predysponujących. Założenia stosowane w podmiocie dotyczące podatności i uwarunkowań predysponujących oraz poziom szczegółowości podano w Zadaniu 2-3.

Prawdopodobieństwo

Podmioty wyraźnie określają proces wykorzystywany do przeprowadzania wyznaczania prawdopodobieństwa oraz wszelkie założenia związane z procesem ustalania prawdopodobieństwa. Jeżeli takie informacje zostaną zidentyfikowane na etapie definiowania ryzyka i włączone do celów zarządzania ryzykiem w podmiocie, nie muszą być powtarzane w każdym indywidualnym szacowaniu ryzyka. Założenia przyjęte w podmiocie dotyczące sposobu określania prawdopodobieństwa zawarte są w zadaniu 2-4.

Wpływ

Podmioty określają potencjalne negatywne skutki w zakresie działań podmiotu (tj. celu, funkcji, wizerunku i reputacji), majątku podmiotu, osób, innych podmiotów i Państwa. Podmioty wyraźnie określają proces wykorzystywany do przeprowadzania określania wpływu oraz wszelkie założenia związane z procesem określania wpływu. Jeżeli takie informacje zostaną zidentyfikowane na etapie definiowania ryzyka i włączone do celów zarządzania ryzykiem w podmiocie, nie muszą być powtarzane w każdym indywidualnym szacowaniu ryzyka. Podmioty zajmują się oddziaływaniem na poziomie szczegółowości, który obejmuje na przykład określone procesy biznesowe lub zasoby informacyjne (np. informacje,

personel, sprzęt, fundusze i technologie informacyjne). Podmioty mogą uwzględniać informacje z analiz wpływu na działalność (BIA) w odniesieniu do dostarczania informacji o wpływie na szacowanie ryzyka. Tabela H-2 zawiera reprezentatywne przykłady rodzajów wpływu (tj. szkód), które mogą być rozważane przez podmiot. Założenia przyjęte w podmiocie dotyczące sposobu określania wpływu i poziomu szczegółowości podano w zadaniu 2-5.

Tolerancja ryzyka i niepewność

Podmioty określają poziomy i rodzaje ryzyka, które są dopuszczalne. Tolerancja ryzyka jest określana jako część celów zarządzania ryzykiem w celu zapewnienia spójności w całym podmiocie. Podmioty udzielają również wskazówek, w jaki sposób określić przyczyny niepewności podczas szacowania czynników ryzyka, ponieważ niepewność jednego lub więcej czynników rozprzestrzeni się na wynik wyznaczania poziomu ryzyka oraz to, w jaki sposób zrekompensować niepełne, niedoskonałe lub zależne od założeń szacunki. Uwzględnienie niepewności jest szczególnie ważne, gdy podmioty rozważają zaawansowane trwałe zagrożenia (APT), ponieważ ocena prawdopodobieństwa wystąpienia zdarzenia zagrożenia może mieć duży stopień niepewności. Aby to zrekompensować, podmioty mogą stosować różne podejścia do określania prawdopodobieństwa, począwszy od założenia najgorszego prawdopodobieństwa (pewne, że zdarzenie zdarzy się w przewidywalnej przyszłości), a skończywszy na założeniu, że jeżeli zdarzenie nie zostanie zaobserwowane, jest mało prawdopodobne, aby do niego doszło. Podmioty określają również, jakie poziomy ryzyka (połączenie prawdopodobieństwa i wpływu) wskazują, że nie jest konieczna dalsza analiza jakichkolwiek czynników ryzyka.

Podejście analityczne

Szacowania ryzyka obejmują zarówno podejścia do szacowania (tj. ilościowe, jakościowe, mieszane), jak i do analizy (tj. zorientowane na zagrożenie, zorientowane na aktywa/wpływ, zorientowane na podatność na zagrożenia). Razem, podejścia do szacowania i analizy tworzą analityczne podejście do oceny ryzyka. Organizacje określają poziom szczegółowości i formę, w jakiej analizowane są zagrożenia, w tym poziom szczegółowości w celu opisania zdarzeń

lub scenariuszy zagrożeń. Różne podejścia analityczne mogą prowadzić do różnych poziomów szczegółowości w charakteryzowaniu zdarzeń niepożądanych, dla których określa się prawdopodobieństwo. Na przykład, zdarzenie niepożądane może być scharakteryzowane na kilka sposobów (o coraz wyższym poziomie szczegółowości): (i) zdarzenie powodujące zagrożenie (dla którego prawdopodobieństwo określa się poprzez przyjęcie maksymalnych ogólnych źródeł zagrożenia); (ii) połączenie zdarzenia powodującego zagrożenie ze źródłem zagrożenia; lub (iii) szczegółowy scenariusz zagrożenia/drzewo ataków. Ogólnie rzecz biorąc, można oczekiwać, że podmioty będą wymagały bardziej szczegółowych informacji na temat celów/funkcji biznesowych o wysokim stopniu krytyczności, wspólnej infrastruktury lub wspólnych usług, od których zależy wiele celu lub funkcji biznesowych (jako od wspólnych punktów awarii) oraz systemów informacyjnych o wysokim stopniu krytyczności lub wrażliwości. Właściciele procesów/procesów biznesowych mogą rozszerzyć te wytyczne o newralgiczne punkty ryzyka (systemy informatyczne, usługi lub elementy infrastruktury krytycznej o szczególnym znaczeniu).

Identyfikacja źródeł informacji

Zadanie 1-4: Zidentyfikuj źródła informacji opisowych dotyczących zagrożeń, podatności na zagrożenia i wpływu, które należy wykorzystać w szacowaniu ryzyka.

Dodatkowe wskazówki: Informacje opisowe pozwalają podmiotom na określenie przydatności informacji o zagrożeniach i podatnościach na zagrożenia. Na poziomie 1 informacje opisowe mogą obejmować na przykład rodzaj zarządzania ryzykiem i struktury zarządzania bezpieczeństwem informacji istniejące w podmiocie oraz sposób, w jaki podmiot identyfikuje i nadaje priorytety krytycznym celom/funkcjom biznesowym. W przypadku poziomu 2 informacje opisowe mogą obejmować na przykład informacje na temat: (i) celu organizacji/procesów biznesowych, procesów zarządzania funkcjonalnego oraz przepływów informacji; (ii) architektury korporacyjnej, architektury bezpieczeństwa informacji oraz opisów technicznych/przepływów procesowych systemów, wspólnych infrastruktur oraz usług wspólnych, które wchodzą w zakres oceny ryzyka; oraz (iii) zewnętrznych środowisk, w których działa podmiot, w tym na przykład relacji i zależności z zewnętrznymi dostawcami.

Informacje takie znajdują się zazwyczaj w dokumentacji architektonicznej (w szczególności w dokumentacji zaawansowanych widoków operacyjnych), planach ciągłości działania i sprawozdaniach z szacowania ryzyka dotyczących systemów informatycznych podmiotu, wspólnych infrastruktur i usług wspólnych, które wchodzą w zakres szacowania ryzyka. Na poziomie 3 informacje opisowe mogą obejmować na przykład informacje na temat: (i) konstrukcji i technologii wykorzystywanych w systemie informatycznym podmiotu; (ii) środowiska, w którym systemy te działają; (iii) łączności z innymi systemami informatycznymi i zależności od nich; oraz (iv) zależności od wspólnych infrastruktur lub usług wspólnych. Takie informacje znajdują się w dokumentacji systemowej, planach awaryjnych i sprawozdaniach z szacowania ryzyka dla innych systemów, infrastruktur i usług informatycznych.

Źródła informacji opisane w tabelach D-1, E-1, F-1, H-1 i I-1 mogą być w stosunku do podmiotu wewnętrzne lub zewnętrzne. Wewnętrzne źródła informacji, które mogą zapewnić wgląd zarówno w zagrożenia, jak i podatności, mogą obejmować na przykład raporty z szacowania ryzyka, raporty o incydentach, dzienniki bezpieczeństwa, karty kontrolne i wyniki monitoringu. Należy pamiętać, że wewnętrznie informacje pochodzące z raportów szacowania ryzyka na jednym poziomie mogą służyć jako wkład do szacowania ryzyka na innych poziomach. Właściciele celu zachęca się do określenia nie tylko wspólnej infrastruktury lub usług pomocniczych, od których są zależni, ale również tych, z których mogą korzystać w określonych okolicznościach operacyjnych. Zewnętrznymi źródłami informacji o zagrożeniach mogą być organizacje wspólnotowe (np. zespoły CSIRT, partnerzy sektorowi, centra wymiany informacji i analizy [ISAC] dla sektorów infrastruktury krytycznej i operatorów usług kluczowych, organizacje badawcze i pozarządowe oraz dostawcy usług z zakresu bezpieczeństwa). Podmioty korzystające ze źródeł zewnętrznych, biorą pod uwagę aktualność, specyfikę i znaczenie informacji o zagrożeniach. Podobnie jak źródła informacji o zagrożeniach, źródła informacji o podatnościach mogą być w stosunku do podmiotu również wewnętrzne lub zewnętrzne (patrz tabela F-1). Źródła wewnętrzne mogą obejmować na przykład raporty z oceny podatności na zagrożenia. Zewnętrzne źródła informacji o podatności na zagrożenia są podobne do źródeł określonych powyżej dla

informacji o zagrożeniach. Jak opisano w tabeli F-1, informacje o stanach predysponujących można znaleźć w różnych źródłach, w tym na przykład w opisach systemów informatycznych, środowisk pracy, usług wspólnych, wspólnej infrastruktury i architektury korporacyjnej. Jak opisano w tabeli H-1, źródła informacji o oddziaływaniu mogą obejmować na przykład analizy oddziaływania na cel, inwentaryzacje komponentów systemów informatycznych oraz kategoryzację bezpieczeństwa. Kategoryzacja bezpieczeństwa stanowi określenie potencjalnych oddziaływań w przypadku wystąpienia pewnych zdarzeń, które zagrażają informacjom i systemom informatycznym potrzebnym organizacji do realizacji powierzonych jej zadań, ochrony jej aktywów, wypełniania obowiązków prawnych, utrzymania codziennych funkcji i ochrony osób. Kategorie bezpieczeństwa należy stosować w powiązaniu z informacjami o podatności na zagrożenia i zagrożeniach przy ocenie ryzyka dla operacji i aktywów podmiotu, osób, innych podmiotów i Państwa. Kategorie bezpieczeństwa stanowią wstępne podsumowanie skutków w zakresie nieosiągnięcia celów bezpieczeństwa w zakresie poufności, integralności i dostępności, a także wynikają z rodzajów szkód przedstawionych w tabeli H-2.

Określanie modelu ryzyka i podejścia analitycznego

Zadnie 1-5: Określ model ryzyka i podejście analityczne, które należy zastosować w ocenie ryzyka.

Dodatkowe wskazówki: Podmioty definiują jeden lub więcej modeli ryzyka do wykorzystania przy przeprowadzaniu szacowania ryzyka (patrz sekcja 2.3.1) i określają, który model ma być stosowany. W celu zapewnienia wzajemności wyników szacowania, modele ryzyka specyficzne dla danego podmiotu obejmują lub mogą zostać przełożone na czynniki ryzyka (tj. zagrożenie, podatność, wpływ, prawdopodobieństwo i stan predyspozycji) określone w załącznikach. Podmioty określają również specyficzne podejście analityczne, które ma być stosowane do szacowania ryzyka, w tym podejście do szacowania (tzn. ilościowe, jakościowe, mieszane) oraz podejście analityczne (tzn. zorientowane na zagrożenie, zorientowane na aktywa/wpływ, zorientowane na podatność na zagrożenia). Dla każdego czynnika ryzyka podlegającego szacowaniu, załączniki zawierają trzy skale oceny (jedna

jakościowa i dwie mieszane) o odpowiednio różnych przedstawieniach. Podmioty zazwyczaj definiują (lub wybierają i dostosowują z załączników) skale oceny, które mają być stosowane w szacowaniu ryzyka, adnotując je za pomocą przykładów mających znaczenie w podmiocie dla konkretnych wartości oraz definiując punkty krytyczne między koszami w przypadku podejścia mieszanego. Ponadto właściciele procesów mogą zamieszczać dodatkowe adnotacje z przykładami specyficznymi dla danej celu. Podmioty mogą zidentyfikować różne skale oceny, które mogą być stosowane w różnych okolicznościach. Na przykład, w przypadku systemów informatycznych o niewielkim wpływie, podmioty mogą stosować wartości jakościowe, natomiast w przypadku systemów o umiarkowanym i dużym wpływie, można stosować najbardziej ziarniste wartości mieszane (0-100). Jak omówiono w publikacji NSC 800-39, zadanie 1-1 *Założenia dotyczące ryzyka* podmioty różnią się pod względem wag stosowanych do czynników ryzyka. Dlatego też niniejsza wytyczna nie określa algorytmów łączenia wartości mieszanych. Modele ryzyka specyficzne dla podmiotu obejmują algorytmy (np. wzory, tabele, reguły) służące do łączenia czynników ryzyka. Jeżeli model ryzyka specyficznego dla danego podmiotu nie został przedstawiony w celach zarządzania ryzykiem w ramach etapu kadrowania ryzyka, wówczas częścią tego zadania jest określenie algorytmów służących do łączenia wartości. Algorytmy łączenia czynników ryzyka odzwierciedlają tolerancję na ryzyko w podmiocie (przykłady znajdują się w wytycznych uzupełniających do zadania 2-4). Modele ryzyka specyficznego dla podmiotu są dopracowywane w ramach przygotowania do szacowania ryzyka przez: (i) identyfikację modelu ryzyka i uzasadnienie jego stosowania (w przypadku dostarczenia wielu modeli ryzyka specyficznego dla danego podmiotu); (ii) dostarczenie dodatkowych przykładów wartości czynników ryzyka; oraz (iii) identyfikację wszelkich algorytmów specyficznych dla danego szacowania (np. algorytmów specyficznych dla stosowania techniki analizy schematu ataku). W przypadku braku istniejących wcześniej modeli ryzyka specyficznych dla danego podmiotu lub podejść analitycznych zdefiniowanych w celach zarządzania ryzykiem w podmiocie, w zadaniu tym określa się i dokumentuje model ryzyka i podejścia analityczne, które mają być stosowane w szacowaniu ryzyka.

Podsumowanie kluczowych działań – Przygotowanie do szacowania ryzyka

- Określ cel oceny ryzyka.
- Określ zakres oceny ryzyka.
- Określ założenia i ograniczenia, w ramach których przeprowadzane jest szacowanie ryzyka.
- Określ źródła zagrożeń, podatności na zagrożenia i informacje o skutkach, które należy wykorzystać w szacowaniu ryzyka (patrz tabele D-1, E-1, F-1, H-1 i I-1, dostosowane do potrzeb podmiotu).
- Zdefiniuj lub udoskonal model ryzyka, podejście do szacowania i podejście do analizy, które mają być stosowane w szacowaniu ryzyka.

3.2. Przeprowadzenie szacowania ryzyka

Drugim krokiem w procesie szacowania ryzyka jest jego przeprowadzenie. Celem tego etapu jest sporządzenie listy zagrożeń dla bezpieczeństwa informacji, które mogą być uszeregowane według poziomu ryzyka i wykorzystane do podjęcia decyzji dotyczących reakcji na ryzyko. Aby osiągnąć ten cel, podmioty analizują zagrożenia i podatności, skutki i prawdopodobieństwo oraz niepewność związaną z procesem szacowania ryzyka. Etap ten obejmuje również zbieranie istotnych informacji w ramach każdego zadania i jest prowadzony zgodnie z kontekstem szacowania ustalonym w ramach etapu Przygotowywanie procesu szacowania ryzyka. Oczekuje się, że szacowania ryzyka obejmą odpowiednio całą przestrzeń zagrożeń zgodnie ze szczegółowymi definicjami, wytycznymi i kierunkami ustalonymi na etapie przygotowania. W praktyce jednak odpowiednie pokrycie w ramach dostępnych zasobów może wymagać uogólnienia źródeł zagrożeń, zdarzeń i podatności na zagrożenia w celu zapewnienia pełnego pokrycia i oceny konkretnych, szczegółowych źródeł, zdarzeń i podatności na zagrożenia tylko w zakresie niezbędnym do osiągnięcia celów szacowania ryzyka. Przeprowadzanie szacowania ryzyka obejmuje następujące konkretne zadania:

- Identyfikacji źródeł zagrożeń, które są istotne dla podmiotu;

- Identyfikacji zdarzeń zagrożeń, które mogą być wywołane przez te źródła;
- Identyfikacji podatności w podmiocie, które mogą być wykorzystane przez źródła zagrożeń poprzez określone zdarzenia zagrożeń oraz predyspozycje, które mogą mieć wpływ na skuteczną eksploatację;
- Określenie prawdopodobieństwa, że zidentyfikowane źródła zagrożeń zainicjują zdarzenia powodujące konkretne zagrożenia oraz prawdopodobieństwo, że zdarzenia te zakończą się sukcesem;
- Określenie niekorzystnych skutków dla działalności podmiotu i jego majątku, osób fizycznych, innych podmiotów i Państwa, wynikających z wykorzystania podatności na zagrożenia przez źródła zagrożeń (poprzez zdarzenia szczególnych zagrożeń);
- Określenie zagrożenia dla bezpieczeństwa informacji, jako kombinacji prawdopodobieństwa wykorzystania podatności i wpływu eksploatacji, w tym wszelkich niepewności związanych z określeniem ryzyka.

Dla jasności poszczególne zadania są przedstawiane w sposób sekwencyjny. W praktyce jednak występują powtórzenia zadań[48]. W zależności od celu szacowania ryzyka podmioty mogą uznać za korzystną zmianę kolejności zadań. Niezależnie od tego, jakich zmian dokonają podmioty w zadaniach opisanych poniżej, szacowanie ryzyka powinno spełniać określony cel, zakres, założenia i ograniczenia ustalone przez podmiot inicjujące szacowanie. Aby pomóc podmiotom w realizacji poszczególnych zadań w procesie szacowania ryzyka, w załącznikach od D do I zamieszczono zestaw szablonów. Załączniki te dostarczają przydatnych informacji dla podmiotów w procesie szacowania ryzyka, a także mogą być wykorzystywane do rejestrowania wyników szacowania uzyskanych podczas istotnych obliczeń i analiz. Szablony są przykładowe i mogą być dostosowane przez podmioty zgodnie

[48] Na przykład, w miarę jak identyfikowane są podatności, dodatkowe zdarzenia zagrożeń mogą być identyfikowane poprzez zapytanie, w jaki sposób nowo zidentyfikowane podatności mogą zostać wykorzystane. Jeśli organizacje najpierw zidentyfikują podatności, a następnie zdefiniują zdarzenia zagrażające, mogą pojawić się zdarzenia, które nie są jednoznacznie powiązane z podatnościami, ale z warunkami je predysponującymi.

z określonymi wymogami biznesowymi podmiotu. Korzystanie z szablonów nie jest obligatoryjne.

Krok 2: Przeprowadzenie szacowania

Identyfikacja źródeł zagrożeń

Zadanie 2-1: Zidentyfikowanie i scharakteryzowanie źródeł zagrożeń, w tym zdolności, zamiarów i cech charakterystycznych dla zagrożeń o charakterze agresywnym oraz zakresu skutków dla zagrożeń o charakterze innym niż agresywny.

Dodatkowe wskazówki: Podmioty identyfikują źródła zagrożeń i określają cechy związane z tymi źródłami zagrożeń. W przypadku źródeł zagrożeń o charakterze agresywnym należy ocenić możliwości, zamiary i ukierunkowanie związane z tymi źródłami zagrożeń. W przypadku źródeł zagrożeń innych niż agresywne należy ocenić potencjalny zakres skutków wywoływanych przez te źródła zagrożeń. Strategia zarządzania ryzykiem i wyniki etapu *Przygotowania* dostarczają wskazówek organizacyjnych i wskazówek do przeprowadzenia identyfikacji i charakteryzacji źródeł zagrożeń, w tym np.: (i) źródła uzyskiwania informacji o zagrożeniach; (ii) źródła zagrożeń do uwzględnienia (według typu/nazwy); (iii) taksonomii zagrożeń do wykorzystania; oraz (iv) procesu identyfikacji źródeł zagrożeń, które mają znaczenie dla szacowania ryzyka. Jak określono w zadaniu 1-3, podmioty wyraźnie przyjmują wszelkie założenia dotyczące źródeł zagrożeń, w tym decyzje dotyczące identyfikacji źródeł zagrożeń, gdy konkretne i wiarygodne informacje o zagrożeniach są niedostępne. Podmioty mogą również spojrzeć na źródła zagrożeń o charakterze agresywnym z szerokiej perspektywy, biorąc pod uwagę czas, w jakim takie źródła zagrożeń mogą być wykorzystane w stosunku do zidentyfikowanych podatności podmiotu, skalę ataku oraz potencjalne wykorzystanie wielu wektorów ataku. Identyfikacja i charakterystyka zaawansowanych trwałych zagrożeń (*ang. Advanced Persistent Threats – APT*) może wiązać się z dużą niepewnością. Podmioty opisują takie źródła zagrożeń odpowiednim uzasadnieniem i odniesieniami (oraz w razie potrzeby zapewniają ich klasyfikację).

Załącznik D zawiera zestaw przykładowych tabel do wykorzystania przy identyfikacji źródeł zagrożeń:

- Tabela D-1 zawiera zestaw przykładowych danych wejściowych do zadania identyfikacji źródeł zagrożeń.
- Tabela D-2 zawiera zestaw przykładowych taksonomii, które mogą być wykorzystane do identyfikacji i charakterystyki źródeł zagrożeń.
- Tabele D-3, D-4 i D-5 zawierają przykładowe skale oceny czynników ryzyka (tj. cech charakterystycznych) źródeł zagrożeń o charakterze agresywnym w odniesieniu do zdolności, zamiarów i celów.
- W tabeli D-6 podano przykładową skalę oceny dla oceny zakresu skutków zdarzeń zagrożenia zainicjowanych przez niepowiązane ze sobą źródła zagrożeń.
- Tabele D-7 i D-8 zawierają szablony do podsumowania i udokumentowania wyników identyfikacji i charakteryzacji źródeł zagrożeń.

Jeżeli konkretny rodzaj źródła zagrożenia znajduje się poza zakresem szacowania ryzyka lub nie jest istotny dla podmiotu, informacje w tabelach D-7 i D-8 mogą zostać odpowiednio zmodyfikowane. Informacje przedstawione w zadaniu 2-1 dostarczają danych wejściowych o źródłach zagrożeń do tabel ryzyka w załączniku I. W tabeli D-7 i D-8 można je odpowiednio skrócić.

Podsumowanie kluczowych działań – zadanie 2-1

- Identyfikacja wejść źródeł zagrożeń (patrz tabela D-1, dostosowana przez podmiot).
- Identyfikacja źródeł zagrożeń (zob. tabela D-2, dostosowana przez podmiot).
- Ustalanie, czy źródła zagrożeń są istotne dla podmiotu i w jakim zakresie (zob. tabela D-1, dostosowana przez podmiot).
- Tworzenie lub aktualizacja oceny źródeł zagrożeń (patrz tabela D-7 dla źródeł zagrożeń o charakterze agresywnym i tabela D-8 dla źródeł zagrożeń o charakterze innym niż agresywny, dostosowana przez podmiot).
  - Dla odpowiednich źródeł zagrożeń o charakterze agresywnym:
    - ✓ Ocena zdolności do przeciwdziałania zagrożeniom (zob. tabela D-3, dostosowana przez podmiot).
    - ✓ Ocena zamiarów przeciwnika (zob. tabela D-4, dostosowana przez podmiot).
    - ✓ Ocena ukierunkowania na przeciwnika (zob. tabela D-5, dostosowana do potrzeb podmiotu.
  - W odniesieniu do odpowiednich, nieagresywnych źródeł zagrożeń:
    - ✓ Ocena zakresu skutków ze źródeł zagrożeń (zob. tabela D-6, dostosowana przez podmiot).

Identyfikacja zdarzeń zagrożeń

Zadanie 2-2: Zidentyfikować zdarzenia potencjalnego zagrożenia, znaczenie zdarzeń oraz źródła zagrożeń, które mogą je zainicjować.

Dodatkowe wskazówki: Zdarzenia zagrażające charakteryzują się źródłami zagrożeń, które mogą inicjować zdarzenia, a w przypadku zdarzeń o charakterze agresywnym, TTP-y używane do przeprowadzania ataków. Podmioty definiują zdarzenia zagrożeń w sposób wystarczająco szczegółowy, aby osiągnąć cel szacowania ryzyka. Na poziomie 1 szczególne znaczenie mają zdarzenia zagrożeń, które mogą mieć wpływ na poziom organizacyjny. Na poziomie 2

szczególnie interesujące są zdarzenia zagrożeń, które przekraczają granice systemów informatycznych, wykorzystują zależności funkcjonalne lub powiązania między systemami lub mają wpływ na właścicieli celu. Na poziomie 3 szczególne znaczenie mają zdarzenia zagrożeń, które można opisać w odniesieniu do konkretnych systemów informatycznych, technologii lub środowisk ich działania. Wiele źródeł zagrożeń może zainicjować jedno zdarzenie zagrażające. I odwrotnie, jedno źródło zagrożenia może potencjalnie zainicjować każde z wielu zdarzeń zagrażających. W związku z tym między zdarzeniami zagrażającymi i źródłami zagrożeń może istnieć związek między wieloma zdarzeniami, który może potencjalnie zwiększyć złożoność szacowania ryzyka. Aby umożliwić skuteczne wykorzystanie i przekazywanie wyników szacowania ryzyka, podmioty dostosowują ogólne opisy zdarzeń zagrożeń w tabelach E-2 i E-3 w celu określenia, w jaki sposób każde zdarzenie może potencjalnie zaszkodzić działaniom podmiotu (w tym celu, funkcjom, wizerunkowi lub reputacji) oraz zasobom, osobom, innym podmiotom lub społeczeństwu. Dla każdego zidentyfikowanego zdarzenia zagrożenia podmioty określają jego znaczenie. W tabeli E-4 przedstawiono szereg wartości dotyczących istotności zdarzeń zagrażających. Wartości wybrane przez podmioty mają bezpośredni związek z tolerancją ryzyka w podmiocie. Im większa awersja do ryzyka, tym większy jest zakres rozpatrywanych wartości. Podmioty akceptujące większe ryzyko lub mające większą tolerancję na ryzyko prawdopodobnie będą wymagały materialnych dowodów przed poważnym rozważeniem zdarzeń zagrażających. Jeżeli zdarzenie powodujące zagrożenie zostanie uznane za nieistotne, dalsze rozważania nie są brane pod uwagę. W przypadku istotnych zdarzeń zagrożeń podmioty identyfikują wszystkie potencjalne źródła zagrożeń, które mogą być inicjatorami tych zdarzeń.
W przypadku zadania 2-4, podmioty mogą zidentyfikować każdą parę źródeł zagrożenia i zdarzenie zagrożenia oddzielnie, ponieważ prawdopodobieństwo zainicjowania i powodzenia zdarzenia zagrożenia może być różne dla każdej pary. Alternatywnie, podmioty mogą zidentyfikować zestaw wszystkich możliwych źródeł zagrożeń, które mogłyby potencjalnie zainicjować zdarzenie zagrożenia.

Załącznik E zawiera zestaw przykładowych tabel do wykorzystania przy identyfikacji zdarzeń zagrożenia:

- Tabela E-1 zawiera zestaw przykładowych danych wejściowych do zadania identyfikacji zdarzeń zagrożenia.
- W tabeli E-2 przedstawiono reprezentatywne przykłady agresywnych zdarzeń zagrożeń wyrażonych jako TTP.
- W tabeli E-3 przedstawiono reprezentatywne przykłady niepowiązanych ze sobą zdarzeń zagrożenia.
- W tabeli E-4 podano przykładowe wartości dotyczące znaczenia zdarzeń zagrożenia dla podmiotu.
- Tabela E-5 zawiera szablon do podsumowania i udokumentowania wyników identyfikacji zdarzenia niebezpiecznego.

Informacje przedstawione w zadaniu 2-2 dostarczają danych wejściowych dotyczących zdarzeń zagrożenia do tabel ryzyka w załączniku I. W tabeli E-5 przedstawiono wzór podsumowujący i dokumentujący wyniki identyfikacji zdarzeń zagrożenia.

Podsumowanie kluczowych działań – zadanie 2-2

- Identyfikacja danych wejściowych dotyczących zdarzeń zagrożenia (patrz tabela E-1, dostosowana przez podmiot).
- Identyfikacja zdarzeń związanych z zagrożeniem (patrz tabela E-2 dla zdarzeń związanych z zagrożeniem o charakterze agresywnym i tabela E-3 dla zdarzeń niezwiązanych z zagrożeniem o charakterze agresywnym, dostosowana przez podmiot); należy stworzyć lub zaktualizować tabelę E-5.
- Identyfikacja źródeł zagrożeń, które mogą inicjować zdarzenia zagrożenia (zob. tabela D-7 i tabela D-8, dostosowane przez podmiot); aktualizacja tabeli E-5.
- Ocena znaczenia zdarzeń zagrażających dla podmiotu (zob. tabela E-4, dostosowana przez podmiot); aktualizacja tabeli E-5.
- Uaktualnienie kolumny 1-6 w tabeli I-5 w odniesieniu do ryzyka związanego z działaniami niepożądanymi (zob. tabela E-5 i tabela D-7) lub uaktualnić kolumny 1-4 w tabeli I-7 w odniesieniu do ryzyka niezwiązanego z działaniami niepożądanymi (zob. tabela E-5 i tabela D-8).

Identyfikacja podatności i warunków predysponujących

Zadanie 2-3: Identyfikacja podatności i predyspozycji, które mają wpływ na prawdopodobieństwo, że zagrażające zdarzenia wywołują niekorzystne skutki.

Dodatkowe wskazówki: Podstawowym celem oceny podatności na zagrożenia jest zrozumienie charakteru i stopnia, w jakim podmioty, ich procesy biznesowe i systemy informatyczne są podatne na źródła zagrożeń określone w zadaniu 2-1 oraz zdarzenia zagrożeń określone w zadaniu 2-2, które mogą być inicjowane przez te źródła zagrożeń. Podatności na poziomie 1 mogą być wszechobecne w podmiotach i mogą mieć daleko idące negatywne skutki, jeśli zostaną wykorzystane przez zdarzenia zagrożenia. Na przykład, nierozpatrzenie przez podmiot działań w ramach łańcucha dostaw może skutkować nabyciem przez podmiot podmienionych komponentów, które przeciwnicy mogą wykorzystać do zakłócenia funkcji biznesowych lub uzyskania poufnych informacji.

Podatności na poziomie 2 można opisać w kategoriach celu podmiotu/procesów biznesowych, architektury korporacyjnej, wykorzystania wielu systemów informatycznych lub wspólnej infrastruktury/usług wspólnych. Na poziomie 2 podatności zwykle przekraczają granice systemów informatycznych. Podatności na poziomie 3 można opisać w kategoriach technologii informatycznych stosowanych w systemach informatycznych organizacji, środowisk, w których te systemy działają lub braku zabezpieczeń albo istnienia w tych zabezpieczeniach podatności. Między zdarzeniami zagrażającymi i podatnościami może istnieć relacja "jeden do wielu". Wielokrotne zdarzenia zagrażające mogą wykorzystywać jedną podatność i odwrotnie, wiele podatności może być wykorzystywane przez jedno zdarzenie zagrażające. Powaga podatności jest oceną względnego znaczenia ograniczenia takiej podatności. Początkowo stan, w którym łagodzenie skutków jest nieplanowane, może służyć jako substytut powagi podatności na zagrożenia. Po dokonaniu szacowania ryzyka związanego z konkretną podatnością na zagrożenia, przy ocenie dotkliwości podatności na zagrożenia można wziąć pod uwagę ich skutki i stopień narażenia, biorąc pod uwagę wdrożone zabezpieczenia i inne podatności. Oceny dotkliwości podatności na zagrożenia wspierają reakcję na ryzyko. Podatności można zidentyfikować w różnym stopniu szczegółowości i specyfiki. Poziom szczegółowości przedstawiony w każdej ocenie podatności jest zgodny z celem szacowania ryzyka i rodzajem danych wejściowych potrzebnych do wsparcia określenia prawdopodobieństwa zajścia zdarzenia i jego wpływu.

Ze względu na stale rosnącą wielkość i złożoność podmiotów, procesów misyjnych/biznesowych oraz systemów informatycznych wspierających te procesy, liczba podatności jest zwykle duża i może zwiększać ogólną złożoność analizy. W związku z tym podmioty mają możliwość wykorzystania zadania identyfikacji podatności w celu zrozumienia ogólnego charakteru podatności (w tym ich zakresu, liczby i rodzaju) istotnych dla szacowania (zob. zadanie 1-3) oraz skatalogowania poszczególnych podatności w razie potrzeby. Podmioty określają, które podatności są istotne dla poszczególnych zdarzeń zagrażających w celu zmniejszenia przestrzeni potencjalnych zagrożeń, które mają być ocenione. Oprócz zidentyfikowania podatności, podmioty identyfikują również wszelkie predysponujące warunki, które mogą mieć wpływ na podatność. Predysponujące warunki

istniejące w organizacji (w tym procesy biznesowe, systemy informatyczne i środowiska ich działania) mogą przyczynić się do (tzn. zwiększyć lub zmniejszyć) prawdopodobieństwo, że jedno lub więcej zdarzeń powodujących zagrożenie, zainicjowanych przez źródła zagrożeń, będzie miało negatywny wpływ na działalność podmiotu, jego aktywa, osoby prywatne, inne podmioty lub społeczeństwo. Podmioty określają, jakie warunki predysponujące są istotne dla poszczególnych zdarzeń zagrażających, w celu zmniejszenia przestrzeni potencjalnego ryzyka, które należy ocenić. Podmioty oceniają powszechność występowania warunków predysponujących w celu wsparcia określenia poziomu (poziomów), na którym reakcja na ryzyko mogłaby być najbardziej skuteczna.

Załącznik F zawiera zbiór przykładowych tabel do wykorzystania w identyfikacji podatności na zagrożenia i warunków predysponujących:

- Tabela F-1 zawiera zbiór przykładowych danych wejściowych do zadania identyfikacji podatności na zagrożenia i stanów predysponujących.
- Tabela F-2 przedstawia przykładową skalę oceny wagi zidentyfikowanych podatności.
- Tabela F-3 dostarcza szablon do podsumowania/dokumentacji wyników identyfikacji podatności.
- Tabela F-4 przedstawia przykładową taksonomię, która może być użyta do identyfikacji i scharakteryzowania warunków predysponujących.
- Tabela F-5 przedstawia przykładową skalę oceny powszechności występowania warunków predysponujących.
- Tabela F-6 stanowi szablon do podsumowania/dokumentacji wyników identyfikacji warunków predysponujących.

Informacje uzyskane w Zadaniu 2-3 dostarczają danych wejściowych na temat podatności na zagrożenia i stanów predysponujących do tabel ryzyka w Załączniku I. W tabeli F-6 przedstawiono wzór podsumowania/dokumentacji wyników identyfikacji stanów predysponujących.

Podsumowanie kluczowych działań – zadanie 2-2

- Identyfikacja podatności na zagrożenia i predysponowanie czynników warunkujących (patrz tabela F-1, dostosowana do potrzeb podmiotu).
- Identyfikacja podatności przy użyciu zdefiniowanych przez podmiot źródeł informacji; utworzenie lub aktualizacja tabeli F-3.
- Ocena powagi zidentyfikowanych podatności (zob. tabela F-2, dostosowana przez podmiot); aktualizacja tabeli F-3.
- Określenie warunków predysponujących (zob. tabela F-4, dostosowana do potrzeb podmiotu); utworzenie lub aktualizacja tabeli F-6.
- Ocena wszechobecności uwarunkowań predysponujących (zob. tabela F-5, dostosowana do potrzeb podmiotu); aktualizacja tabeli F-6.
- Uaktualnienie kolumny 8 w tabeli I-5 w odniesieniu do ryzyka niekorzystnego; lub uaktualnienie kolumny 6 w tabeli I-7 w odniesieniu do ryzyka niekorzystnego (zob. tabela F-3 i tabela F-6).
- Uaktualnienie kolumny 9 w tabeli I-5 w zakresie ryzyka agresywnego; lub uaktualnienie kolumny 7 w tabeli I-7 w zakresie ryzyka innego niż agresywne (zob. tabela F-2 i tabela F-5).

Określenie prawdopodobieństwa

Zadanie 2-4: Ustalenie prawdopodobieństwa, że zagrażające zdarzenia wywołują niekorzystne skutki, biorąc pod uwagę: (i) charakterystykę źródeł zagrożeń, które mogą być przyczyną tych zdarzeń; (ii) stwierdzoną podatność na zagrożenia/stan zagrożenia; oraz (iii) organizacyjną podatność podmiotu odzwierciedlającą planowane lub wdrożone środki ochronne/przeciwdziałające mające na celu powstrzymanie takich zdarzeń.

Dodatkowe wskazówki: Podmioty stosują trzyetapowy proces w celu określenia ogólnego prawdopodobieństwa wystąpienia zagrożeń. Po pierwsze, podmioty oceniają prawdopodobieństwo, że zdarzenia zagrażające zostaną zainicjowane (w przypadku agresywnych zdarzeń zagrażających) lub wystąpią (w przypadku nieagresywnych zdarzeń

zagrażających). Po drugie, podmioty oceniają prawdopodobieństwo, że zdarzenia zagrażające po ich rozpoczęciu lub wystąpieniu spowodują niekorzystne skutki dla działalności podmiotu, jego aktywów, osób fizycznych, innych podmiotów lub Państwa. Wreszcie, podmioty oceniają ogólne prawdopodobieństwo, jako kombinację prawdopodobieństwa inicjacji/wystąpienia i prawdopodobieństwa spowodowania negatywnych skutków.

Podmioty oceniają prawdopodobieństwo inicjacji zdarzenia zagrożenia, biorąc pod uwagę charakterystykę źródeł zagrożeń, w tym zdolności, zamiary i ukierunkowanie (patrz zadanie 2-1 i załącznik D). Jeżeli zdarzenia zagrożenia wymagają większej zdolności niż posiadają przeciwnicy (a przeciwnicy są świadomi tego faktu), nie oczekuje się, że przeciwnicy rozpoczną zdarzenia. Jeżeli przeciwnicy nie spodziewają się osiągnąć zamierzonych celów poprzez realizację zdarzeń związanych z zagrożeniem, nie oczekuje się od nich inicjowania zdarzeń. I wreszcie, jeśli przeciwnicy nie kierują aktywnie swoich działań do konkretnych podmiotów lub ich celów/funkcji biznesowych, nie oczekuje się od nich, że zainicjują zdarzenia zagrażające. podmioty korzystają ze skali oceny zamieszczonej w tabeli G-2 i przedstawiają uzasadnienie oceny pozwalające na jednoznaczne rozważenie kwestii odstraszania i przenoszenia zagrożeń. Podmioty mogą ocenić prawdopodobieństwo wystąpienia zdarzenia niebezpiecznego (nie przekrojowego) przy użyciu tabeli G-3 i przedstawić podobne uzasadnienie oceny.

Podmioty oceniają prawdopodobieństwo wystąpienia niekorzystnych skutków zdarzeń zagrażających, biorąc pod uwagę zestaw zidentyfikowanych podatności i warunków predysponujących (zob. zadanie 2-3 i załącznik F). W przypadku zdarzeń zagrożeń inicjowanych przez przeciwników, organizacje biorą pod uwagę charakterystykę powiązanych ze sobą źródeł zagrożeń. W przypadku zdarzeń niemających charakteru agresywnego, organizacje biorą pod uwagę przewidywaną dotkliwość i czas trwania zdarzenia (zawarte w opisie zdarzenia). Podmioty korzystają ze skali oceny zamieszczonej w tabeli G-4 i przedstawiają uzasadnienie oceny pozwalające na jej wyraźne uwzględnienie, jak podano powyżej. Zdarzenia zagrażające, w przypadku których nie zidentyfikowano podatności lub warunków predysponujących, mają bardzo małe prawdopodobieństwo

wystąpienia negatywnych skutków. Takie zdarzenia zagrożeń można uwypuklić i przenieść na koniec tabeli (lub do osobnej tabeli), tak aby można je było śledzić w celu rozważenia ich w dalszych szacowania ryzyka. Nie jest jednak uzasadnione dalsze rozważania w ramach aktualnego szacowania.

Ogólne prawdopodobieństwo wystąpienia zdarzenia zagrażającego jest kombinacją różnych czynników: (i) prawdopodobieństwa wystąpienia zdarzenia (np. z powodu błędu ludzkiego lub klęski żywiołowej) lub jego zainicjowania przez przeciwnika; oraz (ii) prawdopodobieństwa, że jego zainicjowanie/wystąpienie spowoduje niekorzystne skutki. Organizacje oceniają ogólne prawdopodobieństwo wystąpienia zdarzeń zagrażających, wykorzystując dane z tabel G-2, G-3 i G-4. Od tego zależy każdy szczególny algorytm lub zasada łączenia ustalonych wartości prawdopodobieństwa: (i) ogólnego podejścia podmiotu do ryzyka, w tym ogólnej tolerancji ryzyka i tolerancji niepewności; (ii) szczególnej tolerancji niepewności różnych czynników ryzyka; oraz (iii) wagi czynników ryzyka w podmiocie. Na przykład, podmioty mogą stosować którąkolwiek z poniższych zasad (lub mogą określić inną zasadę): (i) stosować maksymalną wartość dwóch wartości prawdopodobieństwa; (ii) stosować minimalną wartość dwóch wartości prawdopodobieństwa; (iii) rozważać wyłącznie prawdopodobieństwo zainicjowania/wystąpienia zdarzenia, zakładając, że w razie zainicjowania lub wystąpienia zdarzeń zagrażających wystąpią niekorzystne skutki; (iv) rozważać wyłącznie prawdopodobieństwo wystąpienia skutków, zakładając, że w razie wystąpienia zdarzeń zagrażających wystąpią niekorzystne skutki, inicjatorami zdarzeń będą przeciwnicy; lub (v) przyjąć średnią ważoną z dwóch wartości prawdopodobieństwa. podmioty wyraźnie określają stosowane zasady.

Załącznik G zawiera zbiór przykładowych tabel do wykorzystania przy określaniu prawdopodobieństwa wystąpienia zdarzeń zagrażających:

- Tabela G-1 zawiera zestaw przykładowych danych wejściowych do zadania określania prawdopodobieństwa.
- W tabeli G-2 przedstawiono przykładową skalę oceny prawdopodobieństwa inicjacji w przypadku niepożądanych zdarzeń zagrożenia

- W tabeli G-3 podano przykładową skalę oceny do celów oceny prawdopodobieństwa wystąpienia niepożądanych zdarzeń zagrażających.
- W tabeli G-4 podano przykładową skalę oceny do celów oceny prawdopodobieństwa wystąpienia niepożądanych skutków zdarzeń zagrażających, jeżeli zdarzenia te są celowo inicjowane (agresywne) lub występują losowo (nieagresywne); oraz
- W tabeli G-5 przedstawiono przykładową skalę oceny ogólnego prawdopodobieństwa wystąpienia zdarzeń zagrażających (tj. połączenie prawdopodobieństwa wszczęcia/wystąpienia i prawdopodobieństwa wpływu).

Informacje opracowane w ramach zadania 2-4 dostarczają danych wejściowych na temat prawdopodobieństwa wystąpienia zdarzeń zagrożenia do tabel ryzyka w załączniku I.

Podsumowanie kluczowych działań – zadanie 2-3

- Określenie czynników określających prawdopodobieństwo (patrz tabela G-1, dostosowana przez podmiot).
- Identyfikacja czynników określających prawdopodobieństwo przy użyciu zdefiniowanych przez podmiot źródeł informacji (np. charakterystyka źródeł zagrożeń, podatności, warunki predysponujące).
- Ocena prawdopodobieństwa zainicjowania zdarzenia zagrożenia w przypadku zagrożeń o charakterze agresywnym oraz prawdopodobieństwo wystąpienia zdarzenia zagrożenia w przypadku zagrożeń o charakterze innym niż agresywne (patrz tabela G-2 i tabela G-3, dostosowane przez podmiot).
- Ocena prawdopodobieństwa wystąpienia zdarzeń powodujących niekorzystne skutki, biorąc pod uwagę prawdopodobieństwo inicjacji lub wystąpienia zagrożenia (patrz tabela G-4, dostosowana przez podmiot).
- Ocena ogólnego prawdopodobieństwa inicjacji/wystąpienia zdarzenia powodującego zagrożenie oraz prawdopodobieństwa wystąpienia zdarzeń powodujących niekorzystne skutki (patrz tabela G-5, dostosowana przez podmiot).
- Uaktualnienie kolumny 7, 10 i 11 w tabeli I-5 w odniesieniu do ryzyka niekorzystnego wpływu (patrz: tabela G-2, tabela G-4 i tabela G-5); lub uaktualnić kolumny 5, 8 i 9 w tabeli I-7 w odniesieniu do ryzyka niekorzystnego wpływu (patrz: tabela G-3, tabela G-4 i tabela G-5).

Określenie wpływu

Zadanie 2-5: Określić niekorzystne skutki wynikające z uwzględnienia zdarzeń zagrażających: (i) charakterystykę źródeł zagrożeń, które mogą być przyczyną tych zdarzeń; (ii) stwierdzoną podatność na zagrożenia/stan zagrożenia; oraz (iii) podatność odzwierciedlającą planowane lub wdrożone środki ochronne/przeciwdziałające mające na celu utrudnienie tych zdarzeń.

Dodatkowe wskazówki: Podmioty opisują niekorzystne skutki w zakresie potencjalnych szkód wyrządzonych w działalności i majątku podmiotu, osobom fizycznym, innym

podmiotom lub społeczeństwu. Miejsce wystąpienia zagrożenia oraz to, czy skutki zdarzenia są ograniczone, czy też rozprzestrzeniają się, wpływa na powagę wpływu. Ocena skutków może obejmować identyfikację zasobów lub potencjalnych celów źródeł zagrożenia, w tym zasobów informacyjnych (np. informacji, repozytoriów danych, systemów informatycznych, aplikacji, technologii informatycznych, łączy komunikacyjnych), ludzi i zasobów fizycznych (np. budynków, zasilania), na które zdarzenia zagrożenia mogą mieć wpływ. Skutki dla podmiotu są określane i uszeregowane pod względem ważności na poziomie 1 i 2 oraz przekazywane do poziomu 3 w ramach określania ryzyka. Na poziomie 3 skutki są związane z możliwościami systemów informatycznych (np. przetwarzanie, wyświetlanie, komunikacja, przechowywanie i wyszukiwanie) oraz zasobami (np. bazami danych, usługami, komponentami), które mogą być zagrożone.

Załącznik H zawiera zestaw przykładowych tabel do wykorzystania przy określaniu negatywnych skutków:

- Tabela H-1 zawiera zestaw przykładowych danych wejściowych do zadania określania oddziaływań.
- Tabela H-2 zawiera reprezentatywne przykłady negatywnych oddziaływań dla organizacji koncentrujących się na szkodach dla działalności i aktywów organizacji, osób, innych organizacji i Państwa.
- W Tabeli H-3 podano przykładową skalę oceny wpływu zdarzeń zagrożenia; oraz
- Tabela H-4 zawiera szablon do podsumowania/dokumentacji negatywnych oddziaływań.

Informacje przedstawione w zadaniu 2-5 zawierają dane wejściowe dotyczące negatywnych skutków w tabelach ryzyka w załączniku I. W tabeli H-4 przedstawiono wzór podsumowania/dokumentacji negatywnych skutków.

Podsumowanie kluczowych działań – zadanie 2-5

- Identyfikacja danych wejściowych do określenia wpływu (patrz tabela H-1, dostosowana przez podmiot).
- Identyfikacja czynników określających wpływ przy użyciu zdefiniowanych przez podmiot źródeł informacji.
- Identyfikacja niekorzystnych wpływów i dotkniętych aktywów (patrz tabela H-2, dostosowana przez podmiot); utworzenie lub aktualizacja tabeli H-4.
- Oszacowanie maksymalnego wpływu związanego z dotkniętymi aktywami (zob. tabela H-3, dostosowana do potrzeb podmiotu); zaktualizować tabelę H-4.
- Aktualizacja kolumny 12 w tabeli I-5 w odniesieniu do ryzyka agresywnego; lub aktualizacja kolumny 10 w tabeli I-7 w odniesieniu do ryzyka nieagresywnego.

Określanie ryzyka

Zadanie 2-6: Ustalenie ryzyka dla podmiotu na podstawie rozważanych zdarzeń zagrażających bezpieczeństwu na podstawie: (i) wpływu, który wynikałby z tych zdarzeń; oraz (ii) prawdopodobieństwa wystąpienia tych zdarzeń.

Dodatkowe wskazówki: Podmioty szacują ryzyko związane ze zdarzeniami zagrażającymi, jako kombinację prawdopodobieństwa i wpływu. Poziom ryzyka związanego ze zidentyfikowanymi zdarzeniami stanowiącymi zagrożenie stanowi określenie stopnia, w jakim podmioty są zagrożone takimi zdarzeniami. Podmioty wyraźnie wskazują na niepewność w określeniu ryzyka, w tym na przykład założenia poczynione w podmiocie i subiektywne osądy/decyzje. Podmioty mogą uporządkować listę zdarzeń stwarzających zagrożenie ze względu na poziom ryzyka określony podczas szacowania ryzyka – z największą uwagą poświęconą zdarzeniom wysokiego ryzyka. Podmioty mogą dalej hierarchizować ryzyko na tym samym poziomie lub z podobną punktacją (zob. załącznik J). Każde ryzyko odpowiada konkretnemu zdarzeniu zagrażającemu o określonym poziomie wpływu w przypadku wystąpienia tego zdarzenia. Ogólnie rzecz biorąc, poziom ryzyka zwykle nie jest wyższy niż poziom wpływu, a prawdopodobieństwo może służyć do zmniejszenia ryzyka poniżej tego poziomu wpływu. Jednak w przypadku rozwiązywania problemów związanych z zarządzaniem ryzykiem w skali całego podmiotu przy dużej liczbie procesów biznesowych

i wspomagających je systemów informatycznych, wpływ, jako górna granica ryzyka może się nie utrzymywać. Na przykład, gdy zmaterializuje się wiele ryzyk, nawet jeśli każde z nich znajduje się na umiarkowanym poziomie, zestaw tych umiarkowanych ryzyk może dla podmiotu sumować się do wyższego poziomu ryzyka. Aby zaradzić sytuacjom, w których szkoda występuje wielokrotnie, podmiot może zdefiniować zdarzenie powodujące zagrożenie, jako wielokrotne wystąpienie szkody i poziom wpływu związany ze skumulowanym stopniem szkody. Podczas realizacji zadań od 2-1 do 2-5 podmioty wychwytują kluczowe informacje związane z niepewnością w szacowaniu ryzyka. Niepewności te wynikają z takich źródeł, jak brakujące informacje, subiektywne ustalenia i przyjęte założenia. Skuteczność wyników szacowania ryzyka jest po części uzależniona od zdolności decydentów do określenia możliwości dalszego stosowania założeń poczynionych w ramach szacowania. Informacje związane z niepewnością są opracowywane i przedstawiane w sposób, który łatwo wspiera świadome decyzje w zakresie zarządzania ryzykiem.

Załącznik I zawiera zestaw przykładowych tabel do wykorzystania przy określaniu ryzyka:

- Tabela I-1 zawiera zestaw przykładowych danych wejściowych do zadania określania ryzyka i niepewności.
- Tabele I-2 i I-3 zawierają przykładowe skale oceny do oceny poziomów ryzyka.
- Tabele I-4 i I-6 zawierają opisy nagłówków kolumn dla kluczowych elementów danych wykorzystywanych do określania ryzyka, odpowiednio dla agresywnych i nieagresywnych zdarzeń zagrożenia.
- Tabele I-5 i I-7 zawierają szablony podsumowujące/dokumentujące kluczowe elementy danych wykorzystywane przy ustalaniu ryzyka odpowiednio dla zdarzeń zagrożeń o charakterze agresywnym i nieagresywnym.

Informacje opracowane w ramach zadania 2-6 dostarczają danych wejściowych do tabel ryzyka w załączniku I.

Podsumowanie kluczowych działań – zadanie 2-6

- Identyfikacja danych wejściowych do określenia ryzyka i niepewności (patrz tabela I-1, dostosowana przez organizację).
- Określanie ryzyka (zob. tabela I-2 i tabela I-3, dostosowane do potrzeb podmiotu); aktualizacja kolumny 13 w tabeli I-5 w przypadku ryzyka agresywnego oraz kolumny 11 w tabeli I-7 w przypadku ryzyka innego niż agresywne.

3.3. Komunikowanie i udostępnianie wyników szacowania ryzyka

Trzecim etapem procesu szacowania ryzyka jest przekazanie wyników szacowania i wymiana informacji związanych z ryzykiem[49]. Celem tego etapu jest zapewnienie decydentom w całym podmiocie odpowiednich informacji związanych z ryzykiem, niezbędnych do informowania i kierowania decyzjami dotyczącymi ryzyka. Przekazywanie i dzielenie się informacjami składa się z następujących konkretnych zadań:

- Informowanie o wynikach szacowania ryzyka;
- dzielenie się informacjami opracowanymi w trakcie przeprowadzania szacowania ryzyka, w celu wsparcia innych działań z zakresu zarządzania ryzykiem.

[49] Proces oceny ryzyka wiąże się z bieżącą komunikacją i wymianą informacji pomiędzy personelem wykonującym czynności związane z oceną, ekspertami w danej dziedzinie oraz kluczowymi interesariuszami organizacyjnymi (np. właściciele misji/biznesu, funkcje zarządzania ryzykiem - RE, CISO, właściciele systemów informatycznych/menadżerowie programów). Taka komunikacja i wymiana informacji zapewnia, że: (i) dane wejściowe do oceny ryzyka są tak dokładne, jak to tylko możliwe; (ii) można zastosować wyniki pośrednie (np. w celu wsparcia oceny ryzyka na innych poziomach); oraz (iii) wyniki są znaczącymi i użytecznymi danymi wejściowymi do reakcji na ryzyko.

Krok 3: Komunikowanie i udostępnianie wyników szacowania ryzyka

Komunikowanie wyników szacowania ryzyka

Zadanie 3-1: Komunikowanie wyników szacowania ryzyka decydentom w celu wsparcia reakcji na ryzyko.

Dodatkowe wskazówki: Podmioty powinny przekazywać wyniki szacowania ryzyka na różne sposoby (np. odprawy dla kierownictwa, raporty z szacowania ryzyka, tablice informacyjne). Komunikaty o ryzyku mogą mieć charakter formalny lub nieformalny, a ich treść i format mogą być określone przez podmioty inicjujące i przeprowadzające Szacowanie. Podmioty udzielają wskazówek dotyczących konkretnych wymogów w zakresie komunikacji i sprawozdawczości na temat ryzyka, uwzględnianych w ramach przygotowania do szacowania ryzyka (jeśli nie zostały one uwzględnione w celów zarządzania ryzykiem w ramach zadania polegającego na opracowaniu ram szacowania ryzyka). Podmioty przyznają priorytet ryzykom na tym samym poziomie lub o podobnych wynikach (patrz Załącznik J). W dodatku K podano przykładowy rodzaj informacji, które mogą być zawarte w sprawozdaniu z szacowania ryzyka lub w preferowanym nośniku służącym do informowania o ryzyku.

Udostępnianie informacji o wynikach szacowania ryzyka

Zadanie 3-2: Udostępnianie odpowiedniemu personelowi organizacyjnemu informacji na temat ryzyka opracowanych w trakcie szacowania ryzyka.

Dodatkowe wskazówki: Podmioty dzielą się informacjami źródłowymi i wynikami pośrednimi oraz udzielają wskazówek dotyczących dzielenia się informacjami związanymi z ryzykiem. Wymiana informacji odbywa się przede wszystkim wewnątrz podmiotu, poprzez raporty i spotkania informacyjne oraz poprzez aktualizację repozytoriów danych związanych z ryzykiem wraz z dowodami potwierdzającymi wyniki szacowania ryzyka. Wymiana informacji jest również wspierana przez dokumentowanie źródeł informacji, procesów analitycznych i wyników pośrednich (np. wypełnione tabele w dodatkach D-I), dzięki czemu szacowanie ryzyk, co ułatwia prowadzenie szacowania. Wymiana informacji może mieć miejsce również z innymi podmiotami.

Podsumowanie kluczowych działań – Przekazywanie informacji i dzielenie się nimi

- Ustalenie odpowiedniej metody (np. odprawa dla kierownictwa, raport z oceny ryzyka lub tablica ogłoszeń) przekazywania wyników szacowania ryzyka.
- Przekazanie wyników szacowania ryzyka wyznaczonym interesariuszom w podmiocie.
- Dzielenie się wynikami oceny ryzyka i dowodami uzupełniającymi zgodnie z polityką i wytycznymi obowiązującymi w podmiocie.

3.4. Utrzymanie wyników szacowania ryzyka

Czwartym krokiem w procesie szacowania ryzyka jest utrzymanie szacowania. Celem tego kroku jest utrzymanie aktualnej, specyficznej wiedzy na temat ryzyka, jakie ponoszą podmioty. Wyniki szacowania ryzyka stanowią podstawę do podejmowania decyzji w zakresie zarządzania ryzykiem oraz ukierunkowują reakcje na ryzyko. W celu wsparcia bieżącego przeglądu decyzji dotyczących zarządzania ryzykiem (np. decyzji o zakupie, decyzji o autoryzacji systemów informatycznych i zabezpieczeń wspólnych, decyzji o połączeniu), organizacje przeprowadzają oceny ryzyka, które uwzględniają wszelkie zmiany wykryte w wyniku monitorowania ryzyka[50]. Monitorowanie ryzyka zapewnia organizacjom środki do ciągłego: (i) określania skuteczności reakcji na ryzyko; (ii) identyfikowania zmian wpływających na ryzyko w organizacyjnych systemach informatycznych i środowiskach,

[50] Monitorowanie ryzyka, czwarty krok w procesie zarządzania ryzykiem, jest opisany w publikacji NSC 800-39. Krok w procesie oceny ryzyka, mający na celu utrzymanie wyników oceny w czasie, pokrywa się w pewnym stopniu z krokiem monitorowania ryzyka w procesie zarządzania ryzykiem i krokiem ciągłego monitorowania w RMF. To nakładanie się wzmacnia istotną koncepcję, zgodnie z którą liczne działania w procesie zarządzania ryzykiem są komplementarne i wzajemnie się wzmacniają. Na przykład, etap ciągłego monitorowania w RMF może być wykorzystany do monitorowania bieżącej skuteczności wdrożonych środków bezpieczeństwa, a wyniki mogą być wykorzystane do informowania i kierowania bardziej rozległym procesem monitorowania ryzyka organizacyjnego. Na poziomie organizacji, monitorowanie ryzyka może obejmować monitorowanie kluczowych czynników ryzyka, które są niezbędne do przeprowadzenia kolejnych ocen ryzyka. Organizacje wykorzystują strategię zarządzania ryzykiem do przekazywania kluczowych wymagań dotyczących przeprowadzania ocen ryzyka, w tym na przykład czynników ryzyka, które należy monitorować, oraz częstotliwości takiego monitorowania.

w których te systemy funkcjonują[51]; oraz (iii) weryfikowania zgodności[52]. Utrzymywanie ocen ryzyka obejmuje następujące szczegółowe zadania:

- monitorowanie na bieżąco czynników ryzyka zidentyfikowanych w procesie szacowania ryzyka oraz zrozumienie kolejnych zmian tych czynników;
- aktualizacja elementów szacowania ryzyka odzwierciedlających działania monitorujące prowadzone przez podmiot.

Krok 4: Utrzymanie wyników szacowania

Monitorowanie czynników ryzyka

Zadanie 4-1: Prowadzenie bieżącego monitoringu czynników ryzyka, które przyczyniają się do zmian w zakresie ryzyka dla działalności i aktywów podmiotu, osób, innych podmiotów lub Państwa.

Dodatkowe wskazówki: Podmioty na bieżąco monitorują czynniki ryzyka o istotnym znaczeniu, aby zapewnić, że informacje potrzebne do podejmowania wiarygodnych, opartych na ryzyku decyzji są nadal dostępne na przestrzeni czasu. Monitorowanie czynników ryzyka (np. źródeł zagrożeń i zdarzeń z nimi związanych, podatności i predyspozycji, możliwości i zamiarów przeciwników, ukierunkowania działań podmiotu, aktywów lub osób) może dostarczyć krytycznych informacji na temat zmieniających się warunków, które mogą potencjalnie wpłynąć na zdolność podmiotu do wykonywania podstawowych celu i funkcji biznesowych. Informacje uzyskane w wyniku bieżącego monitorowania czynników ryzyka mogą być wykorzystane do odświeżenia szacowania ryzyka z dowolną częstotliwością, która zostanie uznana za właściwą. Podmioty powinny również starać się uchwycić zmiany w zakresie skuteczności środków reagowania na ryzyko w celu utrzymania aktualności szacowania ryzyka. Celem jest utrzymanie bieżącej świadomości

[51] Publikacja NIST SP 800-137 zawiera wytyczne dotyczące bieżącego monitorowania systemów informatycznych i środowisk działania organizacji.

[52] Weryfikacja zgodności zapewnia, że organizacje wdrożyły wymagane środki reagowania na ryzyko oraz że spełnione zostały wymagania dotyczące bezpieczeństwa informacji wynikające z misji/funkcji biznesowych organizacji, ustawodawstwa, dyrektyw, rozporządzeń, polityk i standardów/ wytycznych.

sytuacyjnej w zakresie struktur i działań zarządzania organizacją, procesów biznesowych, systemów informatycznych i środowisk działania, a tym samym wszystkich czynników ryzyka, które mogą mieć wpływ na ryzyko ponoszone przez Podmiot. Dlatego też, stosując kontekst lub ramy szacowania ryzyka (tj. zakres, cel, założenia, ograniczenia, tolerancje ryzyka, priorytety i kompromisy), podmioty biorą pod uwagę rolę czynników ryzyka w realizowanym planie reagowania na ryzyko. Na przykład, dość powszechnie oczekuje się, że jest znany stan bezpieczeństwa systemów informatycznych (tj. czynniki ryzyka mierzone w tych systemach), który odzwierciedla tylko część reakcji na ryzyko w podmiocie, przy czym działania podejmowane na poziomie podmiotu lub na poziomie celu/procesu biznesowego stanowią znaczącą część tej reakcji. W takich sytuacjach monitorowanie tylko stanu bezpieczeństwa systemów informatycznych prawdopodobnie nie zapewniłoby wystarczających informacji do określenia ogólnego ryzyka ponoszonego przez podmiot. Można oczekiwać, że wysoce wydajne, dobrze wyekwipowane i celowo ukierunkowane źródła zagrożeń pokonają powszechnie dostępne mechanizmy ochrony (np. poprzez ominięcie lub ingerencję w takie mechanizmy). W związku z tym, środki reagowania na ryzyko na poziomie procesu, takie jak przebudowa procesów biznesowych, mądre wykorzystanie technologii informatycznych lub zastosowanie alternatywnych procesów wykonawczych, w przypadku zagrożenia systemów informatycznych, może być głównymi elementami planów reagowania na ryzyko w podmiocie.

Aktualizacja szacowania ryzyka

Zadanie 4-2: Aktualizacja istniejącego szacowania ryzyka z wykorzystaniem wyników bieżącego monitorowania czynników ryzyka.

Dodatkowe wskazówki: Podmioty określają częstotliwość i okoliczności, w których szacowania ryzyka są aktualizowane. Ustalenia takie mogą obejmować na przykład aktualny poziom ryzyka i/lub znaczenie podstawowych funkcji biznesowych podmiotu. Jeżeli od czasu przeprowadzenia szacowania ryzyka zaszły istotne zmiany (określone przez politykę, kierunek lub wytyczne podmiotu), podmioty mogą ponownie przeanalizować cel, zakres, założenia i ograniczenia szacowania, aby ustalić, czy wszystkie zadania w procesie

szacowania ryzyka muszą zostać powtórzone. W przeciwnym razie, aktualizacje stanowią kolejne etapy szacowania ryzyka, identyfikując i oceniając jedynie sposób, w jaki na przykład zmieniły się wybrane czynniki ryzyka: (i) identyfikacja nowych zdarzeń związanych z zagrożeniem, podatności, warunków predysponujących, niepożądanych skutków i/lub aktywów, których dotyczą zmiany; oraz (ii) ocena charakterystyki źródła zagrożenia (np. zdolności, zamiarów, ukierunkowania, zakresu skutków), prawdopodobieństwa i skutków. Podmioty przekazują wyniki kolejnych szacowań ryzyka osobom na wszystkich szczeblach zarządzania ryzykiem, aby zapewnić tym osobom dostęp do krytycznych informacji niezbędnych do podejmowania bieżących decyzji opartych na analizie ryzyka.

Podsumowanie kluczowych działań – Utrzymanie szacowania ryzyka

- Identyfikacja kluczowych czynników ryzyka, które zostały zidentyfikowane na potrzeby bieżącego monitorowania.
- Określenie częstotliwości działań związanych z monitorowaniem czynników ryzyka oraz okoliczności, w których szacowanie ryzyka wymaga aktualizacji.
- Potwierdzenie celu, zakresu i założeń szacowania ryzyka.
- W razie potrzeby przeprowadzenie odpowiednich zadań związanych z szacowaniem ryzyka.
- Przekazywanie kolejnych wyników szacowania ryzyka określonemu personelowi organizacyjnemu.

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 800-18	Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych – na podstawie NIST SP 800- 18
NSC 800-30	Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne – na podstawie NIST SP 800-30
NSC 800-34	Poradnik planowania awaryjnego– na podstawie NIST SP 800-34
NSC 800-37	Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia system – na podstawie NIST SP 800-37
NSC 800-39	Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informatycznego – na podstawie NIST SP 800-39
NSC 800-53	Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji – na podstawie NIST SP 800-53

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA	
NSC 800-53A	Ocenianie 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
NSC 800-61	Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego – na podstawie NIST SP 800-61
NSC 7298	Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa

LAWS, POLICIES, DIRECTIVES, INSTRUCTIONS, STANDARDS, AND GUIDELINES

LEGISLATION	
1.	E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
2.	Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.

POLICIES, DIRECTIVES, INSTRUCTIONS	
1.	Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.
2.	Committee on National Security Systems Instruction (CNSSI) No. 4009, *National Information Assurance (IA) Glossary*, April 2010.
3.	Committee on National Security Systems Instruction (CNSSI) No. 1253, *Security Categorization and Control Selection for National Security Systems*, March 2012.
4.	Department of Homeland Security Federal Continuity Directive 2 (FCD 2), *Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process*, February 2008.

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

STANDARDS	
2.	National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.
3.	ISO/IEC 31000:2009, *Risk management – Principles and guidelines*.
4.	ISO/IEC 30101:2009, *Risk management – Risk assessment techniques*.
5.	ISO/IEC Guide 73, *Risk management – Vocabulary*.
6.	ISO/IEC 27005:2011, *Information technology – Security techniques – Information security risk management*.

GUIDELINES	
1.	National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.
2.	National Institute of Standards and Technology Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, May 2010.
3.	National Institute of Standards and Technology Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010.

GUIDELINES	
4.	National Institute of Standards and Technology Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.
5.	National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009.
6.	National Institute of Standards and Technology Special Publication 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, June 2010.
7.	National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.
8.	National Institute of Standards and Technology Special Publication 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.
10.	National Institute of Standards and Technology Special Publication 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*, October 2008.
11.	National Institute of Standards and Technology Special Publication 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, January 2005.

GUIDELINES	
12.	National Institute of Standards and Technology Special Publication 800-70, Revision 2, *National Checklist Program for IT Products--Guidelines for Checklist Users and Developers*, February 2011.
13.	National Institute of Standards and Technology Special Publication 800-117, Version 1.0, *Guide to Adopting and Using the Security Content Automation Protocol (SCAP)*, July 2010.
14.	National Institute of Standards and Technology Special Publication 800-126, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.0*, November 2009.

ZAŁĄCZNIK B SŁOWNIK

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

ZAŁĄCZNIK C AKRONIMY

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

ZAŁĄCZNIK D ŹRÓDŁA ZAGROŻEŃ

Taksonomia źródeł zagrożeń zdolnych do inicjowania zdarzeń zagrożeń

Niniejszy załącznik zapewnia: (i) opis potencjalnie użytecznych danych wejściowych do zadania identyfikacji źródeł zagrożeń; (ii) przykładową taksonomię źródeł zagrożeń według rodzaju, opisu i czynników ryzyka (tj. cech charakterystycznych) wykorzystanych do oceny prawdopodobieństwa i/lub wpływu takich źródeł zagrożeń inicjujących zdarzenia powodujące zagrożenie; (iii) przykładowy zestaw dostosowanych do potrzeb skali oceny tych czynników ryzyka; oraz (iv) szablony do podsumowania i udokumentowania wyników zadania 2-1 dotyczącego identyfikacji źródeł zagrożeń. Skale taksonomii i oceny zawarte w niniejszym załączniku mogą być wykorzystywane przez podmioty, jako punkt wyjścia przy odpowiednim dostosowaniu do warunków specyficznych dla danego podmiotu. Tabele D-7 i D-8, wyniki zadania 2-1, dostarczają odpowiednich danych wejściowych do tabel ryzyka w załączniku I.

Tabela D-1. Wejście – źródła identyfikacji zagrożeń.

Opis	Warunek		
	poziom 1	**poziom 2**	**poziom 3**
Z poziomu 1: (poziom organizacji) • Źródła informacji o zagrożeniach uznane za wiarygodne (np. otwarte lub niejawne raporty o zagrożeniach, wcześniejsze szacowania ryzyka). (sekcja 3.1, zadanie 1-4) • Informacje o źródłach zagrożeń i wskazówki specyficzne dla poziomu 1 (np. zagrożenia związane z zarządzaniem podmiotem, podstawowymi funkcjami biznesowymi, polityką, procedurami i strukturami zarządzania/operacji, zewnętrznymi celami/kontaktami biznesowymi). • Taksonomia źródeł zagrożeń, w razie potrzeby opatrzona adnotacjami przez podmiot. (Tabela D-2) • Charakterystyka agresywnych i nieagresywnych źródeł zagrożeń. • Skale oceny zdolności, zamiarów i celów przeciwnika, w razie potrzeby opatrzone adnotacjami przez podmiot. (Tabela D-3, tabela D-4, tabela D-5)	Nie	Tak	Tak *o ile nie są uwzględnione na poziomie 2*

Opis	Warunek		
	poziom 1	poziom 2	poziom 3
• Skala oceny zakresu efektów, w razie potrzeby opatrzona adnotacjami przez podmiot. (Tabela D-6) • Źródła zagrożeń zidentyfikowane w poprzednich szacowaniach ryzyka, w stosownych przypadkach.			
Z poziomu 2: (poziom procesu biznesowego) • Informacje i wytyczne dotyczące źródeł zagrożeń specyficzne dla poziomu 2 (np. zagrożenia związane z procesami biznesowymi, segmentami EA, wspólną infrastrukturą, usługami wsparcia, zabezpieczeniami wspólnymi i zależnościami zewnętrznymi). • Specyficzna dla procesów biznesowych charakterystyka przeciwstawnych oraz nieprzeciwstawnych źródeł zagrożeń.	Tak *poprzez RAR*[53]	Tak *poprzez wzajemne udostępnianie*	Tak

[53] RAR – raport z szacowania ryzyka (*ang. Risk Assessment Report*)

Opis	Warunek		
	poziom 1	**poziom 2**	**poziom 3**
Z poziomu 3: (poziom systemu informatycznego) • Informacje i wskazówki dotyczące źródeł zagrożeń właściwe dla poziomu 3 (np. zagrożenia związane z systemami informatycznymi, technologiami informatycznymi, elementami systemów informatycznych, aplikacjami, sieciami, środowiskami działania). • Specyficzna dla systemu informatycznego charakterystyka agresywnych i nieagresywnych źródeł zagrożeń.	Tak *poprzez RAR*	Tak *poprzez RAR*	Tak *poprzez wzajemne udostępniani e*

Tabela D-2. Taksonomia źródeł zagrożeń.

Typ źródła zagrożeń	Opis	Charakterystyki
Wrogie • Osoba fizyczna ➢ Ousider ➢ Insider ➢ Zaufany Insider ➢ Uprzywilejowany Insider • Grupa ➢ Powołana ad hoc ➢ Uprzednio założona • Organizacja ➢ Konkurent ➢ Dostawca ➢ Partner ➢ Klient • Państwo	Osoby fizyczne, grupy, organizacje lub państwa, które starają się wykorzystać zależność podmioty od zasobów informatycznych (tj. informacji w postaci elektronicznej, technologii informacyjno-komunikacyjnych oraz możliwości w zakresie komunikacji i obsługi informacji, jakie zapewniają te technologie).	Zdolność, Zamiar, Ukierunkowanie
Przypadkowe • Użytkownik • Użytkownik uprzywilejowany lub Administrator	Niezamierzone błędne działania podejmowane przez osoby fizyczne w trakcie wykonywania swoich codziennych obowiązków.	Zakres skutków

Typ źródła zagrożeń	Opis	Charakterystyki
Strukturalne • Sprzęt informatyczny (IT) ➢ Pamięć ➢ Procesor ➢ Komunikacja ➢ Wyświetlacz ➢ Czujnik ➢ Sterownik • Sterowanie środowiskowe ➢ Sterowanie temperaturą lub wilgotnością ➢ Zasilanie energetyczne • Oprogramowanie ➢ System operacyjny ➢ Oprogramowanie sieciowe ➢ Aplikacja ogólnego przeznaczenia ➢ Aplikacja specyficzna	Awarie sprzętu, sterowania środowiskiem lub oprogramowania, spowodowane starzeniem się, wyczerpywaniem się zasobów lub innymi okolicznościami, które przekraczają oczekiwane parametry operacyjne.	Zakres skutków

Typ źródła zagrożeń	Opis	Charakterystyki
Środowiskowe • Klęska żywiołowa lub katastrofa spowodowana przez człowieka ➢ Ogień ➢ Powodzie/Tsunami ➢ Wichura/Tornado ➢ Huragan ➢ Trzęsienie ziemi ➢ Zamach terrorystyczny ➢ Skrajne warunki pogodowe • Nietypowe zdarzenia naturalne (np. burze słoneczne) • Awaria lub wyłączenie infrastruktury ➢ Telekomunikacyjnej ➢ Zasilania energetycznego	Klęski żywiołowe i awarie infrastruktur krytycznych, od których jest zależny podmiot, ale które są poza jego kontrolą. Uwaga: Klęski żywiołowe i katastrofy spowodowane przez człowieka można również scharakteryzować pod względem ich dotkliwości i czasu trwania. Ponieważ jednak źródło zagrożenia i zdarzenie zagrożenia są silnie zidentyfikowane, w opisie zdarzenia zagrożenia można uwzględnić jego dotkliwość i czas trwania (np. huragan kategorii 5 powoduje rozległe szkody w obiektach, w których znajdują się systemy o znaczeniu krytycznym, przez co systemy te są niedostępne przez trzy tygodnie).	Zakres skutków

Tabela D-3. Skale szacowania – charakterystyka zdolności przeciwnika.

Wartości jakościowe	Wartości mieszane		Opis
Bardzo wysoki	96-100	10	Przeciwnik ma bardzo wysoki poziom wiedzy specjalistycznej, jest dobrze wyposażony w zasoby i może generować możliwości wspierania wielu udanych, ciągłych i skoordynowanych ataków.
Wysoki	80-95	8	Przeciwnik ma wysoki poziom wiedzy specjalistycznej, dysponuje znacznymi zasobami i możliwościami wsparcia wielu udanych skoordynowanych ataków.
Umiarkowany	21-79	5	Przeciwnik dysponuje umiarkowanymi zasobami, wiedzą fachową i możliwościami wsparcia wielu udanych ataków.
Niski	5-20	2	Przeciwnik ma ograniczone zasoby, wiedzę fachową i możliwości wsparcia udanego ataku.
Bardzo niski	0-4	0	Przeciwnik dysponuje bardzo ograniczonymi zasobami, wiedzą fachową i możliwościami wspierania udanego ataku.

Tabela D-4. Skale szacowania – charakterystyka intencji przeciwnika.

Wartości jakościowe	Wartości mieszane		Opis
Bardzo wysoki	96-100	10	Przeciwnik dąży do osłabienia, poważnego utrudnienia lub zniszczenia podstawowej funkcji biznesowej, programu lub przedsięwzięcia poprzez wykorzystanie obecności w systemach informatycznych lub infrastrukturze organizacji. Przeciwnik obawia się, że ujawnienie informacji na temat jego umiejętności może utrudnić jego zdolność do osiągnięcia wyznaczonych celów.
Wysoki	80-95	8	Przeciwnik dąży do podważenia krytycznych aspektów kluczowej funkcji biznesowej, programu lub przedsięwzięcia lub też znalezienia się podmiotu w takiej sytuacji w przyszłości, poprzez utrzymanie obecności w systemach informatycznych lub infrastrukturze organizacji. Przeciwnik jest bardzo zaniepokojony możliwością wykrywania ataków, w szczególności podczas przygotowań do przyszłych ataków.

Wartości jakościowe	Wartości mieszane		Opis
Umiarkowany	21-79	5	Przeciwnik dąży do uzyskania lub modyfikacji określonych krytycznych lub wrażliwych informacji lub uzurpuje sobie prawo do ingerencji w informatyczne zasoby organizacji poprzez stworzenie zaplecza w jej systemach informatycznych lub infrastrukturze. Przeciwnik obawia się możliwości wykrywania ataku, szczególnie w przypadku przeprowadzania ataku w długim okresie czasu. Aby osiągnąć te cele przeciwnik ma zamiar utrudniać realizację funkcji biznesowych podmiotu.
Niski	5-20	2	Przeciwnik aktywnie dąży do uzyskania krytycznych lub wrażliwych informacji lub zamierza naruszyć zasoby informatyczne podmiotu i robi to bez obawy o wykrycie ataku.
Bardzo niski	0-4	0	Przeciwnik próbuje zakłócić lub zniszczyć zasoby informatyczne podmiotu i robi to bez obawy o wykrycie ataku.

Tabela D-5. Skale szacowania – charakterystyki ukierunkowania przeciwnika.

Wartości jakościowe	Wartości mieszane		Opis
Bardzo wysoki	96-100	10	Przeciwnik analizuje informacje uzyskane w wyniku rozpoznania i ataków w celu wytrwałego ukierunkowania na konkretny podmiot, przedsięwzięcie, program lub funkcję biznesową, koncentrując się na konkretnych informacjach o wysokiej wartości lub o krytycznym znaczeniu dla celu działania podmiotu, jego zasobach, przepływie dostaw lub funkcjach; konkretnym personelu lub stanowiskach; dostawcach usług, dostawcach infrastruktury wspierającej lub organizacjach partnerskich.
Wysoki	80-95	8	Przeciwnik analizuje informacje uzyskane podczas rekonesansu w celu wytrwałego ukierunkowania na konkretną organizację, przedsięwzięcie, program lub funkcję biznesową, koncentrując się na konkretnych informacjach o wysokiej wartości lub krytycznych dla celu działania podmiotu, jego zasobach, przepływach dostaw lub funkcjach, konkretnym personelu wspierających te funkcje lub kluczowych stanowiskach.

Wartości jakościowe	Wartości mieszane		Opis
Umiarkowany	21-79	5	Przeciwnik analizuje publicznie dostępne informacje w celu ukierunkowania ataku na konkretne podmioty o istotnym znaczeniu (w tym na osoby o istotnym znaczeniu dla funkcjonowania podmiotu np. CIO).
Niski	5-20	2	Przeciwnik wykorzystuje publicznie dostępne informacje, aby dotrzeć do pewnej klasy podmiotów lub informacji o wysokiej wartości i poszukuje możliwości osiągnięcia swoich celów w ramach tej klasy.
Bardzo niski	0-4	0	Przeciwnik może, ale nie musi, skierować się przeciwko konkretnym podmiotom lub klasom podmiotów.

Tabela D-6. Skale szacowania – zakres skutków dla źródeł zagrożeń o innym charakterze niż wrogi.

Wartości jakościowe	Wartości mieszane		Opis
Bardzo wysoki	96-100	10	Skutki błędu, wypadku lub działania sił natury są rozległe i dotyczą prawie wszystkich zasobów informatycznych [poziom 3: systemy informatyczne; poziom 2: procesy biznesowe lub segmenty EA[54], wspólna infrastruktura lub usługi wsparcia; poziom 1: struktura organizacyjna/administracyjna].
Wysoki	80-95	8	Skutki błędu, wypadku lub działania sił natury są rozległe i dotyczą większości zasobów informatycznych [poziom 3: systemy informatyczne; poziom 2: procesy biznesowe lub segmenty EA, wspólna infrastruktura lub usługi wsparcia; poziom 1: struktura organizacyjna/administracyjna], w tym wielu zasobów krytycznych.

[54] EA – architektura korporacyjna (*ang. Enterprise Architecture*)

Wartości jakościowe	Wartości mieszane		Opis
Umiarkowany	21-79	5	Skutki błędu, wypadku lub działania sił natury mają szeroki zakres i dotyczą znacznej części zasobów informatycznych [poziom 3: systemy informatyczne; poziom 2: procesy biznesowe lub segmenty EA, wspólna infrastruktura lub usługi wsparcia; poziom 1: struktura organizacyjna/administracyjna], w tym niektórych zasobów krytycznych.
Niski	5-20	2	Skutki błędu, wypadku lub działania sił natury są ograniczone i dotyczą niektórych zasobów cybernetycznych [poziom 3: systemy informatyczne; poziom 2: procesy biznesowe lub segmenty EA, wspólna infrastruktura lub usługi wsparcia; poziom 1: struktura organizacyjna/administracyjna], ale nie obejmują krytycznych zasobów.

Wartości jakościowe	Wartości mieszane		Opis
Bardzo niski	0-4	0	Skutki błędu, wypadku lub działania sił natury są minimalne i dotyczą niewielu, jeśli w ogóle, zasobów informatycznych [poziom 3: systemy informatyczne; poziom 2: procesy biznesowe lub segmenty EA, wspólna infrastruktura lub usługi wsparcia; poziom 1: struktura organizacyjna/administracyjna] i nie obejmują krytycznych zasobów.

Tabela D-7. Szablon – Identyfikacja wrogich źródeł zagrożeń.

Identyfikator	Źródło informacji o źródłach zagrożeń	W zakresie	Zdolność	Zamiar	Ukierunkowanie
Definiowane przez podmiot	Tabela D-2 i Zadanie 1-4 lub Definiowane przez podmiot	Tak / Nie	Tabela D-3 lub Definiowane przez podmiot	Tabela D-4 lub Definiowane przez podmiot	Tabela D-5 lub Definiowane przez podmiot

Tabela D-8. Szablon – Identyfikacja źródeł zagrożeń o innym charakterze niż wrogi.

Identyfikator	Źródło informacji o źródłach zagrożeń	W zakresie	Zakres skutków
Definiowane przez podmiot	Tabela D-2 i Zadanie 1-4 lub Definiowane przez podmiot	Tak / Nie	Tabela D-6 lub Definiowane przez podmiot

ZAŁĄCZNIK E ZDARZENIA ZAGROŻEŃ

Reprezentatywne zdarzenia zagrożeń zainicjowane przez źródła zagrożeń

Niniejszy załącznik przedstawia: (i) opis potencjalnie użytecznych danych wejściowych do zadania identyfikacji zdarzeń zagrożenia; (ii) reprezentatywne przykłady wrogich zdarzeń zagrożenia wyrażone, jako taktyka, techniki i procedury (TTP) oraz zdarzenia zagrożenia innym charakterze niż wrogi; (iii) przykładową skalę oceny przydatności tych zdarzeń zagrożenia; oraz (iv) wzory podsumowujące i dokumentujące wyniki zadania 2-2 identyfikacji zagrożeń. Podmioty mogą wyeliminować pewne zdarzenia powodujące zagrożenie z dalszego rozpatrywania, jeżeli nie zidentyfikowano przeciwnika posiadającego niezbędne zdolności. Podmioty mogą również modyfikować przedstawione zdarzenia powodujące zagrożenie w celu opisania konkretnych TTP z wystarczającą szczegółowością oraz na odpowiednim poziomie klasyfikacji. Tabela E-5, będąca wynikiem zadania 2-2, zawiera odpowiednie dane wejściowe do tabel ryzyka w Załączniku I.

Tabela E-9. Wejście – Identyfikacja zdarzeń zagrożeń.

Opis	Pod warunkiem		
	poziom 1	poziom 2	poziom 3
Z poziomu 1: (poziom organizacji) • Źródła informacji o zagrożeniach uznane za wiarygodne (np. otwarte źródła i/lub niejawne raporty o zagrożeniach, wcześniejsze oceny ryzyka/zagrożeń. (sekcja 3.1, zadanie 1-4.) • Informacje o zdarzeniach zagrożeń i wytyczne właściwe dla poziomu 1 (np. zagrożenia związane z zarządzaniem podmiotem, podstawowymi zadaniami/funkcjami biznesowymi, zewnętrznymi zadaniami/kontaktami biznesowymi, polityką, procedurami i strukturami zarządzania/operacji). • Przykładowe zdarzenia zagrożeń o charakterze agresywnym, w razie potrzeby opatrzone adnotacją przez organizację. (Tabela E-2) • Przykładowe zdarzenia zagrożeń o innym charakterze niż agresywny, w razie potrzeby opatrzone adnotacją organizacji. (Tabela E-3)	Nie	Tak	Tak, *o ile nie są uwzględnione na poziomie 2*

Opis	Pod warunkiem		
	poziom 1	poziom 2	poziom 3
• Skala oceny trafności zdarzeń zagrożeń, w razie potrzeby opatrzona adnotacjami przez organizację. (Tabela E-4) • Zdarzenia zagrażające zidentyfikowane w poprzednich ocenach ryzyka, w stosownych przypadkach			
Z poziomu 2: (poziom procesu biznesowego) • Informacje i wytyczne dotyczące zdarzeń zagrożeń specyficzne dla poziomu 2 (np. zagrożenia związane z procesami biznesowymi, segmentami EA, wspólną infrastrukturą, usługami wsparcia, zabezpieczeniami wspólnymi i zależnościami zewnętrznymi). • Specyficzna dla procesów biznesowych charakterystyka agresywnych i nieagresywnych zdarzeń zagrożeń.	Tak *poprzez RAR*	Tak *poprzez wzajemne udostępnianie*	Tak

Opis	Pod warunkiem		
	poziom 1	poziom 2	poziom 3
Z poziomu 3: (poziom systemu informatycznego) • Informacje o zdarzeniach powodujących zagrożenie i wytyczne charakterystyczne dla poziomu 3 (np. zagrożenia związane z systemami informatycznymi, technologiami informatycznymi, elementami systemów informatycznych, aplikacjami, sieciami, środowiskami działania). • Specyficzna dla systemu informatycznego charakterystyka agresywnych i nieagresywnych zdarzeń zagrożeń. • Raporty o zdarzeniach.	Tak *poprzez RAR*	Tak *poprzez RAR*	Tak *Poprzez wzajemne udostępnia nie*

Tabela E-10. Reprezentatywne przykłady zdarzeń zagrożeń o charakterze agresywnym.

Zdarzenie zagrożenia (charakteryzowane przez TTP)	Opis
Przeprowadzenie rozpoznania i zebranie informacji.	
Wykonanie rozpoznania/skanowania brzegu sieci.	Przeciwnik używa komercyjnego lub wolnego oprogramowania do skanowania brzegu sieci podmiotu w celu uzyskania lepszego zrozumienia infrastruktury informatycznej i poprawy zdolności do przeprowadzania udanych ataków.
Wykonanie podsłuchu (snifing) eksponowanych sieci	Przeciwnik z dostępem do odsłoniętych przewodowych lub bezprzewodowych kanałów danych używanych do przesyłania informacji dokonuje podsłuchu ruchu w sieci w celu identyfikacji komponentów, zasobów i zabezpieczeń.
Zbieranie informacji z otwartych źródeł w celu uzyskania informacji o podmiocie.	Przeciwnik wydobywa publicznie dostępne informacje w celu zebrania informacji o systemach informatycznych podmiotu, jego procesach biznesowych, użytkownikach lub personelu, lub relacjach zewnętrznych, które może następnie wykorzystać do wsparcia ataku.

Zdarzenie zagrożenia (charakteryzowane przez TTP)	Opis
Prowadzenie rozpoznania i inwigilacji podmiotu mającego się stać celem ataku	Przeciwnik przez pewien czas używa różnych środków (np. skanowania, obserwacji fizycznej), aby zbadać i ocenić podmiot oraz ustalić podatności na zagrożenia.
Wykonanie rozpoznania z wykorzystaniem oprogramowania złośliwego.	Przeciwnik używa złośliwego oprogramowania zainstalowanego wewnątrz systemu teleinformatycznego podmiotu w celu identyfikacji możliwości osiągnięcia celu ataku. Ponieważ skanowanie, sondowanie lub obserwacja nie przekraczają granic systemu, nie są one wykrywane przez umieszczone na granicy systemu narzędzia wykrywania włamań.

Zdarzenie zagrożenia (charakteryzowane przez TTP)	Opis
Tworzenie narzędzi ataku.	
Tworzenie ataku typu phishing (fiszing).	Przeciwnik rozsyła sfałszowane komunikaty, które mają służyć do pozyskiwania poufnych informacji, takich jak nazwy użytkowników lub hasła. Typowe ataki mają miejsce za pośrednictwem poczty elektronicznej, komunikatorów internetowych lub podobnych środków; komunikaty takie zwykle kierują użytkowników na strony internetowe, które wydają się być legalne, a jednocześnie faktycznie kradną wprowadzone informacje albo zachęcają do pobrania załączników zawierających oprogramowanie złośliwe.
Tworzenie kierowanych ataków fiszingowych.	Przeciwnik stosuje ataki fiszingowe ukierunkowane na cele o wysokiej wartości (np. kierownictwo podmiotu, użytkownicy uprzywilejowani, administratorzy systemu).
Tworzenie ataków z wykorzystaniem wiedzy o środowisku informatycznym podmiotu.	Przeciwnik rozwija atak (np. tworząc ukierunkowane złośliwe oprogramowanie), które wykorzystuje wiedzę przeciwnika na temat środowiska informatycznego podmiotu.

Zdarzenie zagrożenia (charakteryzowane przez TTP)	Opis
Tworzenie podrobionych stron internetowych.	Przeciwnik tworzy duplikaty legalnych stron internetowych; gdy użytkownik odwiedza podrobioną witrynę, przeciwnik może gromadzić poufne informacje lub przekazywać złośliwe oprogramowanie.
Tworzenie sfałszowanych certyfikatów.	Przeciwnik podszywa się lub kompromituje organ wydający certyfikat, tak aby złośliwe oprogramowanie lub połączenia wydawały się legalne.
Tworzenie i obsługa fałszywych podmiotów fasadowych w celu wstrzyknięcia złośliwych komponentów do łańcucha dostaw.	przeciwnik tworzy fałszywe podmioty o charakterze fasadowym na pozór wyglądających jak legalni dostawcy na krytycznej ścieżce cyklu życia systemu, które to podmioty wprowadzają do łańcucha dostaw atakowanego podmiotu uszkodzone lub złośliwe elementy systemu informatycznego.

Zdarzenie zagrożenia (charakteryzowane przez TTP)	Opis
Dostarczanie, wprowadzanie, instalowanie złośliwego oprogramowania	
Dostarczanie znanego złośliwego oprogramowania do wewnętrznych systemów informatycznych organizacji (np. wirusów za pośrednictwem poczty elektronicznej).	Przeciwnik wykorzystuje powszechne mechanizmy dostarczania (np. pocztę elektroniczną), aby zainstalować/wprowadzić znane złośliwe oprogramowanie do systemów informatycznych podmiotu.
Dostarczanie zmodyfikowanego złośliwego oprogramowania do wewnętrznych systemów informatycznych podmiotu.	Przeciwnik wykorzystuje bardziej zaawansowane mechanizmy dostarczania niż poczta elektroniczna (np. ruch w sieci, komunikatory internetowe, FTP) do dostarczania złośliwego oprogramowania i ewentualnie modyfikacji znanego złośliwego oprogramowania w celu uzyskania dostępu do wewnętrznych systemów informatycznych podmiotu.
Dostarczanie celowanego oprogramowania złośliwego do kontroli systemów wewnętrznych i eksfiltracji danych.	Przeciwnik instaluje złośliwe oprogramowanie, które zostało zaprojektowane specjalnie w celu przejęcia kontroli nad wewnętrznymi systemami informatycznymi podmiotu, identyfikacji informacji wrażliwych, przekazania ich z powrotem do przeciwnika i ukrycia tych działań.

Zdarzenie zagrożenia (charakteryzowane przez TTP)	Opis
Dostarczanie oprogramowania złośliwego na wymiennych nośnikach danych.	Przeciwnik umieszcza nośniki wymienne (np. pendrive'y) zawierające złośliwe oprogramowanie w miejscach poza fizycznymi granicami podmiotu, ale w których pracownicy mogą je znaleźć (np. parkingi obiektów, wystawy na konferencjach, w których uczestniczą pracownicy) z założeniem, że te nośniki zostaną wykorzystane w systemach informatycznych podmiotu i w ten sposób zainfekują ten system.
Umieszczanie niecelowanego oprogramowania złośliwego w oprogramowaniu do pobrania i/lub do komercyjnych produktów informatycznych.	Przeciwnik niszczy lub wprowadza złośliwe oprogramowanie do powszechnie stosowanych programów typu freeware, shareware lub komercyjnych produktów informatycznych. Przeciwnik nie kieruje ataku do konkretnego podmiotu, po prostu szuka punktów wejścia do wewnętrznych systemów informatycznych jakiegokolwiek podmiotu. Należy pamiętać, że jest to szczególnie ważne w przypadku aplikacji mobilnych.

Zdarzenie zagrożenia (charakteryzowane przez TTP)	Opis
Wprowadzanie celowanego oprogramowania złośliwego do systemów informatycznych podmiotu.	Przeciwnik wstawia złośliwe oprogramowanie do systemów informatycznych podmiotu oraz do komponentów systemów informatycznych (np. do komercyjnych produktów informatycznych), ukierunkowane specjalnie na sprzęt, oprogramowanie i firmware wykorzystywane przez podmiot (w oparciu o wiedzę zdobytą podczas rekonesansu).
Wprowadzanie specjalistycznego oprogramowania złośliwego do systemów informatycznych podmiotu bazując na konfiguracji systemu.	Przeciwnik wprowadza specjalistyczne, niewykrywalne, oprogramowanie złośliwe do systemów informatycznych atakowanego podmiotu, w szczególności do krytycznych komponentów systemów, w oparciu o konfiguracje systemowe.
Wprowadzenie do łańcucha dostaw podrobionego lub przerobionego sprzętu.	Przeciwnik przechwytuje sprzęt od legalnych dostawców, modyfikuje go lub zastępuje sprzętem wadliwym lub w inny sposób zmodyfikowanym.
Wprowadzenie do systemów informatycznych podmiotu zmienionych komponentów o znaczeniu krytycznym.	Przeciwnik zastępuje, poprzez łańcuch dostaw, skorumpowany personel lub jakąś kombinację tych sposobów, krytyczne komponenty systemu informatycznego komponentami zmodyfikowanymi lub uszkodzonymi.

Zdarzenie zagrożenia (charakteryzowane przez TTP)	Opis
Instalowanie sniferów wewnątrz sieci podmiotu.	Przeciwnik instaluje powszechnie dostępne oprogramowanie podsłuchujące ruch w sieci do wewnętrznych systemów informatycznych podmiotu lub jego sieci wewnętrznej.
Instalowanie trwałych i ukierunkowanych sniferów w systemach i sieciach informatycznych podmiotu.	Przeciwnik instaluje specjalizowane oprogramowanie podsłuchujące ruch do wewnętrznych systemów informatycznych podmiotu lub jego sieci wewnętrznej.
Instalowanie urządzenia skanującego (np. bezprzewodowy snifer) wewnątrz systemu teleinformatycznego podmiotu.	Przeciwnik wykorzystuje tradycyjne usługi pocztowe lub inne komercyjne usługi doręczania przesyłek, aby dostarczyć do kancelarii pocztowych podmiotu urządzenie, które jest w stanie skanować komunikację bezprzewodową dostępną w otoczeniu, a następnie bezprzewodowo przesyłać informacje z powrotem do przeciwnika.
Umieszczanie w podmiocie podstawionych osób.	Przeciwnik umieszcza w podmiocie osoby, które są chętne i zdolne do podejmowania działań mających na celu zaszkodzenie podmiotowi.

Zdarzenie zagrożenia (charakteryzowane przez TTP)	Opis
Umieszczanie w podmiocie podstawionych osób na uprzywilejowanych stanowiskach.	Przeciwnik podstawia w podmiocie na uprzywilejowanych stanowiskach osoby, które są chętne i zdolne do podejmowania działań mających na celu zaszkodzenie podmiotowi. Przeciwnik może ukierunkować swoje działanie w celu uzyskania dostępu do uprzywilejowanych funkcji w celu uzyskania dostępu do poufnych informacji (np. kont użytkowników, plików systemowe itp.) i może wykorzystać dostęp do jednej uprzywilejowanej funkcji w celu uzyskania dostępu do innej funkcji.
Wykorzystanie podatności i kompromitacja zabezpieczeń	
Wykorzystanie autoryzowanego personelu, aby uzyskać fizyczny dostęp do obiektów podmiotu.	Przeciwnik podąża za upoważnionymi osobami ("ogon") do obszaru bezpieczeństwa w celu uzyskania dostępu do obiektów, omijając zabezpieczenia fizyczne.
Wykorzystanie podatności w słabo skonfigurowanych lub nieautoryzowanych systemach informatycznych mających kontakt z Internetem.	Przeciwnik uzyskuje za pośrednictwem Internetu dostęp do systemów informatycznych, które nie są autoryzowane do łączenia się z Internetem lub nie spełniają wymogów bezpiecznej konfiguracji.

Zdarzenie zagrożenia (charakteryzowane przez TTP)	Opis
Wykorzystanie tunelowania	Przeciwnik korzysta z zewnętrznych stacji roboczych (np. laptopów w odległych lokalizacjach), które są bezpiecznie podłączone do systemów informatycznych lub sieci albo połączenia zdalne nie są właściwie zabezpieczone.
Wykorzystanie podatności powodującej przesłuch pomiędzy tenantami w rozwiązaniach chmurowych.	Przeciwnik w środowisku chmury obliczeniowej wykorzystuje podatność umożliwiającą z jednego tenantu obserwowania zachowań procesów, pozyskiwania informacji lub ingerowania w terminowe lub prawidłowe funkcjonowanie procesów w innym tenancie.
Wykorzystanie znanych podatności w systemach mobilnych (np. laptopach, PDA, smartfonach).	Przeciwnik z uwagi na to, że mobilne systemy informatyczne znajdują się poza fizyczną ochroną podmiotu oraz logiczną ochroną zapór sieciowych systemu, wykorzystuje znane podatności, aby zdobyć poufne informacje.
Wykorzystanie nowoodkrytych podatności.	Przeciwnik wykorzystuje niedawno podatności w systemie informatycznym, próbując skompromitować te systemy, zanim zostaną udostępnione lub wprowadzone środki zaradcze.

Zdarzenie zagrożenia (charakteryzowane przez TTP)	Opis
Wykorzystanie podatności wewnątrz systemu teleinformatycznego.	Przeciwnik wyszukuje znane podatności w wewnętrznych systemach informatycznych podmiotu i wykorzystuje te podatności.
Wykorzystanie podatności w ataku z użyciem „zero day exploit”.	Przeciwnik stosuje ataki, które wykorzystują jeszcze niepublikowane podatności. Ataki takie umożliwiają wgląd przeciwnikowi w systemy informatyczne i aplikacje wykorzystywane przez podmiot.
Synchronizacja czasu ataku z momentem krytycznych działań podmiotu.	Przeciwnik przeprowadza ataki na podmiot w czasie i w taki sposób, aby jak najdotkliwiej zaszkodzić działalności podmiotu.
Wykorzystanie niepewnego lub niekompletnego usuwania danych w środowisku wielo-tenantowym.	Przeciwnik uzyskuje informacje z powodu niepewnego lub niepełnego usunięcia danych w środowisku wielo-tenantowym (np. w środowisku chmury obliczeniowej).
Naruszenie izolacji w środowisku wielo-tenantowym.	Przeciwnik obchodzi lub pokonuje mechanizmy izolacji w środowisku wielo-tenantowym (np. w środowisku chmury obliczeniowej) w celu obserwacji, niszczenia informacji/danych lub odmowy świadczenia usług.
Kompromitacja krytycznych systemów informatycznych poprzez dostęp fizyczny.	Przeciwnik uzyskuje fizyczny dostęp do systemów informatycznych organizacji i dokonuje modyfikacji.

Zdarzenie zagrożenia (charakteryzowane przez TTP)	Opis
Kompromitacja systemu lub urządzenia na zewnątrz podmiotu i ponowne wprowadzenie go do eksploatacji.	Przeciwnik instaluje złośliwe oprogramowanie w systemach lub urządzeniach informatycznych, podczas gdy systemy/urządzenia są zewnętrzne w stosunku do podmiotu w celu późniejszego zainfekowania systemu po ponownym podłączeniu.
Kompromitacja oprogramowania krytycznych systemów informatycznych.	Przeciwnik umieszcza złośliwe oprogramowanie lub w inny sposób niszczy wewnętrzne, krytyczne systemy informacyjne atakowanego podmiotu.
Kompromitacja systemów informatycznych ułatwiająca eksfiltrację danych/informacji.	Przeciwnik wprowadza do systemu informatycznego podmiotu złośliwe komponenty, które z czasem doprowadzają do wyprowadzenia informacji na zewnątrz.
Kompromitacja informacji o krytycznym znaczeniu dla procesów biznesowych	Przeciwnik naraża na szwank integralność informacji o krytycznym znaczeniu dla działalności podmiotu, uniemożliwiając w ten sposób lub utrudniając podmiotowi, któremu dostarczane są informacje prowadzenie działalności.

Zdarzenie zagrożenia (charakteryzowane przez TTP)	Opis
Kompromitacja projektowania, produkcji lub dystrybucji elementów systemu informacyjnego (w tym sprzętu, oprogramowania i oprogramowania sprzętowego).	Przeciwnik naraża na szwank projekt, produkcję lub dystrybucję krytycznych komponentów systemu informatycznego u wybranych dostawców.
Prowadzenie ataku	
Ataki przechwytywania komunikacji.	Przeciwnik wykorzystuje komunikację niezaszyfrowaną lub wykorzystującą słabe szyfrowanie (np. szyfrowanie zawierające publicznie znane wady), przekierowuje tą komunikację i uzyskuje dostęp do przekazywanych informacji i kanałów jej przekazywania.
Atak poprzez zagłuszanie komunikacji bezprzewodowego	Przeciwnik podejmuje środki mające na celu zakłócenie komunikacji bezprzewodowej, tak aby utrudnić lub uniemożliwić dotarcie komunikacji do zamierzonych odbiorców.
Atak z wykorzystaniem nieautoryzowanych portów, protokołów i usług sieciowych.	Przeciwnik przeprowadza ataki z wykorzystaniem portów, protokołów i usług, które nie są dopuszczone do użytku przez podmiot.

Zdarzenie zagrożenia (charakteryzowane przez TTP)	Opis
Atak z wykorzystaniem dozwolonych metod komunikowania.	Przeciwnik korzysta z dozwolonych przepływów informacji (np. komunikacja za pomocą poczty elektronicznej, nośniki wymienne) w celu kompromitacji wewnętrznych systemów informacyjnych, co pozwala przeciwnikowi na uzyskiwanie i przekazywanie poufnych informacji przez zabezpieczenia obwodowe.
Proste ataki w celu odmowy usługi (DoS)	Przeciwnik podejmuje próbę uczynienia zasobu dostępnego w Internecie niedostępnym dla docelowych użytkowników lub uniemożliwienia mu sprawnego lub całkowitego funkcjonowania, tymczasowo lub bezterminowo.
Rozproszone ataki w celu odmowy usługi (DDoS)	Przeciwnik wykorzystuje wiele skompromitowanych systemów informatycznych do atakowania jednego celu, powodując tym samym odmowę świadczenia usług dla użytkowników docelowych systemów informatycznych.
Celowane ataki w celu odmowy usługi (DoS)	Przeciwnik wykonuje atak DoS na krytyczne systemy informatyczne podmiotu, jego komponenty lub infrastrukturę wspierającą lub bazując na swojej wiedzy o zależnościach występujących w systemie.

Zdarzenie zagrożenia (charakteryzowane przez TTP)	Opis
Fizyczne ataki na obiekty.	Przeciwnik przeprowadza fizyczny atak na obiekty (np. poprzez podpalenie).
Fizyczne ataki na infrastrukturę wspierającą obiekty podmiotu.	Przeciwnik przeprowadza fizyczny atak na jedną lub więcej infrastruktur wspierających obiekty podmiotu (np. przerywa sieć wodociągową, przerywa linię energetyczną).
Cyberataki na obiekty podmiotu.	Przeciwnik przeprowadza cyberatak na obiekty podmiotu (np. zdalnie zmienia ustawienia HVAC).
Przeprowadzanie ataków poprzez odzyskiwanie niedostatecznie skutecznie wykasowanych danych w środowisku chmury obliczeniowej.	Przeciwnik uzyskuje dostęp do danych wykorzystywanych w przetwarzaniu chmurowym, które po wykorzystaniu nie zostały skutecznie usunięte.
Ataki typu „brute force” na hasła służące do logowania	Przeciwnik próbuje uzyskać dostęp do systemów informatycznych organizacji podmiotu poprzez losowe lub systematyczne odgadywanie haseł, ewentualnie wspomagane przez narzędzia do łamania haseł.
Przeprowadzanie nieukierunkowanych ataków typu zero-day.	Przeciwnik stosuje ataki, które wykorzystują jeszcze niepublikowane podatności. Ataki nie są kierowane pod adresem konkretnego podmiotu.

Zdarzenie zagrożenia (charakteryzowane przez TTP)	Opis
Atak poprzez przechwycenie sesji zewnętrznej.	Przeciwnik przejmuje kontrolę (dokonuje „porwania") nad już ustalonymi, legalnymi sesjami systemu informatycznego pomiędzy danym podmiotem i podmiotami zewnętrznymi (np. użytkownikami łączącymi się z lokalizacji zewnętrznych).
Atak poprzez przechwycenie sesji wewnętrznej.	Przeciwnik umieszcza w podmiocie osobę w celu uzyskania dostępu do systemów informatycznych przejęcia kontroli („porwania") nad już istniejącą, legalną sesją (np. użytkownicy łączący się z odległych lokalizacji) albo pomiędzy dwoma lokalizacjami w ramach sieci wewnętrznych.

Zdarzenie zagrożenia (charakteryzowane przez TTP)	Opis
Przeprowadzanie ataków polegających na zewnętrznej modyfikacji ruchu sieciowego (rodzaj ataku typu „man in the middle").	Przeciwnik, działając poza system podmiotu, przechwytuje/podsłuchuje komunikat od nadawcy i modyfikuje treść przekazu. Następnie przeciwnik przekazuje wiadomości do właściwego odbiorcy, sprawiając, że wierzy on, iż nadawca i odbiorca komunikują się bezpośrednio przez prywatne połączenie, podczas gdy w rzeczywistości cała komunikacja jest kontrolowana przez przeciwnika. Ataki takie mogą mieć miejsce w szczególności, gdy podmiot korzysta z usług chmurowych wspólnotowych, hybrydowych lub publicznych.
Przeprowadzanie ataków polegających na wewnętrznej modyfikacji ruchu sieciowego (rodzaj ataku typu „man in the middle").	Przeciwnik działający w ramach infrastruktury podmiotu przechwytuje lub niszczy sesje przekazu danych.
Prowadzenie z zewnątrz ataku o charakterze inżynierii społecznej w celu uzyskania informacji.	Zewnętrzny przeciwnik podejmuje działania (np. za pomocą poczty elektronicznej, telefonu) z zamiarem przekonania lub w inny sposób oszukania osób w podmiocie skłaniających do ujawnienia krytycznych/wrażliwych informacji (np. danych osobowych, danych służących uwierzytelnieniu).

Zdarzenie zagrożenia (charakteryzowane przez TTP)	Opis
Prowadzenie z wewnątrz ataku o charakterze inżynierii społecznej w celu uzyskania informacji.	Przeciwnik umieszczony wewnątrz podmiotu podejmuje działania (np. za pomocą poczty elektronicznej, telefonu), tak aby osoby zatrudnione w podmiocie ujawniały informacje krytyczne/wrażliwe.
Przeprowadzanie ataków na urządzenia osobiste krytycznych pracowników.	Przeciwnik kieruje atak na kluczowych pracowników podmiotu poprzez umieszczanie złośliwego oprogramowania w ich osobistych systemach i urządzeniach informatycznych (np. laptopach, smartfonach). Intencją jest wykorzystanie wszelkich przypadków, w których pracownicy wykorzystują systemy lub urządzenia osobiste do obsługi krytycznych/wrażliwych informacji.
Przeprowadzanie ataków w ramach łańcucha dostaw ukierunkowanych na krytyczny sprzęt, oprogramowanie lub oprogramowanie sprzętowe.	Przeciwnik prowadzi działanie polegające na kompromitacji oprogramowania (np. poprzez wstrzyknięcia złośliwego kodu), oprogramowania sprzętowego i sprzęt, który pełni dla podmiotu funkcje krytyczne. Jest to w dużej mierze osiągane w formie ataków w łańcuchu dostaw zarówno na produkty dostarczane przez legalnych dostawców, jak i poprzez podszycie się pod legalnego dostawcę.

Zdarzenie zagrożenia (charakteryzowane przez TTP)	Opis
Osiągnięcie wyników (tj. spowodowanie negatywnych skutków, uzyskanie informacji)	
Pozyskiwanie poufnych informacji poprzez podsłuch w sieci zewnętrznej.	Przeciwnik z dostępem do odsłoniętych przewodowych lub bezprzewodowych kanałów danych, które podmioty lub ich personel wykorzystują do przesyłania informacji (np. kioski, publiczne sieci bezprzewodowe) przechwytuje komunikację.
Uzyskiwanie poufnych informacji poprzez eksfiltrację.	Przeciwnik umieszcza złośliwe oprogramowanie w systemie informatycznym podmiotu w celu zlokalizowania i ukrytego przekazywania poufnych informacji.
Powodowanie degradacji lub odmowy dostępu do wybranych usług atakowanego.	Przeciwnik wprowadza złośliwe oprogramowanie do systemu informatycznego podmiotu w celu osłabienia prawidłowego i terminowego wsparcia funkcji biznesowych tego podmiotu.
Powodowanie uszkodzenia/zniszczenia krytycznych elementów i funkcji systemu informatycznego.	Przeciwnik niszczy lub uszkadza krytyczne elementy systemu informatycznego w celu utrudnienia lub wyeliminowania zdolności podmiotu do wykonywania funkcji biznesowych. Wykrycie tego działania nie stanowi problemu.

Zdarzenie zagrożenia (charakteryzowane przez TTP)	Opis
Powodowanie utraty integralności poprzez tworzenie, usuwanie i/lub modyfikowanie danych w publicznie dostępnych systemach informatycznych (np. usuwanie danych ze stron www)	Przeciwnik dewastuje lub w inny sposób dokonuje nieautoryzowanych zmian na stronach internetowych, podmiotu.
Powodowanie utraty integralności poprzez zanieczyszczenie lub uszkodzenie krytycznych danych.	Przeciwnik zniekształca krytyczne dane lub wprowadza w ich miejsce dane błędne powodujące nieoptymalne działanie systemu lub utratę zaufania do danych/usług podmiotu.
Powodowanie utraty integralności poprzez wprowadzanie fałszywych, ale wiarygodnych danych do systemów informatycznych podmiotu.	Przeciwnik wprowadza fałszywe, ale wiarygodne dane do systemów informatycznych podmiotu, co skutkuje nieoptymalnymi działaniami lub utratą zaufania do danych/usług podmiotu.
Powodowanie ujawnienia krytycznych lub wrażliwych informacji przez upoważnionych użytkowników.	Przeciwnik skłania (np. poprzez inżynierię społeczną) upoważnionych użytkowników do nieumyślnego ujawnienia krytycznych/wrażliwych informacji.

Zdarzenie zagrożenia (charakteryzowane przez TTP)	Opis
Powodowanie nieautoryzowanego ujawnienia lub niedostępności poprzez rozlewanie poufnych informacji.	Przeciwnik zanieczyszcza systemy informatyczne podmiotu (w tym urządzenia i sieci), powodując, że obsługują one informacje o klasyfikacji, do których nie zostały upoważnione. Informacja jest narażona na kontakt z osobami, które nie są upoważnione do dostępu do takich informacji, a system informatyczny, urządzenie lub sieć stają się niedostępne podczas badania wycieku i ograniczania jego skutków.
Uzyskiwanie informacji poprzez zewnętrzne przechwytywanie ruchu w sieci bezprzewodowej.	Przeciwnik przechwytuje komunikację podmiotu prowadzoną poprzez sieci bezprzewodowe. Przykładem może być używanie publicznego dostępu bezprzewodowego lub połączenia sieciowego w hotelach, a także przełamanie zabezpieczeń routerów bezprzewodowych.
Uzyskanie nieautoryzowanego dostępu.	Przeciwnik z autoryzowanym dostępem do systemów informatycznych podmiotu, uzyskuje dostęp do zasobów wykraczający poza autoryzację.
Uzyskiwanie danych wrażliwych informacji z publicznie dostępnych systemów informatycznych.	Przeciwnik skanuje lub wydobywa informacje na publicznie dostępnych serwerach i stronach internetowych podmiotu z zamiarem znalezienia informacji wrażliwych.

Zdarzenie zagrożenia (charakteryzowane przez TTP)	Opis
Uzyskiwanie informacji poprzez kradzież elementów systemu informatycznego lub odzyskiwanie niestarannie usuniętych danych.	Przeciwnik kradnie systemy informatyczne lub ich komponenty (np. laptopy lub nośniki danych), które są pozostawione bez nadzoru poza fizycznymi granicami organizacji, lub odzyskuje dane z wyrzuconych komponentów systemu.
Utrzymanie obecności lub zestawu możliwości	
Obezwładnianie przeciwdziałań.	Przeciwnik podejmuje działania mające na celu zahamowanie skuteczności systemów wykrywania włamań lub zdolności audytowych w podmiotach.
Dostosowywanie cyberataków w oparciu o rozpoznanie sposobu nadzoru i środków bezpieczeństwa.	Przeciwnik dostosowuje zachowanie w odpowiedzi na nadzór i środki bezpieczeństwa stosowane w podmiocie.
Koordynacja kampanii	
Koordynacja kampanii ataków prowadzonych z wielu źródeł.	Przeciwnik przenosi źródło złośliwych poleceń lub działań z jednego przechwyconego i zainfekowanego systemu informatycznego do drugiego, utrudniając analizę.

Zdarzenie zagrożenia (charakteryzowane przez TTP)	Opis
Koordynacja kampanii łączącej ataki wewnętrzne i zewnętrzne prowadzone z wielu systemów informatycznych i stosujących różne technologie informatyczne.	Przeciwnik, aby osiągnąć sukces łączy ze sobą ataki, które wymagają zarówno fizycznej obecności w obiektach podmiotu, jak i metod informatycznych. Etapy fizycznego ataku mogą być tak proste, jak przekonanie pracowników obsługi technicznej, aby pozostawili otwarte drzwi lub szafki.
Koordynacja kampanii w wielu podmiotach w celu uzyskania konkretnych informacji lub osiągnięcia pożądanych rezultatów.	Przeciwnik nie ogranicza planowania do ukierunkowania ataku na jeden podmiot. Przeciwnik śledzi aktywność wielu podmiotów w celu uzyskania niezbędnych informacji na temat celów swojego zainteresowania.
Koordynacja kampanii, która rozprzestrzenia ataki na systemy podmiotu z istniejącej już obecności w jakimś systemie podmiotu.	Przeciwnik wykorzystuje istniejącą obecność w jakimś systemie podmiotu w celu rozszerzenia zakresu swoich działań na inne systemy, w tym na infrastrukturę. W ten sposób przeciwnik jest w stanie jeszcze bardziej osłabić zdolność podmiotu do realizowania funkcji biznesowych lub jest w stanie pozyskać szczególnie wrażliwe dane.
Koordynacja kampanii ciągłych, adaptacyjnych i zmieniających się ataków cybernetycznych w oparciu o szczegółowy nadzór.	Prowadzone przez przeciwnika ataki stale zmieniają się w odpowiedzi na ich rozpoznanie przez nadzór po stronie atakowanego podmiotu i podejmowane środki bezpieczeństwa.

Zdarzenie zagrożenia (charakteryzowane przez TTP)	Opis
Koordynacja cyberataków z wykorzystaniem wektorów ataku w postaci źródeł zewnętrznych (outsider), wewnętrznych (insider) i łańcucha dostaw (dostawców).	Przeciwnik stosuje ciągłe, skoordynowane ataki, potencjalnie wykorzystując wszystkie trzy wektory ataku w celu utrudnienia przeciwdziałania służb podmiotu.

Tabela E-11. Reprezentatywne przykłady zdarzeń zagrożeń o charakterze nieagresywnym.

Zdarzenie zagrożenia	Opis
Wyciek wrażliwej informacji.	Autoryzowany użytkownik błędnie zanieczyszcza urządzenie, system informatyczny lub sieć, umieszczając na nim lub wysyłając do niego informacje o klasyfikacji, do których obsługi nie został upoważniony. Informacje te są narażone na dostęp nieautoryzowanych osób, w wyniku czego urządzenie, system lub sieć są niedostępne podczas badania i ograniczania wycieku.
Niewłaściwe postępowanie z informacjami krytycznymi lub szczególnie chronionymi przez upoważnionych użytkowników.	Upoważniony uprzywilejowany użytkownik nieumyślnie eksponuje krytyczne/wrażliwe informacje.
Nieprawidłowe ustawienia przywilejów.	Upoważniony uprzywilejowany użytkownik lub administrator błędnie przydziela użytkownikowi wyjątkowe uprawnienia lub ustawia zbyt niskie wymagania dotyczące uprawnień na zasobie.
Kolizje w komunikacji.	Zdegradowana wydajność łączności z powodu kolizji.
Nieczytelny wyświetlacz.	Wyświetlacz nieczytelny z powodu starzenia się sprzętu.
Trzęsienie ziemi w obiekcie głównym.	Trzęsienie ziemi w głównym obiekcie, o magnitudzie przekraczającej zakładany stopień, powodującej, że obiekt nie może funkcjonować.

Zdarzenie zagrożenia	Opis
Pożar w obiekcie głównym.	Pożar (niewynikający z działalności przeciwnika) w obiekcie głównym powoduje, że obiekt jest niezdatny do użytku.
Pożar w obiekcie zapasowym.	Pożar (niespowodowany działaniem przeciwnika) w obiekcie kopii zapasowej powoduje, że obiekt nie nadaje się do użytku lub doszło do zniszczenia kopii zapasowych oprogramowania, konfiguracji, danych lub dzienników.
Powódź w obiekcie głównym.	Powódź (niespowodowana działaniem przeciwnika) w głównym obiekcie powoduje, że obiekt jest niezdatny do użytku.
Powódź w obiekcie zapasowym.	Powódź (niespowodowana działaniem przeciwnika) w obiekcie zapasowym powoduje, że obiekt nie nadaje się do użytku lub doszło do zniszczenia kopii zapasowych oprogramowania, konfiguracji, danych lub dzienników.
Huragan w obiekcie głównym.	Huragan w głównym obiekcie, o sile przekraczającej zakładany stopień, powoduje, że obiekt jest niezdatny do użytku.
Huragan w obiekcie zapasowym.	Huragan w obiekcie zapasowym powoduje, że obiekt nie nadaje się do użytku lub doszło do zniszczenia kopii zapasowych oprogramowania, konfiguracji, danych lub dzienników.
Wyczerpanie zasobów.	Zdegradowana wydajność przetwarzania w związku z wyczerpywaniem się zasobów

Zdarzenie zagrożenia	Opis
Wprowadzanie podatności w oprogramowaniu.	Ze względu na występujące niedoskonałości języków programowania i środowisk tworzenia oprogramowania, w sposób niezamierzony do wytwarzanego oprogramowania są wprowadzane błędy i podatności.
Błędy dysków.	Uszkodzenie zawartości pamięć masowej z powodu błędu dysku.
Wielokrotne błędy dysków.	Wielokrotne błędy dyskowe wynikające ze starzenia się zestawu urządzeń nabytych w tym samym czasie od tego samego dostawcy.
Wichura/tornado w obiekcie podstawowym.	Wichura / tornado o sile przekraczającej zakładany stopień w głównym obiekcie sprawia, że obiekt nie nadaje się do użytku.
Wichura/tornado w obiekcie zapasowym.	Wichura / tornado o sile przekraczającej zakładany stopień w obiekcie zapasowym powoduje, że obiekt nie nadaje się do użytku lub doszło do zniszczenia kopii zapasowych oprogramowania, konfiguracji, danych lub dzienników.

Tabela E-12. Znaczenie zdarzeń zagrożeń.

Wartość	Opis
Potwierdzone	Zdarzenie zagrażające lub TTP było obserwowane w podmiocie.
Spodziewane	Zdarzenie zagrażające lub TTP było obserwowane w podobnych podmiotach lub w podmiotach współpracujących
Oczekiwane	Zdarzenie zagrożenia lub TTP zostało zgłoszone przez zaufane źródło.
Przewidywane	Zdarzenie zagrożenia lub TTP zostało zapowiedziane przez zaufane źródło.
Możliwe	Zdarzenie zagrożenia lub TTP zostało opisane przez dość wiarygodne źródło.
Nie dotyczy	Zdarzenie zagrożenia lub TTP nie ma obecnie zastosowania. Na przykład, zdarzenie zagrażające lub TTP może zakładać specyficzne technologie, architektury lub procesy, które nie są obecne w podmiocie, procesie biznesowym, segmencie EA lub systemie informatycznym lub nie zachodzą warunki predysponujące (np. lokalizacja na obszarze zalewowym). Alternatywnie, jeżeli podmiot posiada szczegółową informację o zagrożeniu, zdarzenie zagrożenia lub TTP może być uznane za niemające zastosowania, ponieważ informacja wskazuje, że przeciwnik nie ma zamiaru zainicjowania zdarzenia zagrożenia lub wykorzystania TTP.

Tabela E-13. Szablon – Identyfikacja zdarzeń zagrożeń.

Identyfikator	Źródło informacji o zdarzeniu zagrożenia	Źródło zagrożeń	Znaczenie
Definiowany przez podmiot	Tabela E-2, tabela E-3, zadanie 1-4 lub definiowane przez podmiot	Tabela D-7, tabela D-8 lub definiowane przez podmiot	Tabela E-4 lub definiowane przez podmiot

ZAŁĄCZNIK F PODATNOŚCI I PREDYSPOZYCJE

Czynniki ryzyka wpływające na prawdopodobieństwo skutecznej eksploatacji zagrożeń

Niniejszy załącznik stanowi: (i) opis potencjalnie użytecznych danych wejściowych do zadania identyfikacji podatności na zagrożenia i stanów predysponujących; (ii) przykładową taksonomię stanów predysponujących; (iii) przykładowe skale oceny ciężaru podatności na zagrożenia oraz powszechności występowania stanów predysponujących; oraz (iv) zestaw szablonów do podsumowania i udokumentowania wyników zadania identyfikacji podatności na zagrożenia i stanów predysponujących. Skale taksonomii i oceny zawarte w niniejszym załączniku mogą być, przy odpowiednim dostosowaniu, wykorzystywane przez podmiot, jako punkt wyjścia do wszelkich specyficznych dla organizacji warunków. Tabele F-3 i F-6, stanowiące wyniki zadania 2-3, dostarczają odpowiednich danych wejściowych do tabel ryzyka w załączniku I.

Tabela F-14. Wejścia – podatności i warunki predestynujące.

Opis	Warunek		
	poziom 1	poziom 2	poziom 3
Z poziomu 1: (poziom organizacji) • Źródła informacji o podatnościach uznane za wiarygodne (np. otwarte źródła i/lub niejawne podatności, wcześniejsze oceny ryzyka/podatności, analizy celu i/lub analizy wpływu na działalność). (sekcja 3.1, zadanie 1-4). • Informacje i wytyczne dotyczące podatności na zagrożenia specyficzne dla Poziomu 1 (np. podatności związane z zarządzaniem podmiotem, podstawowymi zadaniami/funkcjami biznesowymi, polityką, procedurami i strukturami zarządzania/operacji, zewnętrznymi zadaniami/stosunkami biznesowymi). • Taksonomia warunków predysponujących, w razie potrzeby opatrzona adnotacjami przez podmiot. (Tabela F-4) • Charakterystyka podatności i warunków predysponujących. • Skala oceny stopnia nasilenia podatności, w razie potrzeby opatrzona adnotacją podmiotu. (Tabela F-2)	Nie	Tak	Tak *o ile nie są uwzględnione na poziomie 2*

Opis	Warunek		
	poziom 1	poziom 2	poziom 3
• Skala oceny wszechobecności warunków predysponujących, w razie potrzeby opatrzona adnotacjami przez podmiot. (Tabela F-5) • Plan Ciągłości Działania, Plan Ciągłości Operacji dla podmiotu, jeżeli plany te są określone dla całego podmiotu.			
Z poziomu 2: (poziom procesu biznesowego) • Informacje i wskazówki dotyczące podatności na zagrożenia specyficzne dla poziomu 2 (np. podatności związane z zadaniami podmiotu/procesami biznesowymi, segmentami EA, wspólną infrastrukturą, usługami wsparcia, zabezpieczeniami wspólnymi i zależnościami zewnętrznymi). • Plany Ciągłości Działania, Plany Ciągłości Operacji dla procesów związanych z zadaniami/procesami biznesowymi, jeśli takie plany są zdefiniowane dla poszczególnych procesów lub jednostek biznesowych.	Tak *poprzez RAR*	Tak *poprzez wzajemne udostępnianie*	Tak

Opis	Warunek		
	poziom 1	poziom 2	poziom 3
Z poziomu 3: (poziom systemu informatycznego) • Informacje i wskazówki dotyczące podatności na zagrożenia specyficzne dla poziomu 3 (np. podatności związane z systemami informatycznymi, technologiami informatycznymi, elementami systemów informatycznych, aplikacjami, sieciami, środowiskami działania). • Sprawozdania z oceny bezpieczeństwa (tj. braki w ocenianych zabezpieczeniach zidentyfikowane, jako podatności). • Wyniki działań w zakresie monitorowania (np. zautomatyzowane i niezautomatyzowane kanały danych). • Oceny podatności, sprawozdania Red Team lub inne sprawozdania z analiz systemów informatycznych, podsystemów, produktów informatycznych, urządzeń, sieci lub aplikacji. • Plany awaryjne, plany przywrócenia gotowości do pracy po katastrofie, raporty o zdarzeniach. • Raporty sprzedawcy/producenta dotyczące podatności.	Tak *poprzez RAR*	Tak *poprzez RAR*	Tak *poprzez wzajemne udostępnianie*

Tabela F-15. Skale szacowania – dotkliwość podatności.

Wartości jakościowe	Wartości mieszane		Opis
Bardzo wysoki	96-100	10	Podatność na zagrożenia jest odsłonięta i możliwa do wykorzystania, a jej wykorzystanie może mieć poważne skutki. Nie wdrożono i nie zaplanowano odpowiednich zabezpieczeń lub innych środków naprawczych; nie można też zidentyfikować żadnych środków bezpieczeństwa, które pozwoliłyby usunąć podatność na zagrożenia.
Wysoki	80-95	8	Podatność, z uwagi na stopień narażenia na zagrożenia i łatwość eksploatacji i/lub dotkliwość oddziaływań, które mogą wynikać z jej eksploatacji, jest wysoce niepokojąca. Planowane są odpowiednie zabezpieczenia lub inne środki zaradcze, ale nie są one wdrażane; istnieją zabezpieczenia wyrównawcze i są co najmniej minimalnie skuteczne.

Wartości jakościowe	Wartości mieszane		Opis
Umiarkowany	21-79	5	Podatność na zagrożenia jest umiarkowana i wynika z łatwości eksploatacji i/lub z powagi oddziaływań, które mogą wynikać z jej eksploatacji. Odpowiednie zabezpieczenia lub inne środki zaradcze są częściowo wdrożone i w pewnym stopniu skuteczne.
Niski	5-20	2	Podatność na zagrożenia jest niewielka, ale skuteczność środków zaradczych mogłaby zostać zwiększona. Odpowiednie zabezpieczenia lub inne środki zaradcze są w pełni wdrożone i dość skuteczne.
Bardzo niski	0-4	0	Podatność nie budzi obaw. Odpowiednie zabezpieczenia lub inne środki zaradcze są w pełni wdrożone, ocenione i skuteczne.

Tabela F-16. Szablon – Identyfikacja podatności.

Identyfikator	Źródło informacji o podatności	Istotność
Definiowany przez podmiot	Zadanie 2-3, zadanie 1-4 lub definiowane przez podmiot	Tabela F2 lub definiowane przez podmiot

Tabela F-17. Taksonomia warunków predysponujących.

Rodzaj warunków predyspozycji	Opis
Powiązanie z informacjami • Informacje niejawne dotyczące bezpieczeństwa narodowego; • Tajemnice prawnie chronione; • Dane osobowe; • Specjalne programy dostępu; • Porozumienie – ustalone na podstawie: ➢ urzędowej klasyfikacji informacji; ➢ własności.	Potrzeby przetwarzania informacji (w miarę ich tworzenia, przesyłania, przechowywania, przetwarzania i/lub wyświetlania) w określony sposób, ze względu na ich wrażliwość (lub brak wrażliwości), wymogi prawne lub regulacyjne i/lub umowy lub inne porozumienia pomiędzy podmiotami.
Techniczne • Architektoniczne: ➢ zgodność z normami technicznymi; ➢ korzystanie z określonych produktów lub linii produktów; ➢ rozwiązania i/lub podejścia do współpracy z użytkownikami i wymiany informacji; ➢ przypisanie konkretnych funkcji bezpieczeństwa do zabezpieczeń wspólnych; • Funkcjonalne systemu: ➢ Sieciowy; ➢ pojedynczy użytkownik;	

➢ samodzielny / niepodłączony do sieci; ➢ ograniczona funkcjonalność (np. komunikacja, czujniki, sterowniki wbudowane).	
Operacyjne / środowiskowe • Mobilność: ➢ stacjonarne; ➢ pokładowe (lądowe, lotnicze, morskie kosmiczne); ➢ mobilne (np. smartfony); • Ilość użytkowników z fizycznym i/lub logicznym dostępem do komponentów systemu informatycznego, procesu biznesowego, segmentu EA: ➢ ilość użytkowników; ➢ upoważnianie/rozliczanie użytkowników.	

Tabela F-18. Skale szacowania – Rozpowszechnienie warunków predyspozycji.

Wartości jakościowe	Wartości mieszane		Opis
Bardzo wysoki	96-100	10	Stosuje się do **wszystkich** zadań podmiotu (poziom 1), procesów biznesowych (poziom 2) lub systemów informatycznych (poziom 3).
Wysoki	80-95	8	Stosuje się do **większości** zadań podmiotu (poziom 1), procesów biznesowych (poziom 2) lub systemów informatycznych (poziom 3).
Umiarkowany	21-79	5	Stosuje się do **wielu** zadań podmiotu (poziom 1), procesów biznesowych (poziom 2) lub systemów informatycznych (poziom 3).
Niski	5-20	2	Stosuje się do **niektórych** zadań podmiotu (poziom 1), procesów biznesowych (poziom 2) lub systemów informatycznych (poziom 3).
Bardzo niski	0-4	0	Stosuje się do **niewielu** zadań podmiotu (poziom 1), procesów biznesowych (poziom 2) lub systemów informatycznych (poziom 3).

Tabela F-19. Szablon – Identyfikacja warunków predyspozycji.

Identyfikator	Źródło informacji o warunkach predyspozycji	Rozpowszechnienie warunków
Definiowany przez podmiot	Tabela F-4, zadanie 1-4 lub definiowane przez podmiot	Tabela F5 lub definiowane przez podmiot

ZAŁĄCZNIK G PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZDARZENIA ZAGROŻENIA

Określanie prawdopodobieństwa wystąpienia zdarzeń zagrożeń

Niniejszy załącznik stanowi: (i) opis potencjalnie użytecznych danych wejściowych do zadania ustalania prawdopodobieństwa; oraz (ii) przykładowe skale oceny prawdopodobieństwa zainicjowania/wystąpienia zdarzenia powodującego zagrożenie, prawdopodobieństwa wystąpienia zdarzeń powodujących niekorzystne skutki oraz ogólnego prawdopodobieństwa zainicjowania lub wystąpienia zdarzeń powodujących zagrożenie i wyrządzenia szkód w działalności podmiotu, jego aktywach lub dla osób. Skale oceny w niniejszym załączniku mogą być stosowane przez podmioty, jako punkt wyjścia przy odpowiednim dostosowaniu do warunków specyficznych dla danego podmiotu. Tabele G-2, G-3, G-4 i G-5, dane wyjściowe z zadania 2-4, zawierają odpowiednie dane wejściowe do tabel ryzyka w załączniku I.

Tabela G-20. Wejścia – Określanie prawdopodobieństwa.

Opis	Warunek		
	poziom 1	poziom 2	poziom 3
Z poziomu 1: (poziom organizacji) • Informacje na temat prawdopodobieństwa i wytyczne charakterystyczne dla poziomu 1 (np. informacje na temat prawdopodobieństwa związane z zarządzaniem podmiotem, podstawowymi zadaniami/funkcjami biznesowymi, polityką, procedurami i strukturami zarządzania/operacji, zewnętrznymi stosunkami biznesowymi). • Wskazówki dotyczące poziomów prawdopodobieństwa w całym podmiocie, które nie wymagają dalszego rozważania. • Skala oceny prawdopodobieństwa inicjacji zdarzenia zagrożenia (zdarzenia zagrożenia agresywnego), w razie potrzeby opatrzona adnotacjami przez podmiot. (Tabela G-2) • Skala oceny prawdopodobieństwa wystąpienia zdarzenia zagrożenia (zdarzenia inne niż agresywne), w razie potrzeby z adnotacjami podmiotu. (Tabela G-3) • Skala oceny prawdopodobieństwa wystąpienia zdarzeń zagrażających skutkujących niekorzystnymi skutkami,	Nie	Tak	Tak *o ile nie są uwzględnione na poziomie 2*

Opis	Warunek		
	poziom 1	poziom 2	poziom 3
w razie potrzeby opatrzona adnotacjami przez podmiot. (Tabela G-4) • Skala oceny ogólnego prawdopodobieństwa zainicjowania lub zaistnienia zdarzeń zagrażających i powodujących niekorzystne skutki, w razie potrzeby opatrzona adnotacjami przez podmiot. (Tabela G-5).			
Z poziomu 2: (poziom procesu biznesowego) • Informacje na temat prawdopodobieństwa i wytyczne charakterystyczne dla poziomu 2 (np. informacje na temat prawdopodobieństwa związane z procesami podmiotu, segmenty EA, wspólna infrastruktura, usługi pomocnicze, zabezpieczenia wspólne i zależności zewnętrzne).	Tak *poprzez RAR*	Tak *poprzez wzajemne udostępnianie*	Tak
Z poziomu 3: (poziom systemu informatycznego) • Informacje na temat prawdopodobieństwa i wytyczne charakterystyczne dla poziomu 3 (np. informacje na temat prawdopodobieństwa związane z systemami informatycznymi, technologiami informatycznymi, elementami systemów	Tak *poprzez RAR*	Tak *poprzez RAR*	Tak *poprzez wzajemne udostępnianie*

Opis	Warunek		
	poziom 1	poziom 2	poziom 3
informatycznych, aplikacjami, sieciami, środowiskami działania). • Dane historyczne dotyczące udanych i nieudanych cyberataków; wskaźniki wykrywania ataków. • Sprawozdania z oceny bezpieczeństwa (tj. braki w ocenionych zabezpieczeniach zidentyfikowanych jako podatności). • Wyniki działań w zakresie monitorowania (np. zautomatyzowane i niezautomatyzowane kanały danych). • Oceny podatności, sprawozdania Red Team lub inne sprawozdania z analiz systemów informatycznych, podsystemów, produktów informatycznych, urządzeń, sieci lub aplikacji. • Plany awaryjne, plany przywrócenia gotowości do pracy po katastrofie, raporty o zdarzeniach. • Raporty sprzedawcy/producenta dotyczące podatności.			

Tabela G-21. Skale szacowania – Prawdopodobieństwo wystąpienia zdarzeń zagrożeń (agresywne).

Wartości jakościowe	Wartości mieszane		Opis
Bardzo wysoki	96-100	10	Jest prawie pewne, że przeciwnik zainicjuje zdarzenie zagrożenia.
Wysoki	80-95	8	Jest bardzo prawdopodobne, że przeciwnik zainicjuje zdarzenie zagrożenia.
Umiarkowany	21-79	5	Przeciwnik jest w pewnym stopniu skłonny zainicjować zdarzenie zagrożenia.
Niski	5-20	2	Jest mało prawdopodobne, aby przeciwnik zainicjował zdarzenie zagrożenia.
Bardzo niski	0-4	0	Jest bardzo mało prawdopodobne, aby przeciwnik zainicjował zdarzenie zagrożenia.

Tabela G-22. Skale szacowania – Prawdopodobieństwo wystąpienia zdarzeń zagrożeń (inne niż agresywne).

Wartości jakościowe	Wartości mieszane		Opis
Bardzo wysoki	96-100	10	Błąd, wypadek lub działanie sił natury **jest prawie pewne** lub występuje ponad 100 razy w roku.
Wysoki	80-95	8	Błąd, wypadek lub działanie sił natury są **wysoce prawdopodobne** lub występuje między 10-100 razy w roku.
Umiarkowany	21-79	5	Błąd, wypadek lub działanie sił natury jest **w pewnym stopniu prawdopodobne** lub występuje od 1-10 razy w roku.
Niski	5-20	2	Błąd, wypadek lub działanie sił natury jest **mało prawdopodobne** lub występuje rzadziej niż raz w roku, ale częściej niż raz na 10 lat.
Bardzo niski	0-4	0	Wystąpienie błędu, wypadku lub zjawiska naturalnego jest **bardzo mało prawdopodobne** lub występuje rzadziej niż raz na 10 lat.

Tabela G-23. Skala szacowania – Prawdopodobieństwo spowodowania szkody przez zdarzenie zagrożenia.

Wartości jakościowe	Wartości mieszane		Opis
Bardzo wysoki	96-100	10	Jeśli zdarzenie zagrożenia zostanie zainicjowane lub wystąpi, jest **prawie pewne**, że będzie miało negatywne skutki.
Wysoki	80-95	8	Jeśli zdarzenie zagrożenia zostanie zainicjowane lub wystąpi, istnieje **duże prawdopodobieństwo**, że będzie ono miało negatywne skutki.
Umiarkowany	21-79	5	Jeśli zdarzenie zagrożenia zostanie zainicjowane lub wystąpi, istnieje **pewne prawdopodobieństwo**, że będzie ono miało negatywne skutki.
Niski	5-20	2	Jeśli zdarzenie zagrożenia zostanie zainicjowane lub wystąpi, jest **mało prawdopodobne**, aby miało ono negatywne skutki.
Bardzo niski	0-4	0	Jeśli zdarzenie zagrożenia zostanie zainicjowane lub wystąpi, jest **bardzo mało prawdopodobne**, aby miało ono negatywne skutki.

Tabela G-24. Skala szacowania – Prawdopodobieństwo całkowite.

Prawdopodobieństwo inicjacji lub wystąpienia zdarzenia zagrożenia	Prawdopodobieństwo szkodliwego wpływu zdarzenia zagrożenia				
	Bardzo niskie	**Niskie**	**Umiarkowane**	**Wysokie**	**Bardzo wysokie**
Bardzo wysokie	Niskie	Umiarkowane	Wysokie	Bardzo wysokie	Bardzo wysokie
Wysokie	Niskie	Umiarkowane	Umiarkowane	Wysokie	Bardzo wysokie
Umiarkowane	Niskie	Niskie	Umiarkowane	Umiarkowane	Wysokie
Niskie	Bardzo niskie	Niskie	Niskie	Umiarkowane	Umiarkowane
Bardzo Niskie	Bardzo niskie	Bardzo niskie	Niskie	Niskie	Niskie

ZAŁĄCZNIK H WPŁYW NA ORGANIZACJĘ

Skutki zdarzenia zagrożenia

Niniejszy załącznik zawiera: (i) opis użytecznych danych wejściowych do realizacji zadania polegającego na określeniu wpływu; (ii) reprezentatywne przykłady negatywnych skutków dla działalności podmiotu i jego aktywów, osób, innych podmiotów lub Państwa; (iii) przykładowe skale oceny wpływu zdarzeń zagrożenia i zakresu skutków zdarzeń zagrożenia; oraz (iv) wzór do podsumowania i udokumentowania wyników zadania 2-5 polegającego na określeniu wpływu. Skale oceny w niniejszym załączniku można wykorzystać, jako punkt wyjścia przy odpowiednim dostosowaniu do wszelkich warunków specyficznych dla danego podmiotu. W tabeli H-4, stanowiącej wynik zadania 2-5, przedstawiono odpowiednie dane wejściowe do tabel ryzyka w załączniku I.

Tabela H-25. Wejścia – Określanie wpływu.

Opis	Warunek		
	poziom 1	poziom 2	poziom 3
Z poziomu 1: (poziom organizacji) • Informacje o wpływie i wytyczne specyficzne dla poziomu 1 (np. informacje o wpływie związane z zarządzaniem podmiotem, podstawowymi zadaniami/funkcjami biznesowymi, polityką, procedurami i strukturami zarządzania i operacyjnymi, zewnętrznymi celami/stosunkami biznesowymi). • Wskazówki dotyczące poziomów wpływu w całym podmiocie, które nie wymagają dalszego rozważania. • Identyfikacja krytycznych zadań/funkcji biznesowych. • Przykładowy zestaw oddziaływań, w razie potrzeby opatrzony adnotacją przez podmiot. (Tabela H-2) • Skala oceny wpływu zdarzeń zagrożeń, w razie potrzeby opatrzona adnotacją podmiotu. (Tabela H-3)	Nie	Tak	Tak *o ile nie są uwzględnione na poziomie 2*

Opis	Warunek		
	poziom 1	poziom 2	poziom 3
Z poziomu 2: (poziom procesu biznesowego) • Informacje i wytyczne dotyczące wpływu charakterystyczne dla poziomu 2 (np. informacje dotyczące wpływu związane z procesami podmiotu, segmentami EA, wspólną infrastrukturą, usługami wsparcia, zabezpieczeniami wspólnymi i zależnościami zewnętrznymi). • Identyfikacja aktywów o wysokiej wartości.	Tak *poprzez RAR*	Tak *poprzez wzajemne udostępnianie*	Tak
Z poziomu 3: (poziom systemu informatycznego) • Informacje o wpływie i wskazówki dotyczące wpływu charakterystyczne dla poziomu 3 (np. informacje o prawdopodobieństwie wpływu na systemy informatyczne, technologie informatyczne, elementy systemów informatycznych, aplikacje, sieci, środowiska działania). • Dane historyczne dotyczące udanych i nieudanych cyberataków, wskaźniki wykrywania ataków. • Sprawozdania z oceny bezpieczeństwa (np. braki w ocenionych zabezpieczeniach zidentyfikowanych jako podatności).	Tak *poprzez RAR*	Tak *poprzez RAR*	Tak *poprzez wzajemne udostępnianie*

Opis	Warunek		
	poziom 1	poziom 2	poziom 3
• Wyniki działań w zakresie ciągłego monitorowania (np. zautomatyzowane i niezautomatyzowane kanały danych). • Oceny podatności, sprawozdania Red Team lub inne sprawozdania z analiz systemów informatycznych, podsystemów, produktów informatycznych, urządzeń, sieci lub aplikacji. • Plany awaryjne, plany przywrócenia gotowości do pracy po katastrofie, raporty o zdarzeniach.			

Tabela H-26. Przykłady negatywnych skutków.

Rodzaj wpływu	Wpływ
Zakłócenie operacji	• Niezdolność do wykonywania bieżących celów/funkcji biznesowych: ➢ w odpowiednim czasie; ➢ z dostateczną pewnością siebie i/lub poprawnością; ➢ w ramach planowanych ograniczeń zasobów. • Niezdolność lub ograniczona zdolność do wykonywania celów/funkcji biznesowych w przyszłości: ➢ niezdolność do przywrócenia celów/funkcji biznesowych; ➢ w odpowiednim czasie; ➢ z dostateczną pewnością siebie i/lub poprawnością; ➢ w ramach zaplanowanych ograniczeń zasobów. • Szkody (np. koszty finansowe, sankcje) wynikające z nieprzestrzegania przepisów: ➢ z obowiązującymi przepisami prawa; ➢ z wymogami umownymi lub innymi wymogami zawartymi w innych wiążących umowach (np. dotyczących odpowiedzialności). • Bezpośrednie koszty finansowe; • Szkody o charakterze relacyjnym: ➢ szkody w relacjach zaufania; ➢ naruszenie wizerunku lub reputacji (a tym samym przyszłych lub potencjalnych relacji opartych na zaufaniu).

Rodzaj wpływu	Wpływ
Uszkodzenie zasobów	• Uszkodzenie lub utrata obiektów fizycznych; • Uszkodzenie lub utrata systemów informatycznych lub sieci; • Uszkodzenie lub utrata technologii informatycznej lub sprzętu; • Uszkodzenie lub utrata części składowych lub materiałów eksploatacyjnych; • Uszkodzenie lub utrata aktywów informacyjnych; • Utrata własności intelektualnej.
Oddziaływanie na ludzi	• Urazy lub utrata życia; • Złe traktowanie fizyczne lub psychiczne; • Kradzież tożsamości; • Utrata informacji umożliwiających identyfikację osobistą; • Uszkodzenie wizerunku lub reputacji.
Szkody w innych podmiotach	• Szkody (np. koszty finansowe, sankcje) wynikające z nieprzestrzegania: ➢ obowiązujących przepisów prawa, ➢ wymogów umów lub innymi wymogami zawartymi w innych wiążących umowach; • Bezpośrednie koszty finansowe; • Szkody o charakterze relacyjnym: ➢ szkody w relacjach opartych na zaufaniu; ➢ utrata reputacji (a tym samym przyszłych lub potencjalnych relacji opartych na zaufaniu).

Rodzaj wpływu	Wpływ
Szkoda dla Państwa	• Uszkodzenie lub obezwładnienie sektora infrastruktury krytycznej; • Utrata ciągłości działania rządu; • Szkody o charakterze relacyjnym: ➢ utrata zaufania w relacjach z innymi rządami lub z podmiotami pozarządowymi; ➢ uszkodzenie reputacji kraju (a tym samym przyszłych lub potencjalnych relacji opartych na zaufaniu). • Uszkodzenie obecnej lub przyszłej zdolności do osiągania celów krajowych: ➢ Szkoda dla bezpieczeństwa narodowego.

Tabela H-27. Skala szacowania – Wpływ zdarzeń zagrożeń.

Wartości jakościowe	Wartości mieszane		Opis
Bardzo wysoki	96-100	10	Można oczekiwać, że zdarzenie zagrażające będzie miało **wiele poważnych lub katastrofalnie negatywnych** skutków dla działalności podmiotu, jej zasobów, osób, innych organizacji lub Państwa.
Wysoki	80-95	8	Można oczekiwać, że zdarzenie zagrażające będzie miało **poważny lub katastrofalnie negatywny** wpływ na działalność podmiotu, jego aktywa, osoby fizyczne, inne organizacje lub społeczeństwo. Poważny lub katastrofalny szkodliwy skutek oznacza, że na przykład może: (i) spowodować poważną degradację lub utratę zdolności do wypełniania zadań w zakresie i przez czas trwania, w którym podmiot nie jest w stanie wykonywać jednej lub więcej ze swoich podstawowych funkcji; (ii) spowodować poważne szkody w aktywach podmiotu; (iii) spowodować poważne straty finansowe; lub (iv) spowodować poważne lub katastrofalne szkody dla osób obejmujące utratę życia lub poważne obrażenia zagrażające życiu.

Wartości jakościowe	Wartości mieszane		Opis
Umiarkowany	21-79	5	Można oczekiwać, że zdarzenie zagrażające będzie miało **poważny**, negatywny wpływ na działalność podmiotu, jego aktywa, osoby prywatne, inne podmioty lub społeczeństwo. Poważny niekorzystny wpływ oznacza, że na przykład zdarzenie zagrażające może mieć: (i) spowodować znaczne pogorszenie zdolności do wykonywania zadań w zakresie i przez czas trwania, w jakim podmiot jest w stanie wykonywać swoje podstawowe funkcje, ale skuteczność tych funkcji jest znacznie ograniczona; (ii) spowodować znaczne szkody w aktywach podmiotu; (iii) spowodować znaczne straty finansowe; lub (iv) spowodować znaczne szkody dla osób, które nie powodują utraty życia lub poważnych obrażeń ciała zagrażających życiu.
Niski	5-20	2	Można oczekiwać, że zdarzenie zagrażające będzie miało **ograniczony** negatywny wpływ na działalność podmiotu, jego aktywa, osoby fizyczne, inne organizacje lub społeczeństwo. Ograniczony niekorzystny wpływ oznacza, że na przykład zdarzenie

Wartości jakościowe	Wartości mieszane		Opis
			zagrażające może mieć miejsce: (i) spowodować pogorszenie zdolności do wykonywania zadań w takim stopniu i na taki okres, że podmiot jest w stanie wykonywać swoje podstawowe funkcje, ale skuteczność tych funkcji jest wyraźnie ograniczona; (ii) spowodować niewielkie szkody w aktywach podmiotu; (iii) spowodować niewielkie straty finansowe; lub (iv) spowodować niewielkie szkody dla osób fizycznych.
Bardzo niski	0-4	0	Można oczekiwać, że zdarzenie zagrażające będzie miało **znikomy** negatywny wpływ na działalność podmiotu, jego aktywa, osoby prywatne, inne podmioty lub społeczeństwo.

Tabela H-28. Szablon – Identyfikacja niekorzystnych skutków.

Identyfikator	Oddziaływanie skutków na zasoby	Maksymalny wpływ
Definiowany przez podmiot	Tabela H2 lub definiowane przez podmiot	Tabela H3 lub definiowane przez podmiot

ZAŁĄCZNIK I OKREŚLANIE RYZYKA

Szacowanie ryzyka dla podmiotu, osób fizycznych i Państwa

Niniejszy załącznik zawiera: (i) opis potencjalnie użytecznych danych wejściowych do zadania określania ryzyka, w tym rozważania dotyczące niepewności ustaleń; (ii) przykładowe skale oceny służące do oceny poziomu ryzyka; (iii) tabele opisujące zawartość (tj. dane wejściowe) dla ustalania ryzyka dla zdarzeń agresywnych i nieagresywnych; oraz (iv) szablony do podsumowania i udokumentowania wyników określania ryzyka zadanie 2-6. Skale oceny w niniejszym załączniku mogą być wykorzystywane, jako punkt wyjścia przy odpowiednim dostosowaniu do wszelkich warunków specyficznych dla danego podmiotu. Tabela I-5 (ryzyko agresywne) i tabela I-7 (ryzyko nieagresywne) są wynikami zadania 2-6.

Tabela I-29. Wejścia – Ryzyko.

Opis	Warunek		
	poziom 1	poziom 2	poziom 3
Z poziomu 1: (poziom organizacji) • Źródła informacji o ryzyku i niepewności zidentyfikowane na użytek całego podmiotu (np. konkretne informacje, które mogą być przydatne do określenia prawdopodobieństwa, takie jak zdolności, zamiary i cele przeciwnika). • Wytyczne dotyczące poziomów ryzyka w skali całego podmiotu (w tym niepewności), które nie wymagają dalszego rozważania. • Kryteria określania niepewności. • Lista zdarzeń wysokiego ryzyka z poprzednich szacowań ryzyka. • Skala szacowania poziomu ryzyka, jako kombinacji prawdopodobieństwa i wpływu, w razie potrzeby opatrzona adnotacjami przez podmiot. (Tabela I-2) • Skala szacowania poziomu ryzyka, w razie potrzeby opatrzona adnotacjami przez podmiot. (Tabela I-3)	Nie	Tak	Tak *o ile nie są uwzględnione na poziomie 2*

Opis	Warunek		
	poziom 1	poziom 2	poziom 3
Z poziomu 2: (poziom procesu biznesowego) • Informacje i wytyczne dotyczące ryzyka specyficzne dla poziomu 2 (np. informacje dotyczące ryzyka i niepewności związane z procesami podmiotu, segmenty EA, wspólna infrastruktura, usługi pomocnicze, zabezpieczenia wspólne i zależności zewnętrzne).	Tak *poprzez RAR*	Tak *poprzez wzajemne udostępnianie*	Tak
Z poziomu 3: (poziom systemu informatycznego) Informacje i wskazówki dotyczące ryzyka specyficzne dla poziomu 3 (np. informacje o prawdopodobieństwie wpływu na systemy informatyczne, technologie informatyczne, elementy systemów informatycznych, aplikacje, sieci, środowiska działania).	Tak *poprzez RAR*	Tak *poprzez RAR*	Tak *poprzez wzajemne udostępnianie*

Tabela I-30. Skala szacowania – poziom ryzyka (kombinacja prawdopodobieństwa i wpływu).

Prawdopodobieństwo (zaszło zdarzenie zagrożenia i wywołało negatywny skutek)	**Poziom wpływu**				
	Bardzo niski	**Niski**	**Umiarkowany**	**Wysoki**	**Bardzo wysoki**
Bardzo wysokie	Bardzo niski	Niski	Umiarkowany	Wysoki	Bardzo wysoki
Wysokie	Bardzo niski	Niski	Umiarkowany	Wysoki	Bardzo wysoki
Umiarkowane	Bardzo niski	Niski	Umiarkowane	Umiarkowany	Wysoki
Niskie	Bardzo niski	Niski	Niski	Niski	Umiarkowany
Bardzo Niskie	Bardzo niski	Bardzo niski	Bardzo niski	Niski	Niski

Tabela I-31. Skala szacowania – poziom ryzyka.

Wartości jakościowe	Wartości mieszane		Opis
Bardzo wysoki	96-100	10	**Bardzo wysokie** ryzyko oznacza, że zdarzenie zagrażające może mieć **wiele poważnych lub katastrofalnych** negatywnych skutków dla działalności podmiotu, jego aktywów, osób, innych podmiotów lub Państwa.
Wysoki	80-95	8	**Wysokie ryzyko** oznacza, że można oczekiwać, iż zdarzenie zagrażające będzie **miało poważne lub katastrofalne** negatywne skutki dla działalności podmiotu, jego aktywów, osób, innych podmiotów lub Państwa.
Umiarkowany	21-79	5	**Umiarkowane** ryzyko oznacza, że można oczekiwać, iż zdarzenie zagrażające będzie miało **poważne** negatywne skutki dla działalności podmiotu, jego aktywów, osób, innych podmiotów lub Państwa.
Niski	5-20	2	**Niskie** ryzyko oznacza, że można oczekiwać, iż zdarzenie zagrażające będzie miało **ograniczone** negatywne skutki dla działalności podmiotu, jego aktywów, osób, innych podmiotów lub Państwa.

Wartości jakościowe	Wartości mieszane		Opis
Bardzo niski	0-4	0	**Bardzo niskie** ryzyko oznacza, że można oczekiwać, iż zdarzenie zagrażające będzie miało **znikome** negatywne skutki dla działalności podmiotu, jego aktywów, osób, innych podmiotów lub Państwa.

Tabela I-32. Opisy kolumn dla tabeli ryzyka agresywnego.

Kolumna	Nagłówek	Zawartość
1	Zdarzenie zagrożenia	Identyfikacja zdarzeń zagrożenia (zadanie 2-2; tabela E-1; tabela E-2; tabela E-5; tabela I-5).
2	Źródło zagrożenia	Identyfikacja źródła zagrożenia, które mogłyby zainicjować zdarzenie zagrożenia (zadanie 2-1; tabela D-1; tabela D-2; tabela D-7; tabela I-5).
3	Zdolność	Ocena zdolności źródła zagrożenia (zadanie 2-1; tabela D-3; tabela D-7; tabela I-5).
4	Zamiar	Ocena intencji źródła zagrożenia (zadanie 2-1; tabela D-4; tabela D-7; tabela I-5).
5	Ukierunkowanie	Ocena ukierunkowania źródła zagrożenia (zadanie 2-1; tabela D-5; tabela D-7; tabela I-5).
6	Znaczenie	Ustalenie znaczenia zdarzenia zagrożenia (zadanie 2-2; tabela E-1; tabela E-4; tabela E-5; tabela I-5). Jeżeli istotność zdarzenia zagrażającego nie spełnia kryteriów podmiotu do dalszego rozpatrywania, nie należy wypełniać pozostałych kolumn.
7	Prawdopodobieństwo inicjacji ataku	Ustalenie prawdopodobieństwa, że jedno lub więcej źródeł zagrożenia zainicjuje zdarzenie zagrożenia, biorąc pod uwagę możliwości, zamiary i ukierunkowanie (zadanie 2-4; tabela G-1; tabela G-2; tabela I-5).

Kolumna	Nagłówek	Zawartość
8	Podatności i warunki predyspozycji	Identyfikacja podatności, które mogłyby zostać wykorzystane przez źródła zagrożeń inicjujące zdarzenie zagrożenia, oraz warunków predysponujących, które mogłyby zwiększyć prawdopodobieństwo wystąpienia negatywnych skutków (zadanie 2-5; tabela F-1; tabela F-3; tabela F-4; tabela F-6; tabela I-5).
9	Nasilenie	Ocena nasilenia podatności i wszechobecności warunków predysponujących (zadanie 2-5; tabela F-1; tabela F-2; tabela F-5; tabela F-6; tabela I-5).
10	Prawdopodobieństwo sukcesu ataku	Ustalenie prawdopodobieństwa, że zdarzenie zagrożenia, po jego rozpoczęciu, będzie miało negatywny wpływ, biorąc pod uwagę możliwości źródła zagrożenia, podatności i warunki predysponujące (zadanie 2-4; tabela G-1; tabela G-4; tabela I-5).
11	Prawdopodobieństwo całkowite	Określenie prawdopodobieństwa, że zdarzenie zagrażające zostanie zainicjowane i doprowadzi do negatywnych skutków (tj. połączenie prawdopodobieństwa zainicjowania ataku i prawdopodobieństwa, że zainicjowany atak zakończy się sukcesem) (zadanie 2-4; tabela G-1; tabela G-5; tabela I-5).

Kolumna	Nagłówek	Zawartość
12	Poziom wpływu	Ustalenie niekorzystnego wpływu (tj. potencjalnej szkody dla działalności podmiotu, jego aktywów, osób, innych podmiotów lub Państwa) wynikającego ze zdarzenia zagrożenia (zadanie 2-5; tablica H-1, tablica H-2; tablica H-3; tablica H-4; tablica I-5).
13	Ryzyko	Określenie poziomu ryzyka, jako kombinacji prawdopodobieństwa i wpływu (zadanie 2-6; tabela I-1; tabela I-2; tabela I-3; tabela I-5).

Tabela I-33. Szablon – Ryzyko agresywne.

1	2	3	4	5	6	7	8	9	10	11	12	13
Zdarzenie zagrożenia	Źródło zagrożenia	Charakterystyka źródeł zagrożeń			Znaczenie	Prawdopodobieństwo inicjacji ataku	Podatności i warunki predyspozycji	Nasilenie	Prawdopodobieństwo sukcesu ataku	Prawdopodobieństwo całkowite	Poziom wpływu	Ryzyko
		Zdolność	Zamiar	Ukierunkowanie								

Tabela I-34. Opisy kolumn dla tabeli ryzyka nieagresywnego.

Kolumna	Nagłówek	Zawartość
1	Zdarzenie zagrożenia	Identyfikacja zdarzenia zagrożenia (zadanie 2-2; tabela E-1; tabela E-3; tabela E-5; tabela I-7).
2	Źródło zagrożenia	Identyfikacja źródła zagrożenia, które mogłoby zainicjować zdarzenie zagrożenia (zadanie 2-1; tabela D-1; tabela D-2; tabela D-8; tabela I-7).
3	Zakres skutków	Identyfikacja zakresu skutków od źródła zagrożenia (zadanie 2-1; tabela D-1; tabela D-6; tabela I-7).
4	Znaczenie	Ustalenie znaczenie zdarzenia zagrożenia (zadanie 2-2; tabela E-1; tabela E-4; tabela E-5; tabela I-7). Jeżeli istotność zdarzenia zagrażającego nie spełnia kryteriów podmiotu do dalszego rozpatrzenia, nie należy wypełniać pozostałych kolumn.
5	Prawdopodobieństwo zajścia zdarzenia zagrożenia	Określenie prawdopodobieństwa wystąpienia zdarzenia zagrażającego (zadanie 2-4; tabela G-1; tabela G-3; tabela I-7).
6	Podatności i warunki predyspozycji	Identyfikacja podatności, które mogłyby zostać wykorzystane przez źródła zagrożeń inicjujące zdarzenie zagrożenia, oraz warunków predysponujących, które mogłyby zwiększyć prawdopodobieństwo wystąpienia negatywnych skutków (zadanie 2-5; tabela F-1; tabela F-3; tabela F-4; tabela F-6; tabela I-7).

7	Nasilenie	Ocena nasilenia podatności i wszechobecności warunków predysponujących (zadanie 2-5; tabela F-1; tabela F-2; tabela F-5; tabela F-6; tabela I-5).
8	Prawdopodobieństwo wywołania skutków przez zdarzenie zagrożenia	Ustalenie prawdopodobieństwa, że zdarzenie zagrożenia, po jego rozpoczęciu, będzie miało negatywny wpływ, biorąc pod uwagę słabe punkty i warunki predysponujące (zadanie 2-4; tabela G-1; tabela G-4; tabela I-7).
9	Prawdopodobieństwo całkowite	Ustalenie prawdopodobieństwa wystąpienia zdarzenia zagrożenia i jego negatywnych skutków (tj. połączenie prawdopodobieństwa wystąpienia zagrożenia i prawdopodobieństwa, że zdarzenie zagrożenia spowoduje negatywne skutki) (zadanie 2-4; tabela G-1; tabela G-5; tabela I-7).
10	Poziom wpływu	Ustalenie niekorzystnego wpływu (tj. potencjalnej szkody dla działalności podmiotu, jego aktywów, osób, innych podmiotów lub Państwa) wynikającego ze zdarzenia zagrożenia (zadanie 2-5; tablica H-1, tablica H-2; tablica H-3; tablica H-4; tablica I-7).
11	Ryzyko	Określenie poziomu ryzyka, jako kombinacji prawdopodobieństwa i wpływu (zadanie 2-6; tabela I-1; tabela I-2; tabela I-3; tabela I-7).

Tabela I-35. Szablon – Ryzyko nieagresywne.

1	2	3	4	5	6	7	8	9	10	11
Zdarzenie zagrożenia	Źródło zagrożenia	Zakres skutków	Znaczenie	Prawdopodobieństwo zajścia zdarzenia zagrożenia	Podatności i warunki predyspozycji	Nasilenie	Prawdopodobieństwo wywołania skutków przez zdarzenie zagrożenia	Prawdopodobieństwo całkowite	Poziom wpływu	Ryzyko

ZAŁĄCZNIK J INFORMOWANIE O RYZYKU

Podejście do udoskonalanie wyników szacowania ryzyka

Szacowanie ryzyka może zidentyfikować szereg rodzajów ryzyka, które mają podobne wyniki (np. 78, 82, 83) lub poziomy (np. umiarkowane, wysokie). W przypadku, gdy zbyt wiele ryzyk jest skupionych na tej samej lub zbliżonej wartości, podmioty, aby lepiej informować element reakcji na ryzyko w procesie zarządzania ryzykiem, potrzebują metody doskonalenia prezentacji wyników szacowania ryzyka, uszeregowania priorytetów w ramach zestawów ryzyk o podobnych wartościach. Ustalanie priorytetów jest kluczowym elementem ochrony opartej na ryzyku i staje się konieczne, gdy wymagania nie mogą być w pełni zaspokojone lub gdy zasoby nie pozwalają na ograniczenie wszystkich ryzyk w rozsądnych ramach czasowych. Aby ułatwić podejmowanie świadomych decyzji dotyczących reakcji na ryzyko przez kierowników wyższego szczebla/wykonawców (np. dlaczego niektóre rodzaje ryzyka zostały lub nie zostały złagodzone), wyniki szacowania ryzyka są opatrzone adnotacjami, aby umożliwić tym decydentom poznanie lub uzyskanie odpowiedzi na poniższe pytania dotyczące każdego z rodzajów ryzyka w zestawie o podobnych wynikach:

Ramy czasowe

W przypadku zmaterializowania się zidentyfikowanego ryzyka-

- Jak duży byłby bezpośredni wpływ na działania podmiotu (w tym na zadania, funkcje, wizerunek lub reputację), jego aktywa, osoby, inne podmioty lub Państwo?
- Jak duży byłby przyszły wpływ na działania podmiotu (w tym na zadania, funkcje, wizerunek lub reputację), jego aktywa, osoby, inne podmioty lub Państwo?

Odpowiedzi na powyższe pytania, a także tolerancja podmiotu na ryzyko, stanowią podstawę do ustalenia priorytetów ryzyka w oparciu o obecne i przyszłe potrzeby podmiotu. Rozważając wpływy natychmiastowe i przyszłe, kierownicy wyższego szczebla muszą zdecydować, czy ryzyko już dziś stanowi zagrożenie dla przyszłych możliwości skutecznego działania podmiotu i możliwości realizowania zadań. Właściciele procesów biznesowych oraz eksperci ds. tych procesów powinni być konsultowani w celu uzyskania najbardziej

kompletnych i aktualnych informacji na temat wpływu ryzyka na te procesy. Można też skonsultować się z innymi ekspertami lub przedstawicielami interesariuszy w celu uzyskania informacji na temat natychmiastowych i przyszłych skutków (np. skonsultowanie się z Urzędem Ochrony Danych Osobowych w celu uzyskania informacji na temat skutków dla poszczególnych osób).

Łączny wpływ skumulowany

- Jaki jest oczekiwany wpływ pojedynczego wystąpienia zagrożenia?
- Jeżeli ryzyko może się zmaterializować więcej niż jeden raz, jaki jest oczekiwany wpływ całkowity (tj. skumulowana strata) w okresie, którego dotyczy zagrożenie?

Należy pamiętać, że jednym z aspektów całkowitego wpływu na podmiot jest koszt odtworzenia po utracie poufności, integralności lub dostępności.

Synergie między zagrożeniami

W przypadku zmaterializowania się ryzyka, które jest ściśle związane z wieloma zagrożeniami, prawdopodobne jest, że klaster zagrożeń zmaterializuje się w tym samym lub zbliżonym czasie. Zarządzanie niekorzystnym wpływem jednego z ryzyk może być możliwe; zarządzanie wieloma ryzykami o dużym wpływie, które materializują się w tym samym czasie, może stanowić wyzwanie dla możliwości organizacji i dlatego musi być zarządzane w znacznie większym stopniu. Poniższe pytania dotyczą relacji pomiędzy poszczególnymi rodzajami ryzyka.

Czy zmaterializowanie się danego ryzyka będzie skutkowało:

- Wysokim prawdopodobieństwem lub praktycznie pewnością zmaterializowania się innych zidentyfikowanych ryzyk?
- Wysokim prawdopodobieństwo lub praktycznie pewnością, że inne zidentyfikowane ryzyka nie zmaterializują się?
- Brakiem szczególnego wpływu na zmaterializowanie się innych zidentyfikowanych ryzyk?

Jeżeli ryzyko jest w wysokim stopniu powiązane z innymi ryzykami lub postrzegane, jako mogące doprowadzić do zmaterializowania się innych ryzyk (niezależnie od tego, czy ryzyko jest przyczyną, czy też materializuje się jednocześnie), należy nadać mu wyższy priorytet niż ryzyku, które nie ma szczególnego wpływu na inne ryzyka. Jeżeli zmaterializowanie się ryzyka rzeczywiście zmniejsza prawdopodobieństwo zmaterializowania się innych ryzyk, wówczas uzasadniona jest dalsza analiza w celu określenia, które z ryzyk stają się niższym priorytetem w ograniczaniu ryzyka.

Podsumowując, podmioty mogą odnieść znaczące korzyści dzięki dopracowaniu wyników szacowania ryzyka w ramach przygotowań do etapu reakcji na ryzyko w procesie zarządzania ryzykiem. W trakcie etapu reakcji na ryzyko, który został opisany w publikacji NSC 800-39, podmioty mogą uzyskać znaczące korzyści: (i) analizując różne kierunki działań; (ii) przeprowadzając analizy kosztów i korzyści; (iii) zajmując się kwestiami skalowalności w przypadku wdrożeń na dużą skalę; (iv) badając interakcje/zależności między podejściami do ograniczania ryzyka (np. zależności między zabezpieczeniami); oraz (v) oceniając inne czynniki wpływające na zadania/funkcje biznesowe podmiotu. Ponadto podmioty zajmują się kwestiami kosztów, harmonogramu i wyników związanych z systemami informatycznymi i infrastrukturą informatyczną wspierającą zadania/funkcje biznesowe podmiotu.

NOTATKA OSTRZEGAWCZA

Podmioty są ostrzeżone, że szacowania ryzyka często nie są precyzyjnymi narzędziami pomiaru i posiadają ograniczenia poszczególnych metod, narzędzi i technik oceny, jak również subiektywność odnoszącą się do jakości i wiarygodności wykorzystywanych danych. Określanie ryzyka może być bardzo niedoskonałe ze względu na wybrane podejście do szacowania, niepewność co do prawdopodobieństwa wystąpienia i wartości wpływu oraz potencjalną błędną charakterystykę zagrożeń. Ryzyka, które znajdują się na granicy przedziałów z wykorzystaniem skal zdefiniowanych przez organizację, muszą być ostatecznie przypisane do jednego z przedziałów. Takie ustalenie może mieć istotny wpływ na proces ustalania priorytetów ryzyka. W związku z tym podczas procesu szeregowania ryzyka podmioty powinny uwzględnić tyle informacji, ile jest to możliwe w praktyce, aby zapewnić, że wartości ryzyka są odpowiednio określone (np. bardzo niskie, niskie, umiarkowane, wysokie, bardzo wysokie).

ZAŁĄCZNIK K SPRAWOZDANIA Z SZACOWANIA RYZYKA

Kluczowe elementy informacji

Niniejszy załącznik zawiera podstawowe elementy informacji, które podmioty powinny wykorzystać do przekazywania wyników szacowania ryzyka. Wyniki oceny szacowania ryzyka zapewniają osobom podejmującym decyzje zrozumienie zagrożenia bezpieczeństwa informacji dla operacji i aktywów podmiotu, osób, innych podmiotów lub Państwa, które wynika z działania i użytkowania systemów informatycznych podmiotu oraz środowisk, w których te systemy działają. Zasadnicze elementy informacji w szacowaniu ryzyka można opisać w trzech sekcjach raportu z szacowania ryzyka (lub w dowolnym innym narzędziu wybranym przez podmiot w celu przekazania wyników oceny): (i) streszczenie; (ii) główna część i szczegółowe wyniki szacowania ryzyka; oraz (iii) załączniki uzupełniające.

Streszczenie

- Podanie daty szacowania ryzyka.
- Podsumowanie celu szacowania ryzyka.
- Opis zakresu szacowania ryzyka.
  - ✓ W przypadku szacowania ryzyka na poziomie 1 i 2 należy określić: struktury zarządzania podmiotem lub procesy związane z szacowaniem (np. zarządzanie ryzykiem [funkcja], proces budżetowy, proces akwizycji, proces inżynierii systemów, architektura korporacyjna, architektura bezpieczeństwa informacji, zadania/funkcje organizacyjne, procesy biznesowe, systemy informatyczne wspierające zadania/procesy biznesowe).
  - ✓ W przypadku szacowania ryzyka na poziomie 3, należy określić: nazwę i lokalizację systemu informatycznego, kategoryzację bezpieczeństwa oraz granicę systemu informatycznego (tj. autoryzację).
- Należy określić, czy jest to wstępne czy kolejne szacowanie ryzyka. Jeżeli jest to kolejne szacowanie ryzyka, należy podać okoliczności, które spowodowały aktualizację oraz podać odniesienie do poprzedniego sprawozdania z szacowania ryzyka.

- Należy opisać ogólny poziom ryzyka (np. bardzo niski, niski, umiarkowany, wysoki lub bardzo wysoki).
- Wymień liczbę rodzajów ryzyk zidentyfikowanych dla każdego poziomu ryzyka (np. bardzo niskie, niskie, umiarkowane, wysokie lub bardzo wysokie).

Część główna

- Opisać cel szacowania ryzyka, w tym pytania, na które należy odpowiedzieć w ramach szacowania. Na przykład:
  - ✓ W jaki sposób wykorzystanie konkretnej technologii informatycznej mogłoby potencjalnie zmienić ryzyko dla zadań/funkcji biznesowych podmiotu, gdyby była ona wykorzystywana w systemach informatycznych wspierających te zadania/funkcje biznesowe;
  - ✓ W jaki sposób wyniki szacowania ryzyka mają być wykorzystywane w kontekście RMF (np. wstępne szacowanie ryzyka, które ma być wykorzystywane przy dostosowywaniu podstawowych zabezpieczeń lub do kierowania innymi decyzjami i informowania o nich oraz służy, jako punkt wyjścia dla kolejnych szacowań ryzyka; późniejsza ocena ryzyka w celu uwzględnienia wyników ocen zabezpieczeń i informowania o decyzjach dotyczących zezwoleń; późniejsza ocena ryzyka w celu wsparcia analizy alternatywnych sposobów reagowania na ryzyko; późniejsza ocena ryzyka oparta na monitorowaniu ryzyka w celu określenia nowych zagrożeń lub podatności; późniejsza ocena ryzyka w celu uwzględnienia wiedzy zdobytej w wyniku incydentów lub ataków).
- Identyfikacja założeń i ograniczeń.
- Opis danych wejściowych dotyczących tolerancji ryzyka w ocenie ryzyka (w tym zakres konsekwencji, które należy uwzględnić).
- Określenie i opis modelu ryzyka i podejścia analitycznego; należy podać odniesienie lub dołączyć, jako załącznik identyfikacje czynników ryzyka, skale wartości i algorytmy łączenia wartości.

- Uzasadnienie dla wszelkich decyzji związanych z ryzykiem w trakcie procesu szacowania ryzyka.
- Opis niepewności występujących w procesie szacowania ryzyka oraz wpływ tych niepewności na podejmowane decyzje.
- Jeśli szacowanie ryzyka obejmuje zadania/funkcje podmiotu należy opisać te zadania/funkcje (np. procesy biznesowe wspierające zadania/funkcje, powiązania i zależności pomiędzy powiązanymi zadaniami/funkcjami biznesowymi oraz technologie informatyczne wspierające zadania/funkcje biznesowe).
- Jeśli szacowanie ryzyka obejmuje systemy informacyjne podmiotu, należy opisać te systemy (np. wspierane zadania/funkcje biznesowe, przepływ informacji do/z systemów oraz zależności od innych systemów, usług wspólnych lub wspólnej infrastruktury).
- Podsumowanie wyników szacowania ryzyka (np. za pomocą tabel lub wykresów), w formie umożliwiającej decydentom szybkie zrozumienie ryzyka (np. liczba zdarzeń zagrożenia dla różnych kombinacji prawdopodobieństwa i wpływu, względny udział zdarzeń zagrożenia na różnych poziomach ryzyka).
- Określenie ram czasowych, dla których szacowanie ryzyka jest ważna (tj. ramy czasowe, dla których szacowanie ma służyć jako podstawa decyzji).
- Wykaz ryzyk związanych z zagrożeniami o charakterze agresywnym (zob. tabela F-1).
- Wykaz ryzyk związanych z zagrożeniami o charakterze nieagresywnym (patrz: tabela F-2).

Załączniki

- Lista referencji i źródeł informacji.
- Wykaz osób przeprowadzających szacowanie ryzyka, w tym dane kontaktowe.
- Wykaz szczegółów szacowania ryzyka oraz wszelkich dowodów potwierdzających (np. tabele D-7, D-8, E-5, F-3, F-6, H-4), w zależności od potrzeb, tak aby zrozumieć i umożliwić ponowne wykorzystanie wyników (np. w celu zapewnienia wzajemności, w celu późniejszego szacowania ryzyka albo żeby służył jako wkład do szacowania ryzyka na poziomie 1 i 2).

ZAŁĄCZNIK L PODSUMOWANIE ZADAŃ

Zadania szacowania ryzyka i tabele z tym związane

Tabela L-36. Podsumowanie zadań szacowania ryzyka.

Zadanie	Opis zadania
Krok 1: Przygotowanie do oceny ryzyka	
Zadanie 1-1 Cel identyfikacji Sekcja 3.1	Określenie celu szacowania ryzyka w odniesieniu do informacji, które szacowanie ma dostarczyć oraz decyzji, które szacowanie ma wspierać.
Zadanie 1-2 Zakres identyfikacji Sekcja 3.1	Określenie zakresu szacowania ryzyka pod względem możliwości organizacyjnych, ram czasowych oraz względów architektonicznych/technologicznych.
Zadanie 1-3 Identyfikacja założeń i ograniczeń Sekcja 3.1	Określenie konkretnych założeń i ograniczeń, na podstawie których przeprowadzane jest szacowanie ryzyka.
Zadanie 1-4 identyfikacja źródeł informacji Sekcja 3.1	Określenie źródła informacji opisujących zagrożenia, podatności na zagrożenia i skutki, które należy wykorzystać w szacowaniu ryzyka.

Zadanie	Opis zadania
Zadanie 1-5 Określenie modelu ryzyka i podejścia analitycznego Sekcja 3.1	Określenie modelu ryzyka i podejścia analitycznego, które należy zastosować w szacowaniu ryzyka
Krok 2: Przeprowadzenie oceny ryzyka	
Zadanie 2-1 Identyfikacja źródeł zagrożeń Sekcja 3.2, Załącznik D	Określenie i scharakteryzowanie źródeł zagrożeń, w tym zdolności, zamiarów i cech charakterystycznych dla zagrożeń o charakterze agresywnym oraz zakresu skutków dla zagrożeń o charakterze innym niż agresywny.
Zadanie 2-2 Identyfikacja zdarzeń zagrożeń Sekcja 3.2, Załącznik E	Identyfikacja zdarzeń potencjalnego zagrożenia, znaczenie zdarzeń oraz źródeł zagrożeń, które mogą być inicjatorami tych zdarzeń.
Zadanie 2-3 Identyfikacja podatności i warunków predysponujących Sekcja 3.2, Załącznik F	Identyfikacja podatności i predyspozycji, które mają wpływ na prawdopodobieństwo, że zdarzenie budzi obawy spowodowania niekorzystnych skutków.

Zadanie	Opis zadania
Zadanie 2-4 Określanie prawdopodobieństwa Sekcja 3.2, Załącznik G	Ustalenie prawdopodobieństwa, że zdarzenia zagrożenia mogą mieć negatywne skutki, biorąc pod uwagę: (i) charakterystykę źródeł zagrożeń, które mogą być przyczyną tych zdarzeń; (ii) stwierdzoną podatność na zagrożenia/stanu zagrożenia; oraz (iii) organizacyjną podatność odzwierciedlającą planowane lub wdrożone środki ochronne/przeciwdziałające mające na celu utrudnienie wystąpienia takich zdarzeń.
Zadanie 2-5 Określenie wpływu Sekcja 3.2, Załącznik H	Określenie negatywnego wpływu zdarzeń zagrażających, biorąc pod uwagę: (i) charakterystykę źródeł zagrożeń, które mogą być przyczyną tych zdarzeń; (ii) zidentyfikowane podatności/warunki narażenia; oraz (iii) organizacyjną podatność odzwierciedlającą planowane lub wdrożone środki ochronne/przeciwdziałające mające na celu powstrzymanie takich zdarzeń.
Zadanie 2-6 Określanie ryzyka Sekcja 3.2, Załącznik I	Określanie ryzyka dla podmiotu wynikającego z uwzględnienia zdarzeń zagrażających bezpieczeństwu: (i) wpływ, który wynikałby z tych zdarzeń; oraz (ii) prawdopodobieństwo wystąpienia tych zdarzeń.
Krok 3: Przekazanie i udostępnienie wyników szacowania ryzyka	
Zadanie 3-1 Przekazywanie wyników szacowania ryzyka Sekcja 3.3, Załącznik K	Przekazywanie wyników szacowania ryzyka decydentom podmiotu w celu wsparcia reakcji na ryzyko.

Zadanie	Opis zadania
Zadanie 3-2 Dzielenie się informacjami związanymi z ryzykiem Sekcja 3.3	Dzielenie się informacjami na temat ryzyka opracowanymi w trakcie szacowania ryzyka z odpowiednim personelem podmiotu.
Krok 4: Utrzymanie oceny ryzyka	
Zadanie 4-1 Monitorowanie czynników ryzyka Sekcja 3.4	Prowadzenie bieżącego monitoringu czynników ryzyka, które przyczyniają się do zmian w zakresie ryzyka dla działalności i aktywów podmiotu, osób, innych podmiotów lub Państwa.
Zadanie 4-2 Aktualizacja szacowania ryzyka Sekcja 3.4	Aktualizacja istniejącego szacowania ryzyka z wykorzystaniem wyników bieżącego monitorowania czynników ryzyka.