Ministerstwo Cyfryzacji

NARODOWY STANDARD CYBERBEZPIECZEŃSTWA
NSC 800-100 wer. 1.0

4 sierpnia 2023

Podręcznik bezpieczeństwa informacji

Przewodnik dla zarządzających

Publikacja dostępna pod adresem:

Narodowe Standardy Cyberbezpieczeństwa

PREAMBUŁA

Szanowni Państwo,

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

Standardy stanowią przewodniki metodyczne, które ułatwiają zbudowanie efektywnego systemu zarządzania bezpieczeństwem informacji w oparciu o praktykę stosowaną w tym zakresie w administracji federalnej USA.
Niniejsza publikacja NSC 800-100, ***Podręcznik bezpieczeństwa informacji. Przewodnik dla zarządzających***, opracowana została za zgodą National Institute of Science and Technology (NIST) na podstawie specjalnej publikacji NIST SP 800-100 rev. 1, *Information Security Handbook: A Guide for Managers*.

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

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

W publikacji posłużono się pojęciami zdefiniowanymi w poradniku źródłowym, na podstawie którego powstały niniejsze zalecenia. W przypadku, gdy tożsame pojęcia zostały zdefiniowane również w powszechnie obowiązujących aktach prawnych lub normatywnych, a ich definicja różni się od tej zamieszczonej w niniejszej publikacji, wówczas należy stosować sformułowania zawarte w tych aktach / w obiegu prawnym.

Podmioty, urządzenia lub materiały o charakterze komercyjnym prezentowane są w niniejszym dokumencie w celu odpowiedniego opisania procedury lub koncepcji eksperymentalnej. Celem ich wskazania nie jest nakłanianie do korzystania z ww. podmiotów, urządzeń lub materiałów lub ich poparcie. Wskazanie ich nie ma również na celu sugerowania, że te podmioty, materiały lub sprzęt są najlepsze z dostępnych w danej dziedzinie.

WSPÓLNE FUNDAMENTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

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

NIST kontynuuje współpracę z sektorem publicznym i prywatnym w celu stworzenia map i relacji pomiędzy opracowanymi przez siebie standardami i wytycznymi, a tymi, które zostały opracowane przez inne organizacje (m. in. ISO[1]), co zapewnia zgodność w przypadku, gdy regulacje wymagają stosowania tych innych standardów.

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

Biorąc pod uwagę wszystkie powyższe aspekty, autorzy niniejszej publikacji polecają opracowania NIST, jako godne zaufania i rekomendują stosowanie ich przez polskie

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

podmioty przy opracowywaniu systemów zarządzania bezpieczeństwem informacji, wdrażaniu zabezpieczeń i ocenie ich działania.

W niniejszej publikacji mogą znajdować się odniesienia do innych opracowywanych przez nas publikacji. Informacje tu zawarte, w tym koncepcje, praktyki i metodologie, mogą być wykorzystywane przez organizacje jeszcze przed ukończeniem innych towarzyszących temu standardowi publikacji. W związku z tym, do czasu ukończenia każdej publikacji powinny obowiązywać dotychczasowe wymagania, wytyczne i procedury, jeśli takie istnieją. W ramach planowanych przez Państwa prac zalecamy śledzenie naszych prac publikacyjnych.

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

 Narodowe Standardy Cyberbezpieczeństwa

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

 +48222455922

 sekretariat.dc@cyfra.gov.pl

Sprawozdania dotyczące technologii systemów informacyjnych

Laboratorium Technologii Informacyjnych (*ang. Information Technology Laboratory – ITL*) przy Narodowym Instytucie Standaryzacji i Technologii (*ang. National Institute of Standards and Technology – NIST*) działa na rzecz gospodarki USA i dobra publicznego poprzez zapewnienie technicznego wsparcia krajowej infrastruktury pomiarowej i normalizacyjnej. ITL opracowuje testy, metody testowe, dane referencyjne, weryfikacje koncepcji (*ang. proof of concept*) oraz analizy techniczne mające na celu rozwój i produktywne wykorzystanie technologii informacyjnych. Zakres zadań ITL obejmuje opracowywanie norm i rekomendacji w zakresie zarządzania, administracji, a także aspektów technicznych i fizycznych w celu zapewnienia bezpieczeństwa i prywatności informacji innych niż związane z bezpieczeństwem narodowym w federalnych systemach informacyjnych przy zachowaniu efektywności kosztowej. Niniejsza publikacja specjalna oznaczona numerem 800 zawiera sprawozdanie dotyczące badań, rekomendacji oraz działań ITL w zakresie komunikacji, bezpieczeństwa systemów informacyjnych oraz o współpracy z przemysłem, jednostkami rządowymi oraz organizacjami akademickimi.

Spis treści

Spis ilustracji

Spis tabel

ROZDZIAŁ 1

1. WSTĘP

Niniejszy *Podręcznik bezpieczeństwa informacji* prezentuje szeroki przegląd elementów programu bezpieczeństwa informacji, którego celem jest pomoc zarządzającym w zrozumieniu tego, jak taki program należy ustanowić i wdrożyć. Organizacje zazwyczaj oczekują od programu wskazania ogólnej odpowiedzialności w zakresie zapewnienia doboru i wdrożenia odpowiednich środków bezpieczeństwa oraz wykazania skutecznego spełnienia ustalonych przez siebie wymagań bezpieczeństwa. Do treści niniejszego podręcznika można się odwoływać w celu podania ogólnych informacji dotyczących danego zagadnienia. Można też je wykorzystać w procesie podejmowania decyzji podczas opracowywania programu bezpieczeństwa informacji. Słownik podstawowych pojęć z zakresu bezpieczeństwa użytych w niniejszym dokumencie znajduje w publikacji NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*. Czytając niniejszy podręcznik należy pamiętać, że zawarte w nim wytyczne nie dotyczą konkretnej organizacji. Dlatego organizacje powinny dostosować je do stanu swojego bezpieczeństwa i wymagań dotyczących prowadzonej działalności.

1.1. CEL I ZASTOSOWANIE

Celem niniejszej publikacji jest poinformowanie personel zarządzający bezpieczeństwem informacji (tj. kierowników jednostek organizacyjnych, osób odpowiedzialnych za technologie informacyjne [*ang. Chief Information Officer- CIO*], kluczowych osób odpowiedzialnych za bezpieczeństwo informacji [*ang. Senior Agency Information Security Officer - SAISO*, również nazywanych *ang. Chief Information Security Officer - CISO*] oraz menadżerów bezpieczeństwa) o różnych aspektach bezpieczeństwa informacji jakie mają wdrożyć i nadzorować w swoich organizacjach. Podręcznik dostarcza również wskazówek ułatwiających realizację spójnego podejścia do programów bezpieczeństwa informacji w organizacjach. Chociaż użyta w niniejszym dokumencie terminologia jest ukierunkowana na sektor publiczny, z podręcznika można też czerpać wskazówki w zakresie wymagań bezpieczeństwa mających zastosowanie do innych podmiotów.

1.2. ZWIĄZEK Z ISTNIEJĄCYMI NARODOWYMI STANDARDAMI CYBERBEZPIECZEŃSTWA

Niniejszy podręcznik podsumowuje i uzupełnia szereg istniejących dokumentów zawierających rekomendacje i wskazówki zawarte w publikacjach NSC oraz dostarcza dodatkowych informacji na powiązane z nimi tematy. Referencje do tych dokumentów znajdują się w odpowiednich podrozdziałach.

1.3. ODBIORCY

Docelowymi odbiorcami niniejszego podręcznika są kierownicy jednostek organizacyjnych, CIO, SAISO (powszechnie nazywani również CISO) oraz menadżerowie ds. bezpieczeństwa. Podręcznik dostarcza informacji, które jego odbiorcy mogą wykorzystać do tworzenia strategii programu bezpieczeństwa informacji. Mimo różnic między środowiskiem sektora publicznego i prywatnego, zwłaszcza w kwestii priorytetów i wymagań prawnych, podstawowe zasady bezpieczeństwa informacji są takie same. Niniejszy podręcznik pomocny będzie zatem dla każdej osoby zarządzającej, która potrzebuje szerokiej wiedzy na temat przeglądu praktyk w zakresie bezpieczeństwa informacji.

ROZDZIAŁ 2

2. ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI

W prowadzeniu codziennej działalności oraz dostarczaniu produktów i usług organizacje w dużej mierze polegają na technologiach informacyjnych (*ang. Information Technology - IT*). Coraz większa zależność od technologii informacyjnych, rosnąca złożoność wykorzystywanej infrastruktury IT, a także ciągłe zmiany dotyczące zagrożeń i ryzyka w zakresie bezpieczeństwa informacji sprawiły, że bezpieczeństwo stało się funkcją o krytycznym znaczeniu dla misji danej organizacji. Funkcja musi podlegać zarządzaniu i regulowaniu w celu zmniejszenia ryzyka dla działań organizacji i zapewnienia, aby organizacje mogły wykonywać swoje obowiązki i wspierać społeczeństwo.

Celem zarządzania bezpieczeństwem informacji jest zapewnienie, by organizacje aktywnie wdrażały odpowiednie środki bezpieczeństwa informacji wspierające ich misję w ekonomicznie efektywny sposób, przy jednoczesnym panowaniu nad rozwijającym się ryzykiem dla bezpieczeństwa informacji. Zarządzanie bezpieczeństwem informacji jako takie posiada własne wymagania, wyzwania, działania i rodzaje możliwej struktury. Zarządzanie bezpieczeństwem informacji pełni również istotną funkcję w określaniu kluczowych zadań i obowiązków w zakresie bezpieczeństwa informacji, a także wpływa na opracowywanie i nadzorowanie polityki oraz bieżących działań monitorujących w tym obszarze.

Dla zapewnienia odpowiedniego poziomu wsparcia swojej misji oraz właściwej realizacji obecnych i przyszłych wymagań w zakresie bezpieczeństwa informacji, każda organizacja powinna ustanowić formalną strukturę zarządzania bezpieczeństwem informacji.

> *Zarządzanie bezpieczeństwem informacji można zdefiniować jako proces ustanowienia i utrzymania ram oraz wspomagających struktur i procesów zarządzania mający na celu zapewnienie, by strategie bezpieczeństwa informacji wspierały realizację celów działalności i były do nich dostosowane, były zgodne z obowiązującymi przepisami i regulacjami dzięki przestrzeganiu polityk i zabezpieczeń wewnętrznych, a także umożliwiały przydzielanie obowiązków.*

2.1. WYMAGANIA DOTYCZĄCE ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Jako minimum, zarządzanie bezpieczeństwem informacji w organizacji musi spełniać wymagania sformułowane w obowiązujących ustawach, rozporządzeniach i dyrektywach. Ponadto, określenie ogólnych dobrych praktyk zarządzania może przynieść organizacjom korzyści w postaci ustanowienia silnego pionu kierownictwa i nadzoru. Organizacje powinny dostosować praktyki z zakresu zarządzania bezpieczeństwem informacji do własnych zadań, działań i potrzeb.

Rys. 2-1 przedstawia kluczowe role organów legislacyjnych, regulacyjnych i nadzorczych w ustanawianiu zarządzania, a także wymagań w zakresie zarządzania bezpieczeństwem informacji w organizacji.

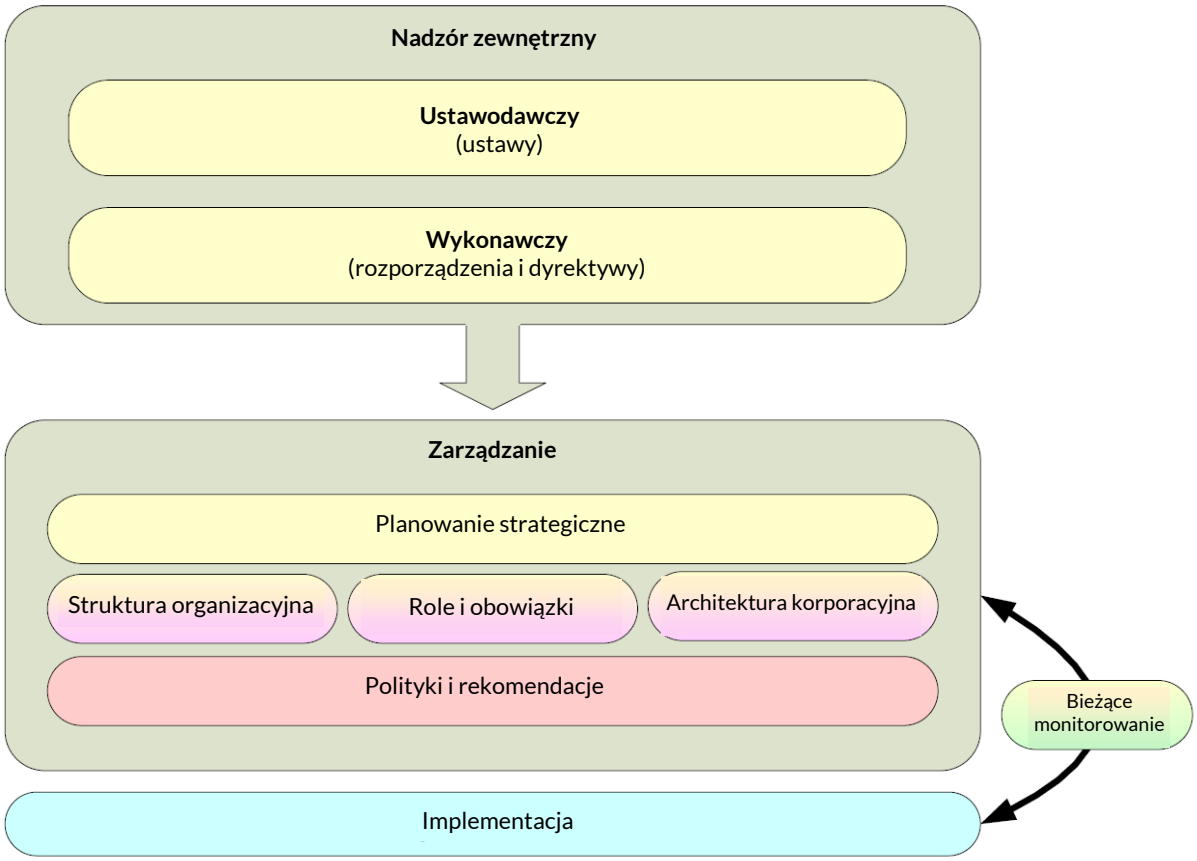
Rysunek 2-1. Kluczowe role legislacyjne, regulacyjne i nadzorcze

Potrzeba określenia i wdrożenia odpowiednich praktyk zarządzania bezpieczeństwem informacji w organizacji może okazać się dużym wyzwaniem. Organizacje powinny określić stosowne wymagania w oparciu o odpowiednie ustawy i rozporządzenia oraz dyrektywy i wydane na poziomie organizacji wytyczne. Ponadto, organizacje powinny zapewnić, by struktury zarządzania bezpieczeństwem informacji były wdrażane w sposób, który najlepiej wspomaga realizację ich własnych misji i działań.

2.2. KOMPONENTY ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Organizacje powinny integrować działania w obszarze zarządzania bezpieczeństwem informacji z własną działalnością i strukturą organizacyjną poprzez zapewnienie odpowiedniego zaangażowania swojego kierownictwa w nadzór nad wdrażaniem

środków bezpieczeństwa informacji w całej organizacji. Kluczowe działania służące takiej integracji to: planowanie strategiczne, zaprojektowanie i rozwój organizacji, ustanowienie ról i obowiązków, zintegrowanie z architekturą przedsiębiorstwa oraz udokumentowanie celów bezpieczeństwa w polityce i wytycznych. Wzajemne powiązania powyższych komponentów przedstawiono na rys. 2-2.



Rysunek 2-2. Komponenty zarządzania bezpieczeństwem informacji

2.2.1. PLANOWANIE STRATEGICZNE BEZPIECZEŃSTWA INFORMACJI

Organizacje powinny zintegrować bezpieczeństwo informacji ze swoimi procesami planowania strategicznego poprzez ustanowienie i udokumentowanie strategii bezpieczeństwa informacji, które są bezpośrednim wsparciem w planowaniu strategii i efektywności. Realizowana przez organizację strategia bezpieczeństwa informacji powinna ustanawiać kompleksowe ramy umożliwiające rozwój, instytucjonalizację, ocenę i doskonalenie programu bezpieczeństwa informacji. Strategia bezpieczeństwa informacji powinna być wsparciem ogólnych planów organizacji w zakresie strategii i wyników oraz strategicznego planu IT (w stosownych przypadkach), a jej treść

powinna w sposób wyraźny odnosić się do stosownych strategii wyższego rzędu. Każda organizacja powinna w swoim programie bezpieczeństwa informacji zdefiniować następujące elementy:

- wyraźna i kompleksowa misja, wizja, cele oraz sposób w jaki odnoszą się one do misji organizacji;
- ogólny plan osiągnięcia celów i zachowania atrybutów bezpieczeństwa informacji, wraz z krótko i długoterminowymi oraz zamierzonymi wynikami dla każdego celu i atrybutu, które będą stosowane w całym okresie realizacji tego planu, aby kierować postępami w realizacji określonych celów;
- mierniki wyników pozwalające na ciągłe monitorowanie realizacji określonych celów i atrybutów oraz postępów w osiąganiu stanu docelowego.

Organizacje powinny zawrzeć swoje strategie bezpieczeństwa informacji w strategicznym planie bezpieczeństwa informacji lub innym stosownym dokumencie. Niezależnie od sposobu udokumentowania strategii bezpieczeństwa informacji, jej treść powinna być zbieżna z ogólnymi działaniami organizacji w zakresie planowania strategicznego. Dokument powinien podlegać weryfikacji w przypadku wystąpienia znaczącej zmiany w otoczeniu organizacji związanym z bezpieczeństwem informacji, w tym:

- zmiany w obowiązujących przepisach, rozporządzeniach lub dyrektywach;
- zmiany w priorytetach misji organizacji;
- pojawiających się kwestii związanych z bezpieczeństwem informacji, takich jak zmiany zagrożeń i podatności lub wdrożenie nowych technologii.

2.2.2. STRUKTURY ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Struktury zarządzania bezpieczeństwem informacji można scharakteryzować na różne sposoby. Istnieją dwa podstawowe modele tych struktur: scentralizowany i zdecentralizowany. O ile, to najwyższe kierownictwo ostatecznie odpowiada za zarządzanie i kierowanie organizacją, o tyle uprawnienia i odpowiedzialność w zakresie bezpieczeństwa informacji w obu tych modelach, różnią się. Główne cechy dwóch omawianych struktur to:

- **Struktura scentralizowana.** CIO (lub w szczególnych przypadkach SAISO) sprawują szczegółową kontrolę nad budżetem na wszystkie działania dotyczące bezpieczeństwa informacji w organizacji. Wszystkie osoby zajmujące się bezpieczeństwem informacji w danej organizacji podlegają SAISO, który odpowiada za zapewnienie wdrażania i monitorowania środków bezpieczeństwa informacji w całej organizacji.
- **Struktura zdecentralizowana.** SAISO są odpowiedzialni za rozwój polityki i nadzór nad nią. SAISO sprawują obowiązki budżetowe w odniesieniu do organizacyjnego programu bezpieczeństwa informacji, ale nie w odniesieniu do programów bezpieczeństwa informacji w komórkach operacyjnych. SAISO jednostek operacyjnych podlegają kierownikowi jednostki organizacyjnej, a nie organizacyjnemu SAISO. SAISO jednostek operacyjnych odpowiadają za wdrażanie i monitorowanie praktyk w zakresie bezpieczeństwa informacji w swoich komórkach.

Całkowicie scentralizowane lub zdecentralizowane struktury zarządzania należą raczej do rzadkości. W rzeczywistości, różnorodność wdrożonych struktury zarządzania bezpieczeństwem informacji obejmuje kontinuum od struktury scentralizowanej z jednej strony do struktury zdecentralizowanej z drugiej. Organizacje przyjmują zazwyczaj struktury hybrydowe, które łączą pewne cechy zarówno struktur scentralizowanych jak i zdecentralizowanych, przy czym zastosowane połączenie tych cech odpowiada misji, rozmiarowi i jednolitości komponentów danej organizacji, a także już istniejącej strukturze zarządzania.

Tworząc lub zmieniając swoją strukturę zarządzania bezpieczeństwem informacji, organizacja powinna ustalić optymalny zakres centralizacji lub decentralizacji biorąc pod uwagę następujące czynniki:

- rozmiar organizacji,
- realizowana przez organizację misja oraz stopień jej dywersyfikacji lub jednolitości,
- istniejąca infrastruktura IT organizacji,
- obowiązujące wymagania prawne i wewnętrzne dotyczące zarządzania,

- wielkość budżetu organizacji,
- zdolności organizacji w zakresie bezpieczeństwa informacji,
- liczba i odległość między fizycznymi lokalizacjami;
- praktyki w zakresie podejmowania decyzji oraz pożądana dynamika zmian w praktykach dotyczących bezpieczeństwa informacji.

W zależności od stopnia ograniczenia lub różnorodności powyższych czynników, przyjęta przez organizację hybrydowa struktura zarządzania bezpieczeństwem informacji będzie plasować się gdzieś między całkowitym scentralizowaniem, a całkowitym zdecentralizowaniem, co przedstawiono na poniższym rys. 2-3. Miejsce zajmowane przez organizację w tym kontinuum może się z czasem przesuwać ku któremuś z krańców w reakcji na zmiany czynników wewnętrznych lub wymagań zewnętrznych.

Ponieważ struktura zarządzania bezpieczeństwem informacji w dużym stopniu zależy od ogólnej struktury organizacyjnej, wybór sposobu organizacji działań w tym zakresie jest często ograniczony. Organizacje powinny mieć świadomość cech i wyzwań struktury scentralizowanej lub zdecentralizowanej oraz pracować w ramach własnych organizacji nad zapewnieniem najlepszego wykorzystania zasobów dotyczących bezpieczeństwa informacji w utworzonych przez siebie strukturach.

2.2.3. KLUCZOWE ROLE I OBOWIĄZKI W ZAKRESIE ZARZĄDZANIA[2]

W strukturach większości organizacji występuje szereg podobnych interesariuszy zawiązanych z zarządzaniem. Należą do nich m.in. wyższa kadra kierownicza, CIO, personel zajmujący się bezpieczeństwem informacji oraz finansami w organizacji (*ang. Chief Financial Officer - CFO*). Szczegółowe wymagania dla każdej z tych ról mogą różnić się w zależności od stopnia centralizacji zarządzania bezpieczeństwem informacji albo konkretnych misji i potrzeb danej organizacji.

[2] Dodatkowe wytyczne dotyczące ról i obowiązków z zakresu bezpieczeństwa, zob. następujące rozdziały niniejszego podręcznika: Rozdział 5 Planowanie finansowe i kontrola inwestycji; Rozdział 8 Planowanie bezpieczeństwa; Rozdział 11 Certyfikacja, akredytacja i oceny bezpieczeństwa; oraz Rozdział 14 Zarządzanie konfiguracją.

Rysunek 2-3. Struktury zarządzania bezpieczeństwem informacji

2.2.3.1. KIEROWNIK JEDNOSTKI ORGANIZACYJNEJ

Podstawowe obowiązki kierownika jednostki organizacyjnej (*ang. head of agency - HA*) w zakresie bezpieczeństwa informacji:

- zapewnienie środków bezpieczeństwa informacji odpowiednich do ryzyka i skali szkód wynikających z nieautoryzowanego dostępu, użytkowania, ujawnienia, zakłócenia, modyfikacji lub zniszczenia informacji przetwarzanych przez organizację lub w jej imieniu, a także w odniesieniu do systemów informacyjnych użytkowanych lub obsługiwanych przez organizację albo jej wykonawcę lub inną organizację w jej imieniu;
- zapewnienie opracowania, udokumentowania i wdrożenia programu bezpieczeństwa informacji w celu zabezpieczenia wszystkich systemów, sieci i danych wspierających działania organizacji;
- zapewnienie zintegrowania procesów bezpieczeństwa informacji z procesami planowania operacyjnego i strategicznego w celu realizacji misji organizacji;
- zapewnienie udzielenia personelowi wyższego szczebla w organizacji niezbędnych uprawnień do zabezpieczania operacji i aktywów znajdujących się pod ich kontrolą;
- wyznaczenie CIO i przekazanie tej osobie uprawnień w zakresie zapewnienia zgodności z wszystkimi stosownymi wymaganiami bezpieczeństwa informacji;

- zapewnienie, aby organizacja przeszkoliła personel w zakresie wsparcia zgodności z zasadami, procesami, normami i wytycznymi dotyczącymi bezpieczeństwa informacji;
- zapewnienie, aby CIO, w koordynacji z innymi członkami wyższej kadry kierowniczej w organizacji, przedstawiał kierownikowi jednostki organizacyjnej coroczne sprawozdania ze skuteczności obowiązującego w organizacji programu bezpieczeństwa informacji, w tym postępów w realizacji działań naprawczych.

2.2.3.2. CHIEF INFORMATION OFFICER - CIO

CIO organizacji powierzone zostają następujące obowiązki:

- wyznaczenie SAISO;
- opracowanie i utrzymanie obowiązującego w całej organizacji programu bezpieczeństwa informacji;
- opracowanie i utrzymanie zasad, procedur i technik bezpieczeństwa informacji spełniających wszystkie stosowne wymagania;
- zapewnienie zgodności ze stosownymi wymaganiami dotyczącymi bezpieczeństwa informacji;
- przedstawianie kierownikowi jednostki organizacyjnej, w koordynacji z innymi członkami wyższej kadry kierowniczej, corocznych sprawozdań ze skuteczności obowiązującego w organizacji programu bezpieczeństwa informacji, w tym postępów w realizacji działań naprawczych.

2.2.3.3. SENIOR AGENCY INFORMATION SECURITY OFFICER - SAISO[3]

SAISO powierzone zostają następujące obowiązki:

- wykonywanie obowiązków dotyczących bezpieczeństwa informacji jako podstawowych zadań;

[3] W niektórych organizacjach odpowiednikiem SAISO jest CISO (*ang. Computer Information Security Officer*) lub CSO (*ang. Chief Security Officer*).

- kierowanie zespołem posiadającym uprawnienia i zasoby w zapewnieniu przestrzegania wymagań bezpieczeństwa przez organizację;
- okresowe szacowanie ryzyka i skali szkód wynikających z nieautoryzowanego dostępu, użytkowania, ujawnienia, zakłócenia, modyfikacji lub zniszczenia informacji i systemów informacyjnych, które wspierają działania i aktywa organizacji;
- opracowanie i utrzymanie ekonomicznych i opartych na analizie ryzyka polityk, procedur i technik zabezpieczeń informacji uwzględniających wszystkie stosowne wymagania w całym cyklu życia każdego systemu informacyjnego organizacji w celu zapewnienia zgodności ze stosownymi wymaganiami;
- wspomaganie opracowywania podporządkowanych planów zapewniania odpowiedniego poziomu bezpieczeństwo informacji w sieciach, obiektach i systemach albo grupach systemów informacyjnych;
- zapewnienie odpowiedniego przeszkolenia personelu organizacji, w tym wykonawców, w zakresie świadomości bezpieczeństwa informacji;
- szkolenie i nadzorowanie personelu odpowiedzialnego za bezpieczeństwo informacji w zakresie wykonywanych obowiązków;
- okresowe testowanie i ocenianie skuteczności polityk, procedur i praktyk z zakresu bezpieczeństwa informacji;
- ustanowienie i utrzymanie procesu planowania, wdrażania, oceniania i dokumentowania działań naprawczych dotyczących niedociągnięć w politykach, procedurach i praktykach organizacji z zakresu bezpieczeństwa informacji;
- opracowanie i wdrożenie procedur wykrywania, raportowania i reagowania na incydenty bezpieczeństwa;
- zapewnienie przygotowania i utrzymania planów i procedur zapewnienia ciągłości działania systemów informacyjnych wspierających działania i aktywa organizacji;
- wspieranie CIO organizacji w przedstawianiu kierownikowi jednostki organizacyjnej corocznych sprawozdań ze skuteczności obowiązującego

w organizacji programu bezpieczeństwa informacji, w tym postępów w realizacji działań naprawczych.

2.2.3.4. GŁÓWNY ARCHITEKT KORPORACYJNY

Główny architekt korporacyjny (*ang. Chief Enterprise Architect*) lub osoba na porównywalnym stanowisku w organizacji odpowiada za:

- kierowanie pracami rozwojowymi i wdrożeniowymi w zakresie architektury korporacyjnej organizacji;
- współpracowanie z pionami organizacji w celu zapewnienia właściwej integracji pionów z architekturą korporacyjną;
- uczestnictwo w działaniach organizacji z zakresu planowania strategii i wyników w celu zapewnienia właściwej integracji architektury korporacyjnej;
- ułatwianie integracji bezpieczeństwa informacji ze wszystkimi warstwami architektury korporacyjnej w celu zapewnienia wdrażania bezpiecznych rozwiązań przez organizację;
- ścisłą współpracę z menadżerami programów, SAISO i właścicielami biznesowymi w celu zapewnienia, aby wszystkie wymagania techniczne dotyczące infrastruktury były odpowiednio uwzględniane poprzez stosowanie federalnej architektury korporacyjnej[4] (*ang. Federal Enterprise Architecture*, *FEA*) oraz profilu bezpieczeństwa i prywatności (*ang. Security and Privacy Profile - SPP*).

2.2.3.5. ROLE POWIĄZANE[5]

W osiąganiu bezpieczeństwa informacji udział ma wiele innych osób w organizacji, począwszy od najwyższego kierownictwa po indywidualnych użytkowników. Poniżej podano kilka podstawowych ról wyższej kadry zarządzającej wraz z towarzyszącymi im obowiązkami. Zakres każdej z ról będzie zależeć od tego, czy będą one redundantne w zdecentralizowanej strukturze zarządzania. Role te powinny zgodnie współpracować

[4] Brak odzwierciedlenia w polskim prawodawstwie. Podano jak przykładowe rozwiązanie.

[5] Role zostały podane w celach informacyjnych.

dla zapewnienia, aby ich odpowiedzialność organizacyjna obejmowała bezpieczeństwo informacji.

Inspektor (*ang. Inspector General - IG*) to statutowy organ w obrębie organizacji do którego obowiązków należy m.in. ocena praktyk organizacji w zakresie bezpieczeństwa informacji oraz identyfikowanie podatności i ewentualnej potrzeby zmodyfikowania środków bezpieczeństwa.

Inspektor realizuje to zadanie poprzez:

- wykrywanie nadużyć finansowych albo przypadków marnotrawstwa, nadużywania lub niewłaściwego używania funduszy organizacji;
- identyfikowanie niedociągnięć operacyjnych w obrębie organizacji;
- zapewnienie, aby problemy leżące u podstaw tych braków zostały naprawione;
- proponowanie zaleceń dotyczących zapobiegania problemom w przyszłości.

Kluczowa osoba w zakresie finansów (*ang. Chief Financial Officer - CFO*) to wysokiej rangi doradca finansowy komisji oceny inwestycji (*ang. Investment Review Board - IRB*) i kierownika jednostki organizacyjnej. Inwestycje z zakresu bezpieczeństwa informacji mieszczą się w zakresie kompetencji CFO i są ujmowane w jego sprawozdaniach.
W tym charakterze, CFO odpowiada za:

- dokonywanie przeglądu celów kosztowych każdej większej inwestycji z zakresu bezpieczeństwa informacji;
- przekazywanie informacji o zarządzaniu finansami do komórki zarządzania i budżetu (*ang. Office of Management and Budget - OMB*);
- przestrzeganie obowiązków legislacyjnych i określonych przez OMB w zakresie, w jakim dotyczą one inwestycji finansowych w obszarze IT;
- dokonywanie przeglądów systemów mających wpływ na zarządzanie finansami
- przekazywanie ocen inwestycji do IRB.

Inspektor ochrony danych lub inny wyznaczona osoba odpowiedzialna za ochronę prywatności. Inspektor ochrony danych (*ang. Chief Privacy Officer*) odpowiada za zgodność z zasadami ochrony prywatności w całej organizacji, w tym za środki zapewnienia tej zgodności stosowane do aktywów i działań z zakresu bezpieczeństwa informacji. Inspektor ochrony danych pracuje na rzecz utrzymania równowagi między wymaganiami dotyczącymi bezpieczeństwa i ochrony prywatności oraz zapewnienia, aby jedno nie było wystawiane na uszczerbek w imię drugiego.

W tym celu, inspektor ochrony danych działa jako osoba odpowiedzialna za:

- opracowywanie, promowanie i wspieranie programów ochrony prywatności w organizacji,
- podnoszenie świadomości możliwych kwestii i zasad dotyczących ochrony prywatności
- dokonywanie przeglądów oraz wdrażanie przepisów dotyczących ochrony prywatności.

Kierownik ds. bezpieczeństwa fizycznego lub inna wyznaczona osoba odpowiedzialna za bezpieczeństwo fizyczne. Kierownik ds. bezpieczeństwa fizycznego (*ang. Physical Security Officer*) odpowiada za ogólne wdrażanie zabezpieczeń fizycznych i zarządzanie nimi w całej organizacji, w tym z uwzględnieniem integracji ze stosownymi zabezpieczeniami informacji. W trakcie opracowywania programów bezpieczeństwa informacji personel wyższego szczebla powinien pracować nad zapewnieniem koordynacji uzupełniających się zabezpieczeń.

W obszarze bezpieczeństwa informacji, kierownik ds. bezpieczeństwa fizycznego działa jako osoba odpowiedzialna za:

- opracowywanie, publikowanie, wdrażanie i monitorowanie programów bezpieczeństwa fizycznego organizacji, w tym z uwzględnieniem odpowiednich środków bezpieczeństwa w alternatywnych miejscach pracy;
- zapewnienie wdrożenia i monitorowania w organizacji środków kontroli dostępu (tzn. autoryzacji, dostępu, kontroli odwiedzających, środków transmisji, środków zobrazowania, logowania);

- koordynowanie zabezpieczeń środowiskowych organizacji (tzn. zasilania bieżącego i awaryjnego oraz zasilania rezerwowego, ochrony przeciwpożarowej, sterowania temperaturą i wilgotnością powietrza, szkód wyrządzanych przez wodę)
- nadzorowanie i zarządzanie zabezpieczeniami dotyczącymi dostaw i usuwania aktywów.

Kierownik ds. bezpieczeństwa osobowego lub inna wyznaczona osoba odpowiedzialna za bezpieczeństwo osobowe. Ten zakres odpowiedzialności jest często spotykany w organizacjach Human Resources lub Human Capital. Kierownik ds. bezpieczeństwa osobowego (*ang. Personnel Security Officer*) odpowiada za ogólne wdrażanie zabezpieczeń osobowych i zarządzanie nimi w całej organizacji, w tym z uwzględnieniem integracji ze stosownymi zabezpieczeniami informacji. W miarę opracowywania programów bezpieczeństwa informacji, personel wysokiego szczebla powinien współpracować dla zapewnienia koordynacji uzupełniających się środków bezpieczeństwa. W obszarze bezpieczeństwa informacji, kierownik ds. bezpieczeństwa osobowego działa jako osoba odpowiedzialna za:

- opracowywanie, publikowanie, wdrażanie i monitorowanie programów bezpieczeństwa osobowego organizacji;
- opracowywanie i wdrażanie kategoryzacji stanowisk pracy (z uwzględnieniem zabezpieczeń osób trzecich), umów w sprawie dostępu, a także dobór, zwalnianie i przenoszenie personelu
- zapewnienie spójnych i odpowiednich sankcji dla personelu naruszającego zarządcze, operacyjne lub techniczne środki bezpieczeństwa informacji.

Rola ds. zakupów/zawierania umów. Funkcja dokonywania zakupów / zawierania umów polega na zarządzaniu umowami i nadzorowaniu ich realizacji. Personel sprawujące tę funkcję ma następujące obowiązki w zakresie bezpieczeństwa informacji:

- współpracowanie z SAISO lub inną odpowiednią osobą w celu zapewnienia, aby realizowana przez organizację polityka zawierania umów odpowiednio uwzględniała wymagania organizacji w zakresie bezpieczeństwa informacji;

- koordynowanie z SAISO lub inną odpowiednią osobą, stosownie do wymagań, zmierzające do zapewnienia, aby wszystkie umowy i zamówienia organizacji były zgodne z realizowaną przez organizację polityką bezpieczeństwa informacji;
- zapewnianie, aby wszystkie osoby w organizacji, których obowiązki obejmują proces zamówień zostały przeszkolone w zakresie bezpieczeństwa informacji;
- wspólnie z SAISO, usprawnianie monitorowania wykonania umów pod kątem zgodności z realizowaną przez organizację polityką bezpieczeństwa informacji.

2.2.4 ARCHITEKTURA KORPORACYJNA[6]

Architektura korporacyjna (*ang. enterprise architecture - EA*) to oparte na działalności biznesowej ramy mające usprawnić funkcjonowanie całej organizacji. Celem EA jest ułatwienie analiz międzyorganizacyjnych oraz identyfikowanie powielających się inwestycji, luk i możliwości współpracy w obrębie poszczególnych organizacji i między nimi. EA ułatwia identyfikację powielających się lub nieekonomicznych inwestycji oraz obszarów, w które należy inwestować i w których organizacje mogą współpracować dla usprawnienia działań lub świadczonych przez nie usług.

Na architekturę korporacyjną składa się pięć modeli referencyjnych:

- Model referencyjny wydajności (*ang. Performance Reference Model - PRM*) stanowi wspólne ramy pomiaru wyników, które można stosować w obrębie całej FEA.
- Model referencyjny działalności (*ang. Business Reference Model - BRM*) stanowi oparte na funkcjach ramy opisujące działalność podmiotu niezależnie od organizacji.
- Model referencyjny komponentu usługowego (*ang. Service Component Reference Model - SRM*) stanowi ramy funkcjonalne oparte na działalności i wydajności klasyfikujące komponenty usługowe pod kątem tego, jak wspierają realizację celów działalności i/lub wydajności.

[6] Przedstawiono w celach informacyjnych.

- Model referencyjny danych i informacji (*ang. Data and Information Reference Model - DRM*) opisuje, na poziomie zbiorczym, dane i informacje będące wsparciem dla działań w obrębie programu i w poszczególnych obszarach działalności.
- Techniczny model referencyjny (*ang. Technical Reference Model - TRM*) stanowi ramy techniczne oparte na komponentach służące identyfikacji standardów, specyfikacji i technologii wspierających i umożliwiających dostarczanie komponentów usługowych i związanych z nimi możliwości.

OMB wymaga od organizacji integracji bezpieczeństwa z cyklem życia ich architektury korporacyjnej. Oprócz spełnienia wymagań stawianych przez OMB, integracja bezpieczeństwa informacji z działaniami organizacji w obszarze architektury korporacyjnej przynosi korzyści zarówno dla samych organizacji, jak i rządu poprzez:

- **Zmniejszenie obciążenia sprawozdawczego.** FEA wymaga od organizacji zbierania i analizowania znaczących ilości danych. Podejmowane obecnie wysiłki związane z bezpieczeństwem dostarczają informacji istotnych dla danych, technologii i wskaźników wyników z całego resortu, takich jak informacje zawarte w kwartalnych i rocznych sprawozdaniach FISMA, pismach akredytacyjnych oraz w planie i etapach działania (*ang. Plan of Actions and Milestones, POA&M*).
- **Integracja danych bezpieczeństwa.** Organizacje powinny wykorzystywać istniejące źródła danych o bezpieczeństwie informacji do identyfikacji danych, które należy ujmować w zgłoszeniach FEA, co pozwoli na ciągłe i niezawodne uzupełnianie i przekazywanie wymagań i środków bezpieczeństwa z początkowej dokumentacji certyfikacyjnej i akredytacyjnej i POA&M do FEA.
- **Zabezpieczenie wymagań bezpieczeństwa.** Udokumentowanie i zabezpieczenie informacji o stosownych wymaganiach bezpieczeństwa zapewnia, że mogą one zostać wykorzystane w ramach dowolnego procesu zarządzania lub podejmowania decyzji. Gdyby, na przykład, rząd zechciał przeprowadzić szeroko zakrojoną reorganizację (np. stworzyć nowy departament lub organizację), świadoma bezpieczeństwa FEA będzie w stanie wyraźnie wskazać nie tylko miejsca przecięcia wspólnych obszarów działalności, ale też odpowiednie wymagania bezpieczeństwa. Kolejny przykład: gdyby jakiś departament miał dopuścić użytkowanie

konkretnego rodzaju narzędzia technologicznego, FEA będzie w stanie wskazać dla tej technologii wymagania w dotyczące bezpieczeństwa i ochrony prywatności, a także wymagania dotyczące danych, jakie obsługiwałoby to narzędzie. Ponieważ rząd prowadzi wiele działań związanych z technologią informacyjną, w tym z procesami w ramach ochrony infrastruktury krytycznej (*ang. Critical Infrastructure Protection)* i planu kontynuacji operacji prowadzonymi z myślą o zabezpieczeniu zasobów narodowych oraz zdolności instytucji i organizacji do działania w niekorzystnych lub nadzwyczajnych warunkach, bezpieczna FEA wesprze te działania, a jednocześnie zapewni odpowiednią ochronę przetwarzanych w ich ramach informacji.

2.2.5 POLITYKI I WSKAZÓWKI DOTYCZĄCE BEZPIECZEŃSTWA INFORMACJI

Polityki bezpieczeństwa informacji to globalny zestaw przepisów, dyrektyw, regulacji i praktyk określających jak organizacja zarządza, chroni i przetwarza informacje[7].

Polityki bezpieczeństwa informacji to niezbędny komponent zarządzania bezpieczeństwem informacji—bez nich zarządzanie nie miałoby ani treści, ani reguł do egzekwowania. Polityki bezpieczeństwa informacji powinny opierać się na połączeniu odpowiednich przepisów (np. ustawy), stosownych norm i standardów (np. norm wydawanych przez Polski Komitet Normalizacyjny - PKN i rekomendacji przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa) oraz wewnętrznych wymagań danej organizacji.

Obowiązujące w organizacji zasady bezpieczeństwa informacji powinny odnosić się do podstaw organizacyjnej struktury bezpieczeństwa informacji, w tym:

- ról i obowiązków dotyczących bezpieczeństwa informacji,
- bazowych środków bezpieczeństwa i reguł dotyczących ich rozszerzenia oraz
- zasad zachowania, których użytkownicy mają przestrzegać oraz minimalnych konsekwencji nieprzestrzegania ich.

Dla wsparcia zasad bezpieczeństwa organizacji należy opracować uzupełniające

[7] NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*.

wytyczne i procedury dotyczące sposobu wdrażania konkretnych zabezpieczeń w całej strukturze korporacyjnej. Wytyczne te, stworzone przez organizację w związku z wytycznymi zewnętrznymi (np. normami PKN publikacjami NSC) powinny być zgodne z politykami bezpieczeństwa informacji i nie mogą ich zastępować, chyba że to same zasady są modyfikowane. Organizacje powinny zapewnić, aby ich polityki bezpieczeństwa informacji były na tyle aktualne, aby uwzględniały warunki środowiska bezpieczeństwa informacji oraz misję i wymagania operacyjne organizacji. Aby uniknąć dezaktualizacji bezpieczeństwa informacji, organizacje powinny wdrożyć cykl przeglądu i rewizji zasad. W ramach okresowego przeglądu i wstępnego rozwoju polityk bezpieczeństwa informacji organizacje powinny podjąć działania dla zapewnienia wystarczającej koordynacji wszystkich wewnętrznych zasad bezpieczeństwa (tzn. bezpieczeństwa fizycznego i osobowego) w celu skutecznej realizacji przekrojowych i zbieżnych celów bezpieczeństwa, np. dotyczących inicjatyw w zakresie kontroli dostępu.

2.2.6 BIEŻĄCE MONITOROWANIE

Skuteczny program zarządzania bezpieczeństwem informacji wymaga stałego przeglądu. Organizacje powinny monitorować status swoich programów, aby upewnić się, że:

- bieżące działania dotyczące bezpieczeństwa informacji są odpowiednim wsparciem dla misji organizacji;
- zasady i procedury są aktualne i w stosownych przypadkach nadążają za ewoluującymi technologiami;
- zabezpieczenia spełniają cel, w jakim zostały wdrożone.

Z upływem czasu, zasady i procedury mogą stać się niewystarczające w związku ze zmianami zachodzącymi w misji i wymaganiach operacyjnych organizacji, zmianami dotyczącymi zagrożeń i środowiska działania, obniżeniem się stopnia zgodności, zmianami w technologii lub infrastrukturze, lub zmianami w procesach biznesowych. Cennym środkiem służącym do identyfikowania obszarów występowania niezgodności mogą być okresowe oceny i sprawozdania z działań, które przypominają użytkownikom o ich obowiązkach i pokazują zaangażowanie kierownictwa w realizację programu

bezpieczeństwa. Chociaż misja organizacji nie ulega częstym zmianom, organizacja może ją rozszerzać dodając kolejne programy i aktywa, w wyniku czego potrzebne mogą być modyfikacje jej zasad i praktyk z zakresu bezpieczeństwa informacji. Ważne jest, aby zmiana w wewnętrznych wymaganiach organizacji została sprawdzona względem wymagań prawnych, ponieważ np. zmiana w stanie bezpieczeństwa systemu informacyjnego może skutkować zmianami w wymogach dotyczących sprawozdawczości.

Dla ułatwienia bieżącego monitorowania, SAISO oraz inne osoby mogą porównywać i korelować szereg różnych informacji statycznych i dostarczanych w czasie rzeczywistym, które pochodzą z bieżących działań realizowanych w obrębie i na zewnątrz ich programów. Przykładowo, przepisy FISMA (*ang. Federal Information Security Management Act*) nakładają na organizacje obowiązek przeprowadzania corocznej oceny ich programów bezpieczeństwa informacji oraz składania kwartalnych i rocznych sprawozdań dotyczących miar wyników w zakresie bezpieczeństwa informacji. Celem tych wymagań jest ułatwienie dokładnej i prowadzonej w czasie rzeczywistym oceny i monitorowania działań w ramach programu bezpieczeństwa informacji. Bieżące monitorowanie polega na wykorzystaniu istniejących danych do nadzorowania programu bezpieczeństwa i zazwyczaj odbywa się we wszystkich fazach cyklu życia programu. Do monitorowania nadzorowanych przez siebie programów organizacje mogą wykorzystywać różnorodne dane pochodzące z bieżących działań w ramach programu bezpieczeństwa informacji, w tym dane z POA&M, pomiarów i metryk wyników, ciągłej oceny, kontroli i zarządzania konfiguracją, monitoringu sieci oraz statystyk dotyczących incydentów.

Tabela 2-1 przedstawia szeroki przegląd kluczowych działań bieżących, które mogą pomóc organizacji w monitorowaniu i doskonaleniu zarządzania informacjami.

Tabela 2-1. Bieżące działania monitorujące[8]

Działania	Opis działań	Procesy i informacje pomocnicze
Plan i etapy działania (POA&M)[9]	POA&M pomaga w identyfikowaniu, ocenianiu, szeregowaniu i monitorowaniu działań naprawczych dotyczących słabości stwierdzonych w programach i systemach. POA&M śledzi wdrożone środki w celu naprawienia braków oraz zniwelowania lub wyeliminowania znanych podatności. POA&M może też pomóc w identyfikowaniu różnic w wynikach, ocenianiu wyników i wydajności organizacji w obszarze bezpieczeństwa oraz prowadzeniu nadzoru.	• Organizacja utrzymuje oddzielne POA&M dla programów i systemów. • Słabości są podawane według kryteriów określanych w stosownych wytycznych. • Systemowe POA&M są powiązane z dokumentami planowania finansowego. • Liczba bieżących działań w ramach POA&M jest stała lub rośnie, natomiast liczba zakończonych działań POA&M rośnie, a liczba opóźnionych działań POA&M maleje. • Po naprawieniu, słabości nie pojawiają się już w POA&M. • Menadżerowie wykorzystują POA&M w swoich systemach i programach jako narzędzia do mitygacji[10] (*ang. mitigation*) słabości. • POA&M podlega aktualizacji w miarę zamykania i odkrywania słabości, a zatem odzwierciedla najświeższy

8 Przykładowy proces realizowany przez agencje federalne USA.

9 Dodatkowe rekomendacje w zakresie procesu POA&M, zob. Rozdział 11 „Certyfikacja, akredytacja i oceny ryzyka" niniejszego podręcznika.

10 Mitygacja - podejmowanie odpowiednich decyzji, działań lub praktyk w celu zmniejszenia poziomu ryzyka związanego z jednym lub większą liczbą zagrożeń, scenariuszy zagrożeń lub podatności na ataki. Tymczasowe ograniczenie lub zmniejszenie wpływu podatności lub prawdopodobieństwa jej wykorzystania.

Działania	Opis działań	Procesy i informacje pomocnicze
		stan działań niwelujących słabości prowadzonych przez organizację. • POA&M można w dowolnym momencie łatwo udostępnić odpowiednim stronom na ich żądanie. • Podsumowanie postępów organizacji w realizacji POA&M jest przekazywane OMB co kwartał.
Pomiary i metryki[11]	Metryki to narzędzia przeznaczone do poprawiania wyników i rozliczalności poprzez zbieranie, analizowanie i raportowanie istotnych danych związanych z wynikami. Metryki bezpieczeństwa informacji monitorują realizację celów poprzez ilościowe przedstawienie poziomu wdrożenia zabezpieczeń oraz ich skuteczności i wydajności, analizowanie adekwatności działań z zakresu bezpieczeństwa oraz identyfikowanie możliwych działań doskonalących.	• Metryki/miary wyników są zgodne ze strategią organizacji oraz strategią w zakresie bezpieczeństwa informacji, a zatem są zgodne z wymaganiami misji. • Organizacja wykorzystuje metryki/miary wyników do kwantyfikowania i oceny swojego działania w obszarze bezpieczeństwa informacji oraz identyfikowania i adresowania działań naprawczych. • Decydenci organizacji wykorzystują metryki/miary wyników jako dane wejściowe w podejmowaniu decyzji w sprawie ustalania priorytetów działań i zasobów oraz przydzielania funduszy. • Organizacja wykorzystuje metryki/miary wyników, które

[11] Dodatkowe wytyczne w zakresie pomiarów i metryk, zob. NIST SP 800-55, *Security Metrics Guide for Information Technology Systems*, a także Rozdział 7 „Miary wyników" niniejszego podręcznika.

Działania	Opis działań	Procesy i informacje pomocnicze
		można pozyskać bez nadzwyczajnych nakładów. • Metryki/miary wyników dostarczają danych liczbowych i empirycznych, a nie opinii. • Metryki/miary wyników są regularnie weryfikowane przez osoby z zewnątrz pod kątem dokładności i wiarygodności. • Metryki/miary wyników dostarczają istotnych danych do oceny wpływu zmian w czasie. • Organizacja zbiera dane do obliczania metryk/miar wyników na możliwie najbardziej dyskretnym, nieprzeanalizowanym poziomie. • Organizacja wykorzystuje dobrze zdefiniowane i sprecyzowane metryki/miary wyników.
Ciągła ocena[12]	Proces ciągłej oceny polega na monitorowaniu wstępnej akredytacji bezpieczeństwa systemu informacyjnego w celu śledzenia zachodzących w nim zmian, a także na analizowaniu wpływu tych zmian na bezpieczeństwo,	• Wiele systemów informacyjnych organizacji podlega certyfikacji i akredytacji częściej niż co trzy lata. • Plany bezpieczeństwa systemu są często aktualizowane w miarę występowania zmian.

[12] Dodatkowe rekomendacje w zakresie ciągłej oceny, zob. NSC 800-30, a także Rozdział 10 „Zarządzanie ryzykiem" i Rozdział 11 „Certyfikacja, akredytacja i oceny ryzyka" niniejszego podręcznika.

Działania	Opis działań	Procesy i informacje pomocnicze
	dokonywaniu odpowiednich korekt w zabezpieczeniach i planie bezpieczeństwa systemu oraz przekazywaniu odpowiednim osobom raportów o stanie bezpieczeństwa systemu.	• Wyniki procesu ciągłej oceny można śledzić za pośrednictwem POA&M systemu. • Odpowiednie osoby w organizacji mają świadomość stanu, w jakim znajdują się podległe im systemy. • Oceny zabezpieczeń systemu oraz ocena i ewaluacja bezpieczeństwa są przeprowadzane co najmniej raz na trzy lata.
Zarządzanie konfiguracją[13]	Zarządzanie konfiguracją (*ang. Configuration Management - CM*) to niezbędny komponent monitorowania stanu zabezpieczeń i identyfikowania ewentualnych problemów związanych z bezpieczeństwem w systemach informacyjnych. Informacje te mogą pomóc menadżerom ds. bezpieczeństwa zrozumieć i monitorować ewoluujący charakter podatności w miarę ich pojawiania się w podległym im systemach, tym samym umożliwiając im nakazywanie odpowiednich zmian.	• Organizacja powołuje komisję kontroli konfiguracji (*ang. Configuration Control Board - CCB*) lub podobny organ. • W CCB uczestniczy specjalista ds. bezpieczeństwa informacji. • Udostępniane przez dostawców poprawki są testowane pod kątem wpływu na bezpieczeństwo informacji i ustawienia systemu. • Organizacje odnotowują spadek liczby incydentów spowodowanych znanymi podatnościami, których poprawki zostały przekazane administratorom systemu. • Znane podatności są rzadko odkrywane podczas różnych ocen.

[13] Dodatkowe wytyczne w zakresie zarządzania konfiguracją, zob. Rozdział 14 „Zarządzanie konfiguracją" niniejszego podręcznika.

Działania	Opis działań	Procesy i informacje pomocnicze
		• Personel odpowiedzialny za zarządzanie konfiguracją zostaje odpowiednio przeszkolony w zakresie bezpieczeństwa i jest świadomy spoczywających na nim obowiązków związanych z bezpieczeństwem. • Organizacja przygotowuje i publikuje ustandaryzowane zasady konfiguracji oraz śledzi liczbę i częstotliwość wdrożeń konfiguracji w całej organizacji.
Monitorowanie sieci[14]	Informacje o działaniu sieci i zachowaniu w niej użytkowników pomogą menadżerom programu bezpieczeństwa zidentyfikować obszary wymagające poprawy oraz wskazać ewentualne udoskonalenia w tym zakresie. Te informacje można korelować z innymi źródłami, np. POA&M i CM, aby stworzyć kompleksowy obraz stanu programu bezpieczeństwa.	• Informacje z monitorowania sieci są zestawiane i przekazywane menadżerom programu bezpieczeństwa informacji. • Informacje z monitorowania sieci są pozyskiwane na potrzeby ustalania trendów i korelowane z innymi źródłami danych, w tym statystykami incydentów, POA&M, CM i innymi dostępnymi źródłami. • Menadżerowie ds. bezpieczeństwa informacji i właściciele systemów są w stanie otrzymywać informacje z monitorowania sieci i wykorzystywać je do oceny stanu bezpieczeństwa ich systemów.

[14] Dodatkowe wytyczne w zakresie monitorowania systemu, zob. NIST 800-42, *Guidelines on Network Security Testing*.

Działania	Opis działań	Procesy i informacje pomocnicze
Statystyki incydentów i zdarzeń[15]	Statystyki incydentów to cenne dane służące ustalaniu skuteczności wdrożenia zasad i procedur bezpieczeństwa. Statystyki incydentów dostarczają menadżerom programu bezpieczeństwa dalszych szczegółów na temat stanu podległych im programów, pozwalają na obserwację trendów w wynikach działań programowych oraz informują menadżerów programu o potrzebie wprowadzenia zmian do zasad i procedur.	• Organizacja zbiera statystyki incydentów w taki sposób, aby można je było wykorzystać w regularnym pozyskiwaniu danych i ustalaniu trendów, a także do doskonalenia procesów obsługi reagowania na incydenty. • Statystyczne informacje o incydentach są zestawiane i przekazywane menadżerom programu bezpieczeństwa informacji. • Statystyki incydentów są pozyskiwane i korelowane na potrzeby ustalania trendów i korelowane z innymi źródłami danych, w tym danymi z monitorowania sieci, POA&M, CM, informacjami ze szkoleń i uświadamiania oraz innymi dostępnymi źródłami. • Menadżerowie ds. bezpieczeństwa informacji i właściciele systemów powinni otrzymywać statystyki incydentów i wykorzystywać je do oceny stanu bezpieczeństwa ich systemów.

[15] Dodatkowe wytyczne w zakresie statystyk incydentów i zdarzeń, zob. NSC 800-61, a także Rozdział 13: „Reagowanie na incydenty” niniejszego podręcznika.

2.3 WYZWANIA I KLUCZE DO SUKCESU W ZARZĄDZANIU BEZPIECZEŃSTWEM INFORMACJI

Spełnienie wymagań dotyczących zarządzania bezpieczeństwem informacji stawia organizację przed koniecznością uwzględnienia licznych i różnorodnych, a niekiedy sprzecznych, priorytetów. Kryteria te są wyzwaniami, jakie organizacja może spotkać na swojej drodze ku ustanowieniu zarządzania bezpieczeństwem informacji.

Najpowszechniejsze z nich to:

- **Zrównoważenie obszernych wymagań stawianych przez liczne organy zarządzające**. Organy zarządcze i nadzorcze ustanawiają wymagania w zakresie zarządzania i bezpieczeństwa informacji w organizacji. Chociaż rzadko zdarza się, by były one sprzeczne, to często wzajemnie się nie uzupełniają, a organizacje mogą stanąć przed koniecznością wdrożenia różnych środków zachowania zgodności i monitorowania tych środków na potrzeby sprawozdawczości.
- **Zrównoważenie przepisów legislacyjnych i zasad specyficznych dla organizacji**. Organizacje mogą realizować surowsze wymagania, które wykraczają poza wymogi wynikające z przepisów, regulacji i rekomendacji dotyczących bezpieczeństwa informacji.
- **Utrzymywanie aktualności**. Standardy i wytyczne w zakresie zarządzania ewoluują wraz z pojawianiem się różnych wymagań. Często wchodzą w życie nowe przepisy.
- **Ustalanie priorytetów dostępnego finansowania zgodnie z wymaganiami**. Rosnąca konkurencja o ograniczone budżety i środki finansowe zmusza organizacje do przeznaczania dostępnych funduszy na najbardziej priorytetowe inwestycje w bezpieczeństwo informacji.

Zarządzanie bezpieczeństwem informacji daje ramy dla ustanowienia i utrzymania programu bezpieczeństwa informacji, który będzie ewoluował razem z organizacją. Poniższa lista jest zestawieniem dobrych praktyk z zakresu zarządzania bezpieczeństwem informacji, które są kluczowe dla zapewnienia bezpieczeństwa zasobów informacyjnych:

- Działania z zakresu bezpieczeństwa informacji powinny być regulowane w oparciu o odpowiednie wymagania, w tym przepisy prawa, regulacje i polityki organizacji.
- Kierownictwo wyższego szczebla powinno aktywnie uczestniczyć w ustanawianiu ram zarządzania bezpieczeństwem informacji i regulowaniu realizacji bezpieczeństwa informacji przez organizację.
- Obowiązki dotyczące bezpieczeństwa informacji muszą być przydzielane i wykonywane przez odpowiednio przeszkolone osoby.
- Osoby odpowiedzialne za bezpieczeństwo informacji w organizacji powinny być rozliczane ze swoich działań lub ich braku.
- Priorytety bezpieczeństwa informacji powinny być komunikowane interesariuszom na wszystkich poziomach w obrębie organizacji, aby zapewnić udaną realizację programu bezpieczeństwa informacji.
- Działania dotyczące bezpieczeństwa informacji należy integrować z innymi działaniami zarządczymi organizacji, w tym z planowaniem strategicznym, planowaniem finansowym oraz architekturą korporacyjną.
- Struktura organizacyjna bezpieczeństwa informacji powinna być odpowiednia dla organizacji, którą wspiera oraz powinna ewoluować wraz ze zmianami zachodzącymi w organizacji.
- Menadżerowie ds. bezpieczeństwa informacji powinni przy użyciu dostępnych narzędzi i informacji ciągle monitorować wyniki programu/działań bezpieczeństwa, za które są odpowiedzialni.
- Informacje pozyskane w wyniku monitorowania powinny być wykorzystywane jako dane wejściowe dla decyzji dotyczących priorytetów i przydzielania funduszy, prowadząc do poprawy stanu bezpieczeństwa i ogólnych wyników organizacji.

ROZDZIAŁ 3

3. CYKL ŻYCIA SYSTEMU

Cykl życia systemu (*ang. system development life cycle - SDLC*) to całościowy proces opracowywania, wdrażania i wycofywania systemów informacyjnych, na który składają się fazy inicjacji, analizy, projektowania, wdrożenia, utrzymania i wycofania z użytku. Istnieje wiele różnych modeli i metodologii SDLC, ale generalnie wszystkie obejmują szereg określonych kroków i faz.

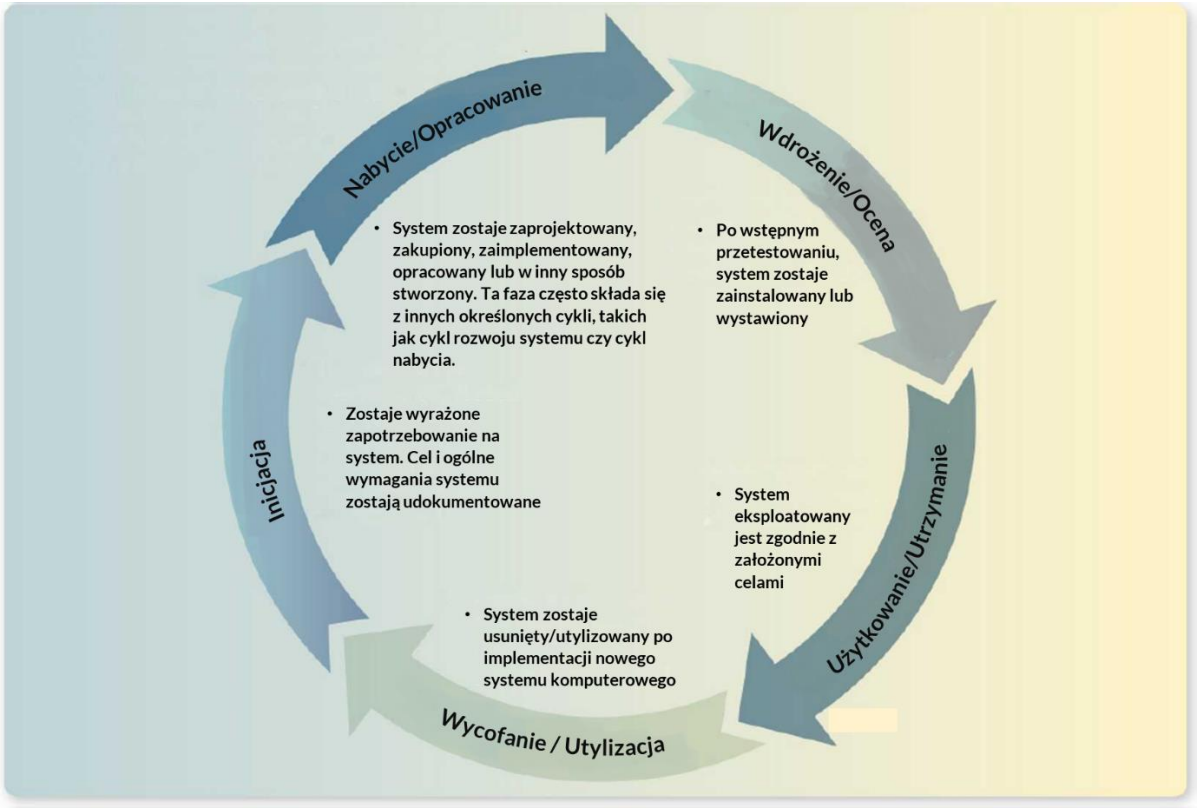
Na potrzeby procesów SDLC opracowano różnorodne metodologie, przy czym w przypadku specyficznych typów projektów niektóre metody działają lepiej niż inne. Niezależnie od tego, jaki cykl życia stosuje organizacja, bezpieczeństwo informacji musi zostać zintegrowane z SDLC dla zapewnienia odpowiedniej ochrony informacji, które dany system ma przesyłać, przetwarzać i przechowywać. Bezpieczeństwo jest najbardziej użyteczne i opłacalne, kiedy taka integracja rozpoczyna się wraz opracowywaniem systemu lub zainicjowaniem projektu integracji i trwa przez cały cykl życia, aż do wycofania systemu z użycia.

W tym rozdziale przedstawiono ogólny przegląd integracji bezpieczeństwa z SDLC, przy czym jego celem nie jest zalecanie jakiegoś konkretnego modelu czy metodologii. Każda faza SDLC obejmuje minimalny zestaw działań związanych z bezpieczeństwem informacji wymaganych do skutecznego włączenia bezpieczeństwa do systemu. Organizacja może wykorzystać standardowy SDLC opisany w tym rozdziale albo opracować taki SDLC, który będzie odpowiadać jej szczególnym potrzebom. Publikacja specjalna NIST SP 800-64 Rev. 1, *Security Considerations in the Information System Development Life Cycle*, przedstawia ramy dla włączania bezpieczeństwa do wszystkich faz SDLC (co przedstawiono na rys. 3-1), aby zapewnić wybór, nabycie i wykorzystanie odpowiednich i ekonomicznych zabezpieczeń[16].

3.1. FAZA INICJACJI

[16] Dodatkowe rekomendacje w zakresie bezpieczeństwa w procesie SDLC, zob. NSC 199, NSC 800-60 oraz NSC 800-37.

Wszystkie projekty informacyjne mają punkt początkowy, który jest powszechnie nazywany fazą inicjacji. Podczas tej fazy organizacja ustanawia potrzebę użytkowania określonego systemu i dokumentuje jego przeznaczenie. Informacje, które mają być w systemie przetwarzane, przesyłane lub przechowywane są zazwyczaj poddawane ewaluacji, podobnie jak to, kto będzie wymagać do nich dostępu i w jaki sposób ten dostęp będzie zapewniany (w ujęciu ogólnym). Ponadto, często ustala się, czy dany projekt będzie niezależnym systemem informacyjnym, czy też częścią już zdefiniowanego systemu. W tej fazie zazwyczaj ma miejsce wstępne oszacowanie ryzyka oraz rozpoczęcie opracowywania dokumentów dotyczących planowania bezpieczeństwa (plan bezpieczeństwa systemu).



Rysunek 3-1. Cykl życia systemu

Po zakończeniu tych zadań i ustaleniu istnienia zapotrzebowania na nowy lub ulepszony produkt lub usługę IT, należy wykonać kilka procesów poprzedzających zatwierdzenie projektu obejmujących wyraźne zdefiniowanie celów i ogólne określenie wymagań w zakresie bezpieczeństwa informacji. W tej fazie, organizacja zazwyczaj określa ogólne wymagania dotyczące zasad bezpieczeństwa informacji oraz

korporacyjnej architektury systemu bezpieczeństwa.

3.2. FAZA OPRACOWANIA/NABYCIA

W tej fazie, system zostaje zaprojektowany, zakupiony, zaprogramowany, opracowany lub w inny sposób skonstruowany. Ta faza często składa się z innych określonych cykli, takich jak cykl rozwoju systemu czy cykl nabycia.

Podczas pierwszej części fazy opracowania/nabycia, organizacja powinna równolegle zdefiniować wymagania dotyczące bezpieczeństwa i funkcjonalności systemu. Mogą one zostać wyrażone jako cechy techniczne (np. kontrola dostępu), mechanizmy zapewniania wiarygodności (np. weryfikacja deweloperów systemów) albo praktyki operacyjne (np. uświadamianie i szkolenie). W ostatniej części tej fazy, organizacja powinna przeprowadzić testy rozwojowe środków/funkcji technicznych i bezpieczeństwa dla zapewnienia, że działają one zgodnie z zamierzeniami, zanim przejdzie do fazy wdrożenia i integracji.

3.3. FAZA WDROŻENIA

W fazie wdrożenia, organizacja konfiguruje i uruchamia zabezpieczenia systemu, testuje ich funkcjonalność, instaluje lub wdraża system i uzyskuje formalną autoryzację do jego działania (*ang. authorization to operate*). Przed oddaniem systemu do użytkowania należy przeprowadzić przeglądy projektu i testy systemu, aby zapewnić spełnienie wszystkich wymaganych specyfikacji bezpieczeństwa. Ponadto, w przypadku dodania do aplikacji lub systemu wsparcia nowych zabezpieczeń, należy wykonać dodatkowe testy akceptacyjne tych zabezpieczeń. Dzięki takiemu podejściu, nowe zabezpieczenia spełniają specyfikacje bezpieczeństwa oraz nie są sprzeczne z istniejącymi zabezpieczeniami ani ich nie unieważniają. Wyniki przeglądów projektu i testów systemu należy w pełni udokumentować, aktualizować w miarę wykonywania kolejnych przeglądów lub testów, a także utrzymywać w oficjalnej ewidencji organizacji.

3.4. FAZA EKSPLOATACJI/UTRZYMANIA

Skuteczny program bezpieczeństwa wymaga kompleksowego i ciągłego zrozumienia słabości programu i systemu. W fazie użytkowania i utrzymania, systemy i produkty są wdrożone i pracują, ulepszenia i/lub modyfikacje systemu zostają opracowane,

przetestowane oraz następuje dodanie lub wymiana sprzętu komputerowego i/lub oprogramowania. Podczas tej fazy organizacja powinna w sposób ciągły monitorować działanie systemu, aby zapewnić jego zgodność z ustanowionymi wcześniej wymaganiami dotyczącymi użytkowników i bezpieczeństwa oraz wprowadzenie potrzebnych modyfikacji systemu.

W przypadku kontroli i zarządzania konfiguracją, ważne jest udokumentowanie proponowanych lub faktycznych zmian w planie bezpieczeństwa systemu. Systemy informacyjne zazwyczaj znajdują się w stanie ciągłej ewolucji za sprawą modernizacji sprzętu komputerowego, oprogramowania i oprogramowania układowego oraz możliwych zmian w otoczeniu systemu. Dokumentowanie zmian w systemie informacyjnym i ocena ich ewentualnego wpływu na bezpieczeństwo systemu, to niezbędna część ciągłego monitorowania oraz klucz do uniknięcia błędów w akredytacji bezpieczeństwa[17].

Monitorowanie zabezpieczeń pomaga zidentyfikować potencjalne problemy związane z bezpieczeństwem systemu informacyjnego, które nie zostały stwierdzone podczas analizy wpływu na bezpieczeństwo przeprowadzanej w ramach procesu kontroli i zarządzania konfiguracją.

3.5. FAZA WYCOFANIA

W cyklu życia systemu, faza wycofania odnosi się do procesu utrwalenia (w stosownych przypadkach) i usunięcia informacji systemowych, sprzętu i oprogramowania. Ten krok jest niezwykle ważny, ponieważ podczas omawianej tu fazy, informacje, sprzęt i oprogramowanie są przenoszone do innego systemu, archiwizowane, wyrzucane lub niszczone. Jeżeli nie zostanie prawidłowo przeprowadzona, faza wycofania może skutkować nieautoryzowanym ujawnieniem wrażliwych danych. Podczas archiwizowania informacji, organizacje powinny rozważyć potrzebę i metody ich przyszłego odzyskania. Chociaż informacje elektroniczne można stosunkowo łatwo przechowywać i odzyskiwać, problemy pojawiają się w przypadku, gdy technologia użyta do ich zapisu przestaje być dostępna w wyniku zestarzenia się lub

[17] Dodatkowe wytyczne w zakresie zarządzania konfiguracją, zob. Rozdział 14 „Zarządzanie konfiguracją" niniejszego podręcznika.

niekompatybilności z nowymi technologiami. Dodatkowo organizacja powinna zastanowić się, jakie środki należy podjąć dla umożliwienia przyszłego wykorzystania zaszyfrowanych danych, np. poprzez zapewnienie długoterminowego i bezpiecznego przechowywania kluczy kryptograficznych. Równie ważne jest rozważenie wymagań prawnych dotyczących przechowywania danych po wycofaniu systemu informacyjnego z użycia. W przypadku systemów publicznych[18], osoby zarządzające systemem powinny skonsultować się w tej sprawie z podmiotem odpowiedzialnym za przechowywanie i archiwizację dokumentów publicznych[19].

Usunięcie informacji z nośnika, np. dysku twardego lub taśmy, nazywane jest sanityzacją. Istnieją cztery kategorie sanityzacji nośników: utylizacja, oczyszczanie, wymazywanie i niszczenie[20]. Ponieważ różne sposoby sanityzacji zapewniają różne poziomy bezpieczeństwa informacji, w wyborze metody, która najlepiej odpowiada ich potrzebom, organizacje powinny kierować się wymaganiami w zakresie bezpieczeństwa informacji.

3.6. DZIAŁANIA ZWIĄZANE Z BEZPIECZEŃSTWEM W TRAKCIE SDLC

Działania związane z bezpieczeństwem należy zintegrować z SDLC, aby zapewnić właściwą identyfikację, projekt, integrację i utrzymanie stosownych zabezpieczeń w całym cyklu życia systemu informacyjnego, zgodnie z zestawieniem przedstawionym w tabeli 3-1.

---

[18] W przypadku systemów teleinformatycznych używanych do realizacji zadań publicznych zastosowanie mają w szczególności:
1) ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2023 r. poz. 57 z późn. zm.);
2) ustawa o narodowym zasobie archiwalnym i archiwach (Dz.U. z 2020 r. poz. 164 z późn. zm.);
wraz z aktami wykonawczymi.

[19] W polskim porządku prawnym organem właściwym w tego rodzaju sprawach jest Archiwum Państwowe.

[20] Dodatkowe wytyczne w zakresie sanityzacji nośników danych, zob. NIST SP 800-88, *Guidelines for Media Sanitization*.

Tabela 3-1. Działania z zakresu bezpieczeństwa w SDLC

Działania SDLC	Działania i definicje dotyczące bezpieczeństwa
A. Faza inicjacji	
Ustalenie potrzeb	• Zdefiniowanie problemu, który można rozwiązać poprzez nabycie produktu. Tradycyjne elementy ustalania potrzeb to: stworzenie podstawowej koncepcji systemu, zdefiniowanie wstępnych wymagań, ocena opłacalności, ocena technologii oraz zidentyfikowanie formy zatwierdzenia potrzebnej do dalszego badania problemu. • Ustanowienie i udokumentowanie potrzeby i przeznaczenia systemu.
Kategoryzacja zabezpieczeń	• Zidentyfikowanie informacji, które będą przesyłane, przetwarzane lub przechowywane w systemie oraz zdefiniowanie stosownych poziomów kategoryzacji informacji wg. NSC 800-60 i NSC 199. Należy wziąć pod uwagę sposób postępowania z danymi osobowymi i ich ochrony.
Wstępne szacowanie ryzyka[21]	• Stworzenie wstępnego opisu podstawowych potrzeb systemu w zakresie bezpieczeństwa. Wstępne oszacowanie ryzyka powinno określać środowisko zagrożenia, w którym system lub produkt będzie działać.
B. Faza opracowania/nabycia	
Analiza/opracowanie wymagań	• Przeprowadzenie dokładniejszego badania potrzeb, które wykorzystuje i rozwija pracę wykonaną w fazie inicjacji. • Opracowanie wymagań bezpieczeństwa i ich włączenie do specyfikacji. • Analiza wymagań funkcjonalnych, wśród których mogą być wymagania w zakresie środowiska bezpieczeństwa systemu (np. korporacyjne zasady bezpieczeństwa informacji i korporacyjna

[21] Dodatkowe wytyczne w zakresie wstępnego szacowania ryzyka, zob. NSC 199, a także Rozdział 10 „Zarządzanie ryzykiem" oraz Rozdział 11 „Certyfikacja, akredytacja i oceny bezpieczeństwa" niniejszego podręcznika.

Działania SDLC	Działania i definicje dotyczące bezpieczeństwa
	architektura bezpieczeństwa) i wymagania funkcjonalne dotyczące bezpieczeństwa. • Analiza wymagań zapewnienia wiarygodności w zakresie wymaganych działań dotyczących nabycia i integracji systemu oraz dowodów wiarygodności niezbędnych do osiągnięcia pożądanego poziomu pewności, że produkt prawidłowo i skutecznie dostarczy wymaganych zabezpieczeń. • Analiza - oparta na wymaganiach prawnych, regulacyjnych, funkcjonalnych i dotyczących zabezpieczeń - zostanie wykorzystana jako podstawa do ustalenia jak silne i jakiego rodzaju gwarancje są potrzebne.
Szacowanie ryzyka[22]	• Przeprowadzenie formalnego oszacowania ryzyka w celu zidentyfikowania wymogów dotyczących ochrony systemu. Ta analiza wykorzystuje wstępne oszacowanie ryzyka przeprowadzone w fazie inicjacji, ale jest bardziej dogłębna i szczegółowa. Podczas procesu szacowania ryzyka pod uwagę brane są zazwyczaj kategorie zabezpieczeń podane w NSC 199, które są pomocne w początkowym wyborze zabezpieczeń systemu informacyjnego.
Kwestie związane z kosztami i sprawozdawczością[23]	• Ustalenie do jakiego stopnia koszt nabycia i integracji produktu można przypisać do bezpieczeństwa informacji w całym cyklu życia systemu. Wśród kosztów tych mogą być sprzęt komputerowy, oprogramowanie, personel i szkolenia.

[22] Dodatkowe wytyczne w zakresie szacowania ryzyka, zob. NSC 800-30, a także Rozdział 10 „Zarządzanie ryzykiem" i Rozdział 11 „Certyfikacja, akredytacja i oceny bezpieczeństwa" niniejszego podręcznika.

[23] Dodatkowe wytyczne w zakresie kwestii kosztów i sprawozdawczości, zob. NIST SP 800-65, *Integrating Security into the Capital Planning Process and Investment and Control Process*, a także Rozdział 5 „Planowanie finansowe i kontrola inwestycji" niniejszego podręcznika.

Działania SDLC	Działania i definicje dotyczące bezpieczeństwa
Planowanie bezpieczeństwa[24]	• Pełne udokumentowanie uzgodnionych zabezpieczeń (planowanych lub wdrożonych). • Opracowanie planu bezpieczeństwa systemu. • Opracowanie dokumentów wspierających organizacyjny program bezpieczeństwa informacji (np. plan CM[25], plan awaryjny, plan reagowania na incydenty, plan uświadamiania i szkolenia w zakresie bezpieczeństwa, zasady zachowania, oszacowanie ryzyka, wyniki testów i oceny bezpieczeństwa, umowy o połączeniu systemów, autoryzacje/akredytacje bezpieczeństwa oraz plany i etapy działania [POA&M]). • Opracowanie wymagań dotyczących uświadamiania i szkolenia, w tym w zakresie podręczników użytkownika i podręczników operacyjnych/administracyjnych.
Opracowanie środków bezpieczeństwa[26]	• Opracowanie, zaprojektowanie i wdrożenie zabezpieczeń opisanych w odpowiednich planach bezpieczeństwa. • W przypadku już eksploatowanych systemów informacyjnych, będą to plany bezpieczeństwa dla systemów, które mogą wymagać opracowania dodatkowych zabezpieczeń uzupełniających zabezpieczenia już wdrożone albo dla systemów wymagających modyfikacji wybranych zabezpieczeń, które uznano za niewystarczająco skuteczne.

[24] Dodatkowe wytyczne w zakresie kwestii kosztów i sprawozdawczości, zob. NSC 800-18; NIST SP 800-65, *Integrating Security into the Capital Planning Process and Investment and Control Process*, a także Rozdział 5 „Planowanie finansowe i kontrola inwestycji" niniejszego podręcznika, a w zakresie planowania bezpieczeństwa - Rozdział 8 „Planowanie bezpieczeństwa" niniejszego podręcznika.

[25] Plan zarządzania konfiguracją - zbiór działań ukierunkowanych na ustanowienie i utrzymanie integralności produktów i systemów informacyjnych, poprzez kontrolę procesów inicjowania, zmiany i monitorowania konfiguracji tych produktów i systemów w całym cyklu życia systemu.

[26] Dodatkowe wytyczne w zakresie opracowywanie środków bezpieczeństwa, zob. NSC 200 oraz NSC 800-53.

Działania SDLC	Działania i definicje dotyczące bezpieczeństwa
Testy rozwojowe i ocena bezpieczeństwa	• Przetestowanie zabezpieczeń opracowanych dla nowego systemu informacyjnego lub produktu w celu zapewnienia właściwego i skutecznego działania. Niektórych rodzajów zabezpieczeń (głównie o charakterze nietechnicznym) nie można przetestować ani ocenić, dopóki system informacyjny nie zostanie uruchomiony. Należą do nich zazwyczaj zabezpieczenia zarządcze i operacyjne. • Opracowanie planu/konspektu/scenariuszy testów.
Pozostałe komponenty planowania	• Zapewnienie, aby podczas włączania bezpieczeństwa do cyklu życia uwzględniono wszystkie niezbędne komponenty procesu nabycia i integracji produktu. Do komponentów tych należą: wybór odpowiedniego rodzaju umowy, zaangażowanie wszystkich niezbędnych grup funkcjonalnych z organizacji, uczestnictwo osoby certyfikującej akredytującej, a także opracowanie i wykonanie niezbędnych planów i procesów kontraktowania.
C. Faza wdrożenia	
Test i ocena bezpieczeństwa	• Opracowanie danych testowych. • Przetestowanie jednostki, podsystemu i całego systemu. • Zapewnienie, aby system przeszedł ocenę techniczną (zgodnie z przepisami regulacjami, politykami, wytycznymi i standardami).
Inspekcja i akceptacja	• Weryfikacja i walidacja, czy opisana w specyfikacji funkcjonalność została dostarczona.
Integracja/instalacja systemu	• Integracja systemu w obiekcie operacyjnym, w którym ma pracować. Włączenie ustawień i przełączników zabezpieczeń zgodnie z instrukcjami dostawcy i odpowiednimi wytycznymi.
Certyfikacja	• Zapewnienie skutecznego wdrożenia zabezpieczeń przy zastosowaniu ustanowionych technik i procedur weryfikacji oraz zapewnienie kierownictwa, że wdrożono odpowiednie

Działania SDLC	Działania i definicje dotyczące bezpieczeństwa
Bezpieczeństwa[27]	środki bezpieczeństwa i przeciwdziałania chroniące informacje organizacji. • Dodatkowo, certyfikacja bezpieczeństwa ujawnia i opisuje znane podatności systemu informacyjnego. Może wystąpić konieczność aktualizacji istniejącej certyfikacji bezpieczeństwa w przypadku wprowadzenia nowych produktów. Publikacja NSC 800-37 stwierdza stopień, w jakim zabezpieczenia systemu informacyjnego zostały wdrożone prawidłowo, działają zgodnie z zamierzeniem i dają pożądany wynik w zakresie spełnienia wymagań bezpieczeństwa dotyczących systemu.
Akredytacja Bezpieczeństwa[28]	• Udzielenie niezbędnej autoryzacji bezpieczeństwa systemu informacyjnego pozwalające mu na przetwarzanie, przechowywanie lub przesyłanie wymaganych informacji. Ta autoryzacja jest udzielana przez członka wyższego kierownictwa organizacji w oparciu o zweryfikowaną skuteczność zabezpieczeń na uzgodnionym poziomie wiarygodności oraz zidentyfikowane ryzyko szczątkowe dla aktywów i operacji organizacji. W procesie tym ustalane jest, czy poziom ryzyka dla operacji, aktywów i personelu organizacji stwarzany przez istniejące znane podatności systemu informacyjnego jest na akceptowalnym poziomie. Po udanym zakończeniu tej fazy, właściciele systemu otrzymują zezwolenie do działania, tymczasowe zezwolenie do działania lub odmowę zezwolenia do działania systemu informacyjnego.

27 Dodatkowe wytyczne w zakresie certyfikacji bezpieczeństwa, zob. NSC 800-37, a także Rozdział 11 „Certyfikacja, akredytacja i oceny bezpieczeństwa" niniejszego podręcznika.

28 Tamże.

Działania SDLC	Działania i definicje dotyczące bezpieczeństwa
D. Faza eksploatacji/utrzymania	
Zarządzanie konfiguracją i zabezpieczenia konfiguracyjne[29]	• Zapewnienie odpowiedniego uwzględnienia potencjalnego wpływu zmian systemu informacyjnego lub jego środowiska na bezpieczeństwo systemu. CM oraz procedury kontroli konfiguracji mają krytyczne znaczenie dla ustanowienia wstępnego poziomu bazowego dla sprzętu komputerowego, oprogramowania i oprogramowania układowego systemu informacyjnego oraz późniejszej kontroli i ewidencji wszelkich zmian w systemie. • Opracowanie planu CM: ✓ ustanowienie poziomów bazowych, ✓ określenie konfiguracji, ✓ opisanie procesu kontroli konfiguracji, ✓ ustalenie harmonogramu audytów konfiguracji.
Ciągłe monitorowanie	• Monitorowanie zabezpieczeń w celu zapewnienia ich skuteczności poprzez okresowe testy i oceny. Monitorowanie zabezpieczeń (tzn. weryfikacja ciągłej skuteczności ich działania) oraz przekazywanie sprawozdań o stanie bezpieczeństwa systemu informacyjnego do odpowiednich osób w organizacji to niezbędne działania w kompleksowym programie bezpieczeństwa informacji. Monitorowanie w celu zapewnienia funkcjonowania zabezpieczeń zgodnie z wymaganiami. • Okresowe przeprowadzanie samodzielnie zarządzonych lub niezależnych audytów lub innych ocen. Rodzaje: użycie zautomatyzowanych narzędzi, audyty kontroli wewnętrznej, listy kontrolne bezpieczeństwa i testy penetracyjne. • Monitorowanie systemu i/lub użytkowników. Metody: przegląd dzienników i raportów systemowych, użycie zautomatyzowanych narzędzi, przegląd zarządzania zmianami,

[29] Dodatkowe wytyczne w zakresie zarządzania konfiguracją i zabezpieczeń konfiguracyjnych, zob. Rozdział 14 *„Zarządzanie konfiguracją”* niniejszego podręcznika.

Działania SDLC	Działania i definicje dotyczące bezpieczeństwa
	monitorowanie źródeł zewnętrznych (literatura branżowa, publikacje, wiadomości elektroniczne itp.) oraz okresowe przeprowadzanie ponownej akredytacji. ✓ POA&M ✓ pomiary i metryki ✓ monitoring sieci
E. Faza wycofania:	
Przechowywanie informacji	• Zachowanie informacji (w razie konieczności) w celu spełnienia wymagań prawnych i uwzględnienie przyszłych zmian technologicznych mogących uczynić metodę ich odzyskania przestarzałą. • Zapewnienie retencji i archiwizacji dokumentów. • Zapewnienie długoterminowego przechowywania kluczy kryptograficznych do zaszyfrowanych danych. • Ustalenie czy informacje należy usunąć, zarchiwizować czy zniszczyć.
Sanityzacja nośników	• Ustalenie poziomu sanityzacji (nadpisanie, demagnetyzacja lub zniszczenie). • Wykasowanie, wymazanie lub nadpisanie danych zgodnie z wymaganiami.
Utylizacja sprzętu komputerowego i oprogramowania	• Utylizacja sprzętu komputerowego i oprogramowania zgodnie z obowiązującą polityką organizacji.

REFERENCJE:

Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

Federal Information Processing Standard 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

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

National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information System*, May 2004.

National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005.

National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.

National Institute of Standards and Technology Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle*, Rev. 1, June 2004.

National Institute of Standards and Technology Special Publication 800-65, *Integrating Security into the Capital Planning and Investment Control Process*, January 2005.

National Institute of Standards and Technology Special Publication 800-88, *Guidelines for Media Sanitization*, September 2006.

ROZDZIAŁ 4

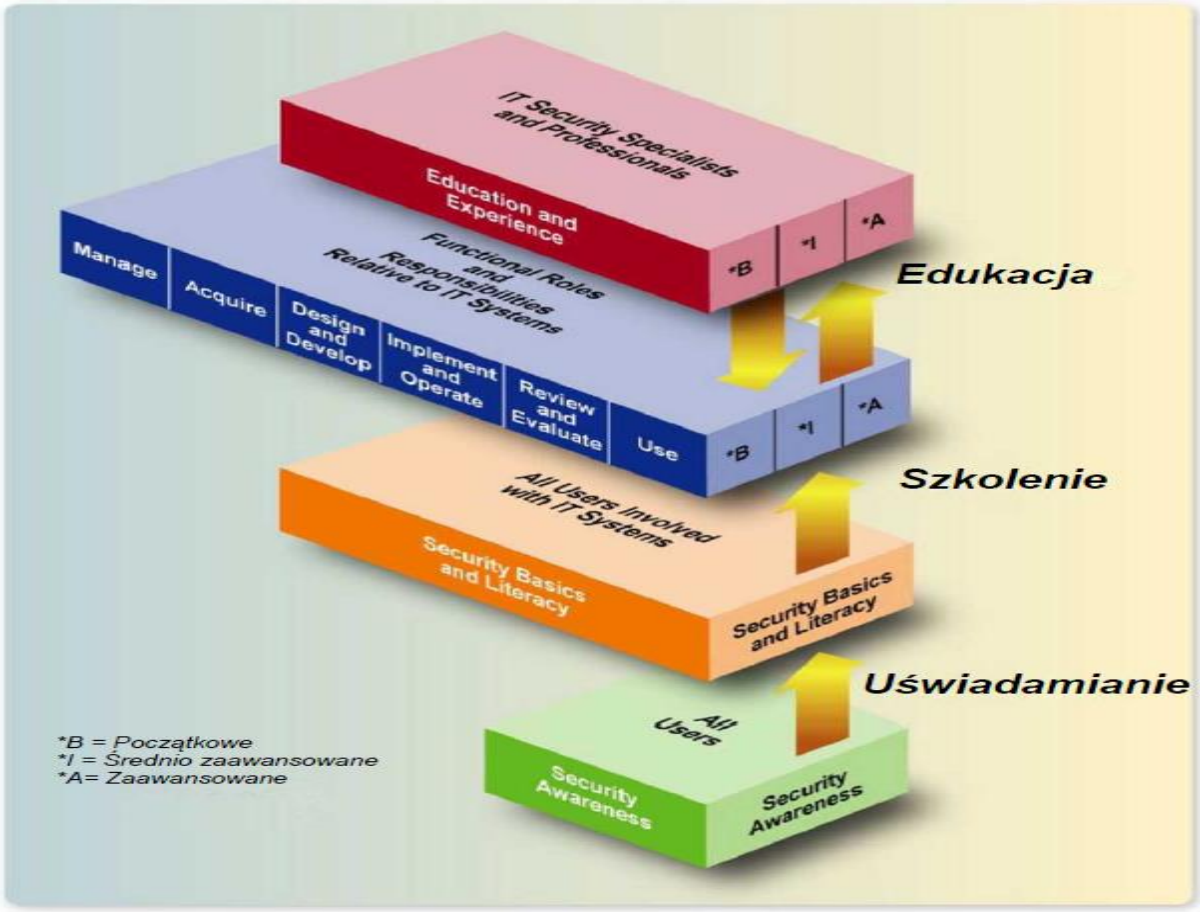
4. UŚWIADAMIANIE I SZKOLENIE

Program uświadamiania i szkolenia w zakresie bezpieczeństwa jest kluczowym komponentem programu bezpieczeństwa informacji. Jest on narzędziem do podnoszenia kompetencji na temat bezpieczeństwa, których personel, w tym kierownictwo, potrzebuje do wykonywania swoich obowiązków. Jeżeli chodzi o całościowe rozwiązanie w zakresie bezpieczeństwa, znaczenie personelu dla realizacji celów bezpieczeństwa informacji oraz waga szkoleń jako środka przeciwdziałania są nie do przecenienia. Ustanowienie i utrzymanie solidnej i odpowiedniej świadomości bezpieczeństwa informacji oraz programu szkoleń w tym zakresie, w ramach ogólnego programu bezpieczeństwa informacji, to główny kanał udzielania personelowi informacji i narzędzi potrzebnych do ochrony żywotnych zasobów informacyjnych organizacji. Programy te zapewnią, że personel na wszystkich poziomach organizacji będzie rozumieć spoczywające na nim obowiązki z zakresu bezpieczeństwa informacji dotyczące właściwego używania i ochrony informacji oraz powierzonych mu zasobów. Organizacje, które nieprzerwanie szkolą swój personel w powyższym zakresie oraz obowiązków dotyczących bezpieczeństwa opartych na podziale ról będą bardziej skuteczne w ochronie informacji.

Według sprawozdań z audytów, czasopism i publikacji, ludzie niewątpliwie stanowią najsłabszy element bezpieczeństwa systemów i sieci. To czynnik ludzki, a nie technologia, jest kluczowym wyznacznikiem często niezauważanym w kontekście bezpieczeństwa. Z tego właśnie powodu należy poświęcić więcej uwagi działaniom uświadamiającym i szkoleniom opartym na podziale obowiązków, ponieważ stanowią one jedyne zabezpieczenia mogące zminimalizować nieodłączne ryzyko związane z ludźmi, którzy używają, zarządzają, obsługują i utrzymują systemy i sieci informacyjne. Aby rozwiązać ten coraz poważniejszy problem potrzebne są kompleksowe programy uświadamiające i szkoleniowe realizowane na poziomie całej organizacji.

Publikacja specjalna NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, zawiera wskazówki, które mogą pomóc organizacjom spełnić spoczywające na nich obowiązki uświadamiania i szkolenia w zakresie bezpieczeństwa informacji. Publikacja ta określa modele budowania i utrzymywania kompleksowego programu uświadamiania i szkolenia w ramach realizowanego przez organizację programu bezpieczeństwa informacji.

NIST SP 800-50 to publikacja towarzysząca dokumentowi NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*. Publikacja NIST SP 800-50 osadzona jest na wyższym poziomie strategicznym i omawia sposoby budowania i utrzymywania programu uświadamiania i szkolenia w zakresie bezpieczeństwa informacji. Publikacja NIST SP 800-16 dotyczy poziomu taktycznego i omawia kontinuum uświadamianie-szkolenie-edukacja, szkolenie oparte na podziale ról oraz kwestie związane z treścią kursów. Kontinuum uczenia się przedstawiono na rys. 4-1.



Rysunek 4-1. Kontinuum uczenia się w zakresie bezpieczeństwa IT

Legenda do rysunku 4-1.

IT Security Specialists and Professionals	Specjaliści i profesjonaliści zawodowo zajmujący się bezpieczeństwem IT
Education and Experience	Edukacja i doświadczenie
Functional Roles and Responsibilities Relative to IT System	Role i obowiązki funkcjonalne dotyczące systemu IT
Manage	Zarządzanie
Acquire	Nabycie
Design and Develop	Zaprojektowanie i rozwój
Implement and Operate	Wdrożenie i eksploatacja
Review and Evaluate	Przegląd i ocena
Use	Użytkowanie
All Users Involved with IT Systems	Wszyscy użytkownicy systemów IT
Security Basics and Literacy	Podstawy bezpieczeństwa i umiejętność obsługi
All Users	Wszyscy użytkownicy
Security Awareness	Świadomość bezpieczeństwa

4.1. POLITYKA UŚWIADAMIANIA I SZKOLENIA

Wszyscy użytkownicy mają obowiązki w zakresie bezpieczeństwa informacji. Wszyscy użytkownicy muszą ukończyć „szkolenie uświadamiające" (*ang. awareness training*). Organizacje mają również zadanie zidentyfikowania i przeszkolenia osób, które mają znaczące obowiązki w zakresie bezpieczeństwa informacji, dotyczące uświadamiania i szkolenia w zakresie bezpieczeństwa informacji. Należy kłaść nacisk na wymóg wśród

użytkowników na „szkolenia uświadamiające" przeprowadzając co najmniej raz w roku „szkolenia specyficzne dla roli". Chociaż nie ma wymogu dotyczącego formalnego kształcenia (prowadzonego przez uczelnie wyższe) i certyfikacji osób zawodowo zajmujących się bezpieczeństwem informacji, zostały one poruszone w niniejszym rozdziale, ponieważ niektóre organizacje uwzględniają je w kompleksowym szkoleniu personelu.

4.2. KOMPONENTY: ŚWIADOMOŚĆ, SZKOLENIE, EDUKACJA I CERTYFIKACJA

Polityka organizacji dotycząca programu bezpieczeństwa informacji powinna zawierać oddzielny rozdział poświęcony wymaganiom w zakresie programu uświadamiania i szkolenia realizowanego w całej organizacji. Chociaż w odniesieniu do uświadamiania i szkolenia w zakresie bezpieczeństwa informacji zazwyczaj używa się pojęcia „program" w liczbie pojedynczej, wiele organizacji uważa uświadamianie i szkolenie za dwie różne funkcje, z których każda kieruje się oddzielnymi zamiarami, celami i podejściem. Właściwa realizacja tych komponentów (z uwzględnieniem takich możliwości jak kształcenie i certyfikacja zawodowa) przyczynia się do rozwoju zawodowego, co prowadzi do wysokiej wydajności pracy.

Wymagania dotyczące programu uświadamiania i szkolenia w zakresie bezpieczeństwa informacji powinny zostać udokumentowane w polityce realizowanej na poziomie całej organizacji i powinny obejmować:

- określenie ról i obowiązków związanych z bezpieczeństwem;
- opracowanie strategii programowej i planu programu;
- realizację planu programu;
- utrzymanie programu uświadamiania i szkolenia w zakresie bezpieczeństwa[30].

4.2.1. ŚWIADOMOŚĆ

Świadomość w zakresie bezpieczeństwa łączy działania promujące bezpieczeństwo, ustanawiające rozliczalność i dostarczające personelowi nowych wiadomości

[30] Dla zainteresowanych – patrz: NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*.

o bezpieczeństwie. Program uświadamiający ma na celu skupienie uwagi jednostki na zagadnieniu lub zbiorze zagadnień. To program, który w sposób ciągły i w różnych formatach dociera do użytkowników z przekazem dotyczącym bezpieczeństwa.

Program uświadamiania obejmuje różne narzędzia, komunikację i popularyzację oraz metryki rozwoju.

- **Narzędzia.** Narzędzia uświadamiania są używane do promowania bezpieczeństwa informacji i informowania użytkowników o zagrożeniach i podatnościach mających wpływ na ich organizację i „osobiste" środowisko pracy poprzez wyjaśnianie „czym" jest bezpieczeństwo (ale nie „jak" działa), a także informowanie o tym, co jest dozwolone, a co zabronione. Uświadamianie nie tylko komunikuje zasady i procedury bezpieczeństwa informacji, których należy przestrzegać, ale też zapewnia fundament dla sankcji i działań dyscyplinarnych w przypadku niezgodności. Uświadamianie służy wyjaśnianiu zasad zachowania podczas korzystania z informacji i systemów informacyjnych organizacji oraz ustala poziom oczekiwań dotyczących akceptowalnego użycia tych informacji i systemów.

  Rodzaje narzędzi to:

  - ✓ wydarzenia, takie jak dzień świadomości bezpieczeństwa,
  - ✓ materiały edukacyjne,
  - ✓ odprawy (dotyczące programu, systemu lub zagadnienia),
  - ✓ zasady zachowania.

- **Komunikacja.** Dużą część działań na rzecz uświadamiania stanowi komunikacja z użytkownikami, osobami zarządzającymi, kierownictwem wysokiego szczebla, właścicielami systemów i innymi podmiotami. Plan komunikacji jest niezbędny do zidentyfikowania interesariuszy, rodzajów informacji do rozpowszechnienia, kanałów rozpowszechniania informacji oraz częstotliwości wymiany informacji. Plan określa również, czy komunikacja jest jedno, czy dwukierunkowa. Działania wspierające komunikację to:

- ✓ ocena (modele jak jest/jak ma być),
- ✓ plan strategiczny,
- ✓ realizacja programu.

- **Popularyzacja.** Popularyzacja jest kluczowa dla wzmocnienia najlepszych praktyk w obrębie sektora publicznego i prywatnego. Składają się na nią dwa elementy uświadamiające: wewnątrzorganizacyjny i międzyorganizacyjny. Element wewnątrzorganizacyjny promuje świadomość wewnętrzną w zakresie bezpieczeństwa informacji. Skutecznym działaniem popularyzującym może być portal internetowy będący kompleksowym źródłem informacji o bezpieczeństwie. Zasady, najczęściej zadawane pytania (*ang. Frequently Asked Questions, FAQ*) elektroniczne biuletyny poświęcone bezpieczeństwu, linki do innych zasobów oraz inne przydatne informacje stają się łatwo dostępne dla wszystkich pracowników. Takie rozwiązanie promuje spójny i ustandaryzowany przekaz. Element międzyorganizacyjny promuje wymianę między organizacjami i służy do podnoszenia świadomości i zwiększania zasobów szkoleniowych.

4.2.2. SZKOLENIE

Szkolenie w zakresie bezpieczeństwa informacji ma za zadanie wykształcić w personelu odpowiednią i potrzebną wiedzę oraz umiejętności. Szkolenie wspiera rozwój kompetencji i pomaga personelowi zrozumieć i nauczyć się w jaki sposób należy pełnić role związane z bezpieczeństwem. Najważniejszą różnicą między szkoleniem i uświadamianiem jest to, że szkolenie ma na celu nauczenie umiejętności, które pozwalają danej osobie na pełnienie konkretnej funkcji, a celem uświadamiania jest skupienie uwagi osoby na zagadnieniu lub zbiorze zagadnień.

Szkolenia oparte na podziale ról zapewniają kursy bezpieczeństwa dostosowane do konkretnych potrzeb każdej grupy osób, które zidentyfikowano jako osoby pełniące w organizacji znaczące obowiązki w zakresie bezpieczeństwa informacji[31].

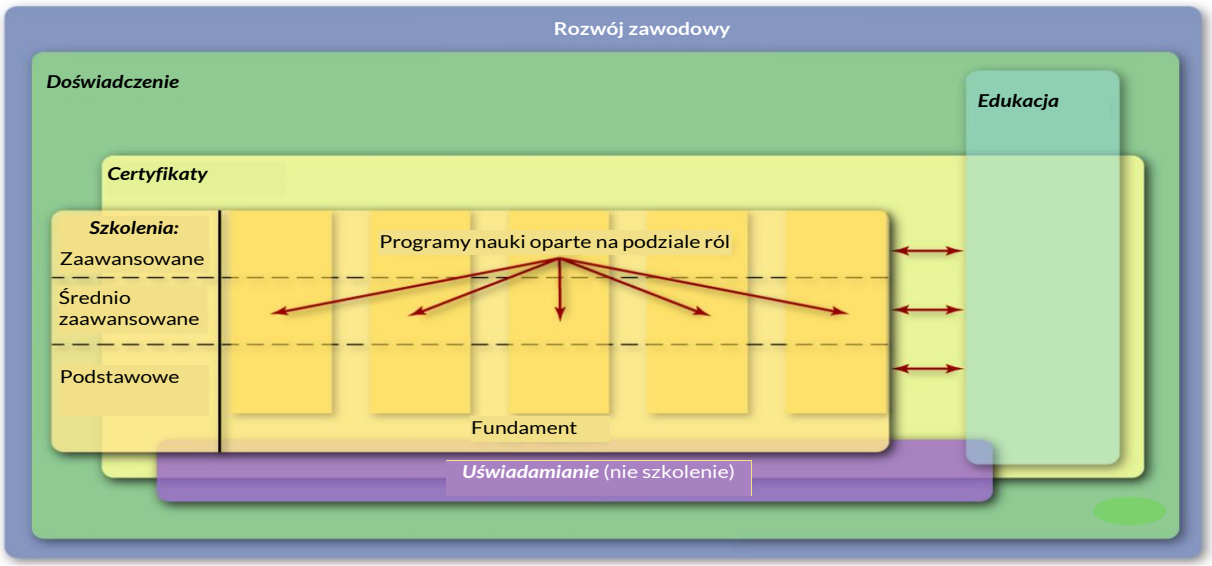
[31] Dla zainteresowanych - wskazówki dotyczące ustanawiania programów szkolenia opartych na podziale ról i działań przedstawiono w publikacji NIST SP 800-16.

4.2.3. EDUKACJA

Edukacja integruje wszystkie umiejętności i kompetencje związane z bezpieczeństwem właściwe dla różnych specjalizacji w jeden zasób wiedzy, dodając do niego multidyscyplinarne studia o koncepcjach, zagadnieniach i zasadach (technologicznych i społecznych). Edukacja w zakresie bezpieczeństwa informacji dąży do wykształcenia specjalistów i osób zawodowo zajmujących się bezpieczeństwem informacji posiadających wizję i zdolność aktywnego reagowania. Niektóre uczelnie wyższe prowadzą programy akademickie wspierające potrzeby dotyczące bezpieczeństwa informacji, które występują w sektorze publicznym i prywatnym. Wiele z tych uczelni zawarło partnerstwo z sektorem publicznym w celu realizacji zadań badawczo-rozwojowych mających poprawić bezpieczeństwo informacji.

4.2.4. CERTYFIKACJA

W odpowiedzi na rosnące zapotrzebowanie na personel zajmujący się bezpieczeństwem informacji w organizacjach, zaczęto skłaniać się ku wyższym standardom zawodowym wśród pracowników i kontraktowego personelu bezpieczeństwa. Taka „profesjonalizacja" integruje szkolenie, edukację i doświadczenie z mechanizmem oceny mającym potwierdzić zdobytą wiedzę i umiejętności, co prowadzi do „certyfikacji" uprzednio określonego poziomu kompetencji. Związek między powyższymi elementami rozwoju zawodowego przedstawiono na rys. 4-2.



Rysunek 4-2. Elementy rozwoju zawodowego

Należy zauważyć, że istnieją wyraźne różnice między certyfikatami oferowanymi przez różne organizacje. Można spotkać się przede wszystkim z certyfikatami ukończenia szkolenia, certyfikatami nadawanymi przez podmioty branżowe i/lub dostawców, a także świadectwami nauki nadawanymi przez instytucje akademickie:

- **Certyfikat ukończenia szkolenia** jest nadawany osobie wyłącznie dla potwierdzenia, że ukończyła ona kurs—nie stwierdza on, czy dana osoba faktycznie nabyła wiedzę i/lub umiejętności.
- **Certyfikaty nadawane przez podmioty branżowe i/lub dostawców** wymagają solidnego połączenia wyszkolenia, wykształcenia i doświadczenia. Posiadanie wiedzy i umiejętności jest potwierdzane w procesie walidacji. Certyfikaty takie oferują różny stopień pewności co do tego, że dana osoba posiadła podstawową wiedzę, umiejętności i zdolności (*ang. Knowledge, Skills, and Abilities - KSA*) z zakresu objętego szkoleniem. Przygotowanie do uzyskania certyfikatu potwierdzającego posiadanie wiedzy lub umiejętności zazwyczaj obejmuje udział w szkoleniu z określonego zakresu wiedzy lub programu nauczania technicznego i jest często uzupełniane przez zajęcia praktyczne.
- **Świadectwa nauki** w zakresie bezpieczeństwa informacji są nadawane przez instytucje akademickie osobom, które spełniły wszystkie wymagania dotyczące określonego programu nauczania. Do uzyskania tych świadectw zazwyczaj wymagane jest zaliczenie odpowiedniej liczby godzin zajęć, ukończenie co najmniej czterech przedmiotów (z możliwością wyboru jednego lub dwóch dodatkowych) oraz może być wymagane napisania pracy badawczej, projektu lub studium przypadku.

4.3. ZAPROJEKTOWANIE, OPRACOWANIE I WDROŻENIE PROGRAMU UŚWIADAMIANIA I SZKOLENIA

Opracowanie programu uświadamiania i szkolenia w zakresie bezpieczeństwa informacji obejmuje trzy główne etapy:

1. *Zaprojektowanie* programu (łącznie z opracowaniem planu programu uświadamiania i szkolenia w zakresie bezpieczeństwa informacji).

2. O*pracowanie* materiału uświadamiającego i szkoleniowego.

3. *Wdrożenie* programu.

Nawet tylko podstawowe programy świadomości i szkolenia w zakresie bezpieczeństwa informacji mogą w znaczący sposób poprawić stan bezpieczeństwa i zachowania organizacji.

4.3.1. ZAPROJEKTOWANIE PROGRAMU UŚWIADAMIANIA I SZKOLENIA

Programy uświadamiania i szkolenia należy projektować z myślą o misji danej organizacji i musi wspierać potrzeby biznesowe organizacji oraz odpowiadać jej kulturze i architekturze technologii informatycznej. Najbardziej udane programy to takie, które w odczuciu użytkowników są istotne dla przedmiotu i prezentowanych zagadnień.

Zaprojektowanie programu uświadamiania i szkolenia w zakresie bezpieczeństwa informacji odpowiada na pytanie „Jaki mamy plan rozwoju i wykorzystania możliwości uświadamiania i szkolenia zgodnie z obowiązującymi dyrektywami?". Na etapie projektowania programu, potrzeby organizacji w zakresie uświadamiania i szkolenia zostają zidentyfikowane, wdrożony zostaje ogólnoorganizacyjny plan uświadamiania i szkolenia, poszukiwane i zabezpieczone zostaje wsparcie organizacyjne i ustanowione zostają priorytety.

4.3.2. OPRACOWANIE PROGRAMU UŚWIADAMIANIA I SZKOLENIA

Po zaprojektowaniu programu uświadamiania i szkolenia, można przystąpić do opracowywania materiału pomocniczego. Należy to zrobić mając na uwadze następujące pytania:

- „Jakie zachowanie chcemy wzmocnić?" (świadomość)
- „Jakie umiejętności mają przyswoić i stosować adresaci programu?" (szkolenie i edukacja)

W obydwu przypadkach należy skupić się na konkretnym materiale, który uczestnicy powinni włączyć do swojej pracy. Uczestnicy zwrócą uwagę i przyswoją to, co zobaczą lub usłyszą podczas szkolenia, jeżeli poczują, że materiał został przygotowany

specjalnie z myślą o nich. Każda prezentacja, która jest tak bardzo bezosobowa i ogólna, że mogłaby zostać przedstawiona dowolnej publiczności zostanie odłożona na półkę jako sesja z gatunku „zebraliśmy się tutaj, bo musieliśmy". Program uświadamiania i szkolenia jest skuteczny, jeżeli prezentowany materiał jest interesujący, aktualny i istotny.

Wśród adresatów muszą znaleźć się wszyscy użytkownicy z danej organizacji. Mogą wśród nich być pracownicy, wykonawcy kontraktowi, zaproszeni badacze z kraju i zagranicy, pozostały personel organizacji, osoby odwiedzające, goście oraz inni współpracownicy i wspólnicy potrzebujący dostępu do edukacji. Przekaz rozpowszechniany przez program lub kampanię uświadamiającą powinien uświadamiać wszystkim osobom spoczywające na nich wspólne obowiązki w zakresie bezpieczeństwa informacji.

Z drugiej strony, przekaz kierowany do odbiorców sali szkoleniowej jest przeznaczony dla konkretnej publiczności. Przekaz zawarty w materiale szkoleniowym powinien zawierać wszystko, co w związku z bezpieczeństwem muszą wiedzieć uczestnicy, aby móc wypełniać swoje obowiązki. Materiał szkoleniowy jest zwykle bardziej szczegółowy niż materiał używany w sesjach lub kampaniach uświadamiających.

4.3.3. WDROŻENIE PROGRAMU UŚWIADAMIANIA I SZKOLENIA

Program uświadamiania i szkolenia w zakresie bezpieczeństwa informacji powinien zostać wdrożony dopiero po ocenie potrzeb, opracowaniu strategii, ukończeniu planu programu uświadamiania i szkolenia służącego realizacji strategii oraz po przygotowaniu materiału uświadamiającego i szkoleniowego.

Wdrożenie programu musi zostać w pełni wyjaśnione organizacji, aby można było uzyskać wsparcie dla jego realizacji oraz zaangażowanie niezbędnych zasobów.

Wspomniane wyjaśnienie powinno objąć oczekiwania kierownictwa organizacji i wsparcie ze strony personelu, a także spodziewanego wyniku programu i korzyści dla organizacji. Należy również poruszyć kwestię finansowania. Przykładowo kierownictwo organizacji musi wiedzieć, czy koszt wdrożenia programu uświadamiania i szkolenia zostanie w całości pokryty z budżetu CIO lub budżetu programu bezpieczeństwa informacji, czy też do pokrycia wdrożenia programu trzeba będzie

zaangażować budżet kierownictwa. Konieczne jest, aby wszystkie osoby zaangażowane we wdrażanie programu rozumiały swoje role i obowiązki. Ponadto, należy zakomunikować harmonogramy i wymagania związane z realizacją programu.

Po wyjaśnieniu kierownictwu (i zaakceptowaniu przez nie) planu wdrożenia programu uświadamiania i szkolenia, można przystąpić do implementacji. Ponieważ materiał uświadamiający i szkoleniowy można rozpowszechniać w organizacji na kilka sposobów, organizacje powinny dopasować wdrożenie do swojego rozmiaru, struktury i stopnia złożoności[32].

4.4. DZIAŁANIA PO WDROŻENIU

Realizowany przez organizację program uświadamiania i szkolenia może szybko stać się przestarzały bez zwrócenia wystarczającej uwagi na rozwój technologii, zmiany w infrastrukturze IT, zmiany w organizacji czy przesunięcia dotyczące misji lub priorytetów. CIO i SAISO muszą być świadomi tego potencjalnego problemu i wdrożyć do swoich strategii mechanizmy zapewniające ciągłą istotność i zgodność programu z ogólnymi celami. Ciągłe doskonalenie powinno być stałym tematem inicjatyw dotyczących uświadamiania i szkolenia, ponieważ jest to jeden z obszarów, gdzie „zawsze jest coś do roboty". Wysiłki wspierające tę pętlę zwrotną po wdrożeniu programu powinny być czynione z uwzględnieniem realizowanego przez organizację ogólnego programu miar wyników[33].

4.4.1. MONITOROWANIE ZGODNOŚCI

Po wdrożeniu programu należy uruchomić procesy monitorowania zgodności i skuteczności. Należy wyznaczyć zautomatyzowany system śledzący, który będzie wychwytywał kluczowe informacje o działaniu programu (np. kursy, daty, publiczność, koszty, źródła). Ponieważ system śledzący powinien wychwytywać te dane na poziomie organizacji, może on umożliwiać ogólnoorganizacyjną analizę i sprawozdawczość w zakresie inicjatyw dotyczących uświadamiania, szkolenia i edukacji.

---

[32] Techniki dostarczania materiałów uświadamiających i szkoleniowych, zob. NIST SP 800-50.

[33] Dodatkowe wytyczne w zakresie pomiarów i metryk, zob. NIST SP 800-55, *Security Metrics Guide for Information Technology Systems*, a także Rozdział 7 „Miary wyników" niniejszego podręcznika.

Śledzenie zgodności polega na ocenie statusu programu w oparciu o informacje z bazy danych pod kontem standardów ustanowionych przez organizację. Do identyfikacji niedociągnięć lub problemów służą sprawozdania. Na ich podstawie można podejmować działania naprawcze i niezbędne czynności końcowe. Czynności te mogą mieć postać formalnych przypomnień dla kierownictwa, dodatkowej oferty w zakresie uświadamiania, szkolenia lub edukacji i/lub ustanowienia planu naprawczego z harmonogramem realizacji.

4.4.2. OCENA I INFORMACJE ZWROTNE

Mechanizmy formalnej oceny i informacji zwrotnych to kluczowe komponenty każdego programu uświadamiania i szkolenia z zakresu bezpieczeństwa. Ciągłe doskonalenie nie jest możliwe bez ogólnego pojęcia o tym, jak działa obecny program. Ponadto, mechanizm informacji zwrotnych musi zostać tak zaprojektowany, aby uwzględniał cele ustanowione dla programu na początku. Po ustaleniu wymagań bazowych można przygotować i wdrożyć strategię w zakresie informacji zwrotnych. Wśród różnych mechanizmów oceny i informacji zwrotnych, których można użyć do aktualizowania planu programu uświadamiania i szkolenia są: ankiety, formularze oceny, niezależne obserwacje, sprawozdania o stanie, wywiady, grupy dyskusyjne, przemiany technologiczne i/lub analizy porównawcze.

Strategia w zakresie informacji zwrotnych powinna uwzględniać elementy dotyczące jakości, zakresu, sposobu wdrożenia (np. Internet, w siedzibie, poza siedzibą), poziomu trudności, łatwości użycia, czasu trwania sesji, istotności, aktualności i sugestii zmian.

Do informacji zwrotnych i oceny niezbędne są metryki. Mogą one być używane do:

- pomiaru skuteczności programu uświadamiania i szkolenia w zakresie bezpieczeństwa,
- udzielania informacji na potrzeby wielu wniosków o dane, które organizacja musi przedstawiać dla zachowania zgodności udzielania ważnych szacunków pokazujących postęp i identyfikujących obszary do poprawy.

4.5. ZARZĄDZANIE ZMIANĄ

Konieczne jest zapewnienie, aby program w swoim kształcie ewoluował wraz z pojawianiem się nowych technologii i związanych z nimi kwestii bezpieczeństwa. Potrzeby szkoleniowe będą się zmieniać wraz z zapotrzebowaniem na nowe umiejętności i zdolności odpowiadające nowym zmianom architektonicznym i technologicznym. Wpływ na pomysły dotyczące najlepszych sposobów projektowania rozwiązań i treści szkoleniowych może mieć również zmiana misji i/lub celów organizacji. Pojawiające się kwestie, np. dotyczące bezpieczeństwa wewnętrznego, również wpływają na charakter i zakres działań dotyczących uświadamiania i szkolenia niezbędnych dla bieżącego informowania/edukowania użytkowników o najnowszych zagrożeniach, podatnościach i środkach przeciwdziałania. Wpływ na politykę organizacji mogą mieć również nowe przepisy i orzeczenia sądów, co z kolei może wpływać na opracowywanie i/lub wdrażanie materiałów uświadamiających i szkoleniowych. W końcu, zmiany wynikające z ewolucji zasad bezpieczeństwa powinny znajdować odzwierciedlenie w materiałach uświadamiających i szkoleniowych z zakresu bezpieczeństwa.

4.6. WSKAŹNIKI SUKCESU PROGRAMU

Głównymi orędownikami uświadamiania, szkolenia, edukacji i profesjonalizacji powinni być CIO, osoby odpowiadające za program i SAISO. Zabezpieczenie infrastruktury i informacji organizacji to wysiłek zespołowy, który wymaga od zdolnych jednostek poświęcenia w realizacji przydzielonych im ról w zakresie bezpieczeństwa. Poniżej wymieniono niektóre kluczowe wskaźniki pozwalające oszacować wsparcie dla programu i jego akceptację:

- kluczowy interesariusz okazuje zaangażowanie i wsparcie;
- wystarczające środki na realizację uzgodnionej strategii uświadamiania i szkolenia zostają zabudżetowane i udostępnione;
- odpowiednie umiejscowienie organizacyjne kluczowych osób odpowiedzialnych za bezpieczeństw (CIO, osoby odpowiadające za program i SAISO) ułatwia realizację strategii;
- sfinansowanie i wdrożenie infrastruktury wspierającej szeroką dystrybucję i publikację materiałów uświadamiających i szkoleniowych w zakresie

bezpieczeństwa (np. Internet, poczta elektroniczna, systemy zarządzania nauką;

- osoby na wyższych stanowiskach kierowniczych przekazują personelowi komunikaty dotyczące bezpieczeństwa (np. spotkania z personelem, audycje szefa organizacji skierowane do wszystkich użytkowników), są orędownikami programu i okazują wsparcie dla szkolenia poprzez przeznaczanie środków na jego finansowanie;
- metryki wskazują na poprawę zachowania pracowników w zakresie bezpieczeństwa (np. spadek liczby incydentów i naruszeń bezpieczeństwa, zmniejszanie się luki między aktualnym zakresem uświadamiania i szkolenia a zidentyfikowanymi potrzebami, rosnący odsetek użytkowników mających kontakt z materiałami uświadamiającymi, rosnący odsetek odpowiednio przeszkolonych użytkowników pełniących ważne obowiązki dotyczące bezpieczeństwa);
- dyrektorzy i kierownicy nie wykorzystują swojej pozycji w organizacji do unikania środków bezpieczeństwa, które są konsekwentnie przestrzegane przez szeregowych pracowników;
- poziom uczestnictwa w forach/briefingach/szkoleniach poświęconych bezpieczeństwu jest niezmiennie wysoki;
- wyrażanie uznania za wkład w bezpieczeństwo (np. nagrody, konkursy) jest w organizacji standardową praktyką;
- osoby pełniące kluczowe role w zarządzaniu/koordynowaniu programu bezpieczeństwa wykazują zaangażowanie w program i motywację do jego promowania.

REFERENCJE:

NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance- Based Model*, April 1998.

NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003.

NIST Special Publication 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003.

ROZDZIAŁ 5

5. PLANOWANIE FINANSOWE I KONTROLA INWESTYCJI[34]

Rosnąca rywalizacja o ograniczone budżety i zasoby organizacyjne wymaga od organizacji przydzielania dostępnych środków finansowych do inwestycji w bezpieczeństwo informacji o najwyższym priorytecie w celu zapewnienia organizacji oraz jej systemom i danym stopnia bezpieczeństwa odpowiadającego jej potrzebom. Ten cel można osiągnąć poprzez realizację formalnego procesu planowania finansowego i kontroli inwestycji (*ang. Capital Planning and Investment Control - CPIC*), którego zadaniem jest ułatwienie i kontrola wydatkowania funduszy organizacji. Praktyki omówione w niniejszym rozdziale mają na celu pomoc osobom zajmującym się bezpieczeństwa i menadżerom w identyfikowaniu potrzeb w zakresie finansowania inwestycji w zabezpieczanie systemów oraz przedstawienie strategii pozyskiwania niezbędnych funduszy.

5.1. PRZEGLĄD UREGULOWAŃ PRAWNYCH

Realizacja bezpieczeństwa informacji odbywa się według zbioru przepisów, reguł i regulacji oraz polityk specyficznych dla poszczególnych organizacji. Pomocnymi dokumentami są:

- **NSC 800-53**, który określa zestaw bazowych zabezpieczeń mających zastosowanie w systemach informacyjnych w oparciu o kategoryzację podaną w NSC 199 (poziom wpływu na bezpieczeństwo informacji: niski, umiarkowany wysoki).
- **Sprawozdania** przedstawiające stan bezpieczeństwa organizacji wraz z ewentualnymi obszarami słabości[35].

[34] Informacje zawarte w rozdziale 5 odnoszą się do specyfikacji rynku amerykańskiego i zostały podane w celach poglądowych. Przy zastosowaniu tych wskazówek każdorazowo należy uwzględniać obowiązujące przepisy krajowe i regulacje wewnętrze organizacji.

[35] Dodatkowe wytyczne w zakresie sprawozdawczości, zob. Rozdział 11 „Certyfikacja, akredytacja i oceny bezpieczeństwa" niniejszego podręcznika.

- **Plan i etapy działania (*ang. Plan of Actions and Milestones, POA&M*)**, który dokumentuje słabości, związane z nimi działania naprawcze i koszty tych działań w każdej organizacji[36].

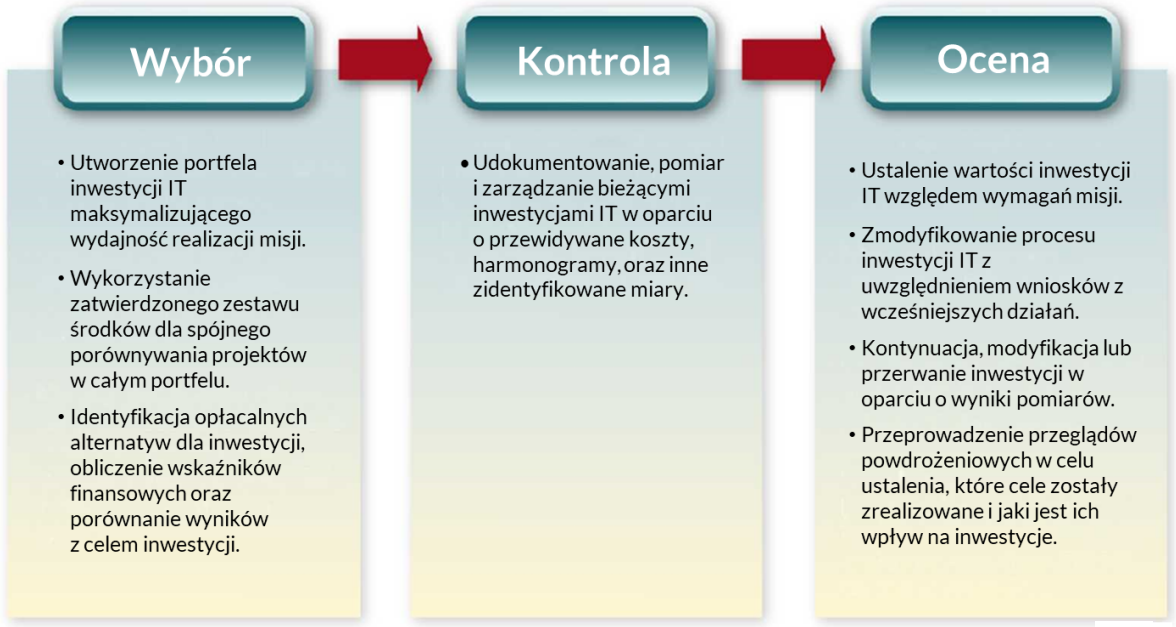
Aby ułatwić skuteczne wdrożenie wymagań w zakresie planowania finansowego oraz wymagań w zakresie bezpieczeństwa, można wykorzystać model cyklu życia inwestycji „Wybór-Kontrola-Ocena" jako najlepszą praktykę w odniesieniu do zarządzania inwestycjami. Chociaż nie jest on obowiązkowy, to artykułuje kluczowe działania dotyczące zarządzania inwestycjami IT w całym cyklu życia. Trzy fazy tego cyklu zapewniają rzetelność i dokładność praktyk zarządzania inwestycją na każdym etapie jej cyklu życia. Zostały one pokazane na rys. 5-1.

Faza wyboru odnosi się do działań realizowanych podczas oceny i ustalania priorytetów bieżących i przyszłych projektów IT w oparciu o potrzeby misji i priorytety doskonalenia; w jej wyniku powstaje portfolio projektów IT dotyczących tych potrzeb i priorytetów. Typowe działania z fazy wyboru to: selekcja nowych projektów, analizowanie i ustalanie rangi wszystkich projektów na podstawie kryteriów korzyści, kosztu i ryzyka, wybór portfela projektów oraz ustanowienie harmonogramów przeglądu projektów.

Faza kontroli odnosi się do działań, których celem jest monitorowanie inwestycji na etapie jej funkcjonowania w celu ustalenia, czy mieści się ona w przedziale kosztów i harmonogramie realizacji, które ustanowiono na początku cyklu życia inwestycji. Typowe procesy z fazy kontroli to: użycie zestawu miar wyników w celu monitorowania postępów każdego projektu IT i umożliwienia wczesnego identyfikowania i rozwiązywania problemów.

W **fazie oceny** ustalana jest skuteczność inwestycji, udzielana jest odpowiedź na pytanie „Czy inwestycja osiągnęła pożądane wyniki i cele określone w fazie wyboru?".

[36] Dodatkowe wytyczne w zakresie POA&M, zob. Rozdział 11 „Certyfikacja, akredytacja i oceny bezpieczeństwa" niniejszego podręcznika.



Rysunek 5-1. Cykl życia inwestycji „Wybór-Kontrola-Ocena"

Na rys. 5-1 pokazano relacje między kluczowymi czynnikami bezpieczeństwa w cyklu życia inwestycji „Wybór- Kontrola-Ocena" i cyklu życia systemu (*ang. System Development Life Cycle - SDLC*). Podczas fazy wyboru czynnikami takimi są działania oceniające mające zapewnić zgodność inwestycji w bezpieczeństwo IT z wymaganiami bezpieczeństwa. Podczas fazy kontroli, inwestycje są monitorowane z wykorzystaniem metryk bezpieczeństwa w celu zapewnienia, że zabezpieczenia zostały wprowadzone i działają oraz że inwestycje zachowują zgodność z wymaganiami. Podczas fazy oceny, czynniki kluczowe dla bezpieczeństwa to: działania polegające na samoocenie mające zapewnić zgodność i sanityzację nośników po wycofaniu ich z użycia i przed zbyciem.

5.2. INTEGRACJA BEZPIECZEŃSTWA INFORMACJI Z PROCESEM PLANOWANIA FINANSOWEGO I KONTROLI INWESTYCJI (CPIC)[37]

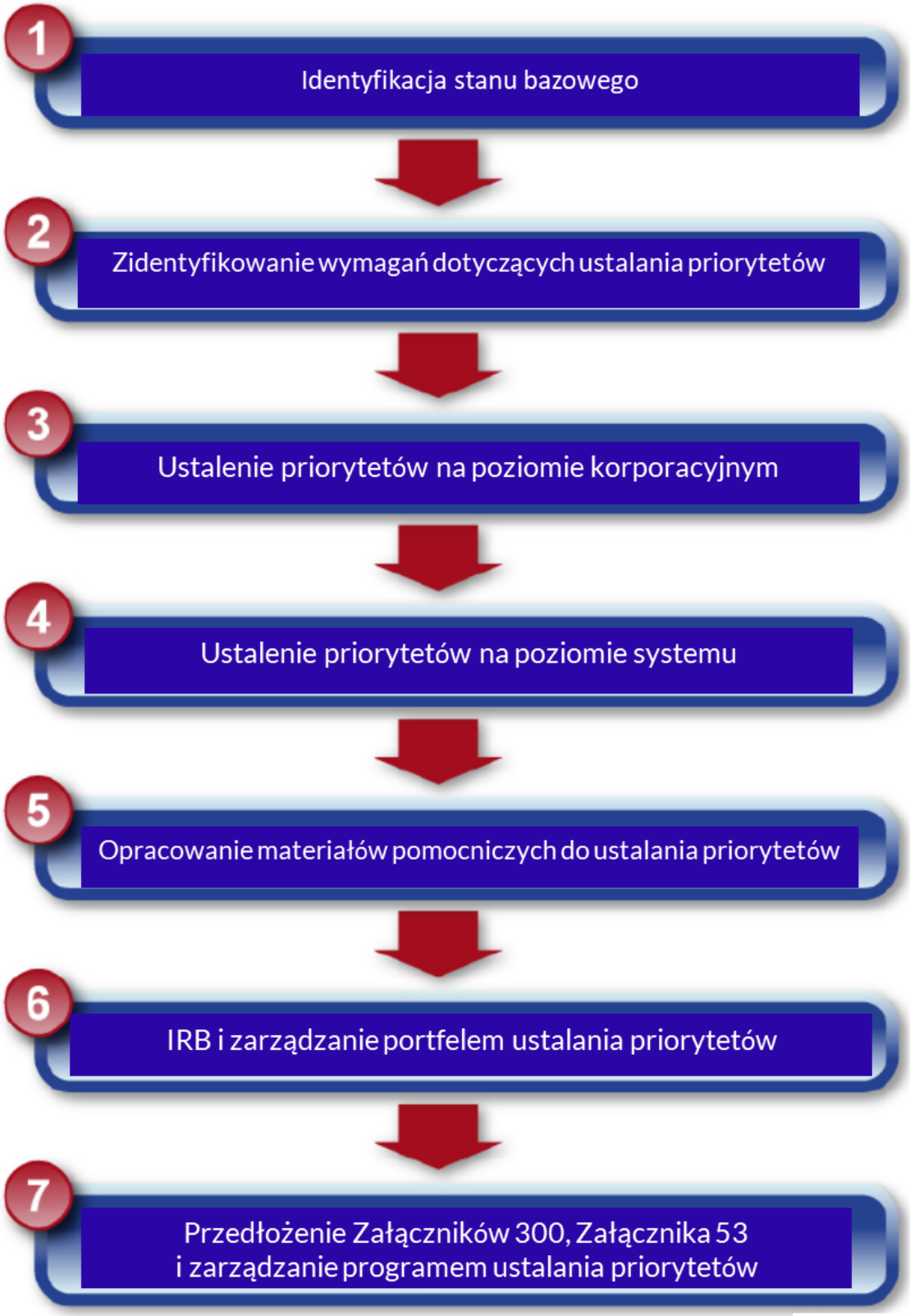
Publikacja NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, przedstawia siedmiostopniowy proces ustalania priorytetów działań związanych z bezpieczeństwem i działań naprawczych (patrz rys. 5-2):

[37] Podano w celach uzupełniających dla zainteresowanych.

1. **Identyfikacja stanu bazowego:** wykorzystanie metryk bezpieczeństwa informacji lub innych dostępnych danych do ustalenia aktualnego bazowego stanu bezpieczeństwa.
2. **Identyfikacja wymagań w zakresie nadawania priorytetów:** ocena stanu bezpieczeństwa pod kątem przepisów, sformułowanych przez CIO wymagań i misji organizacji.
3. **Ustalenie priorytetów na poziomie organizacji:** ustalenie priorytetów dla inwestycji w bezpieczeństwo informacji na poziomie organizacji w odniesieniu do misji i wpływu finansowego wdrożenia odpowiednich zabezpieczeń.
4. **Ustalenie priorytetów na poziomie systemu:** ustalenie priorytetów ewentualnych działań naprawczych na poziomie systemu w odniesieniu do kategorii systemu i wpływu działań naprawczych.
5. **Opracowanie materiałów pomocniczych:** w przypadku inwestycji na poziomie organizacji - opracowanie koncepcji, analiza uzasadnienia biznesowego i Załącznik 300[38]. W przypadku inwestycji na poziomie systemu – dostosowanie Załącznika 300 tak, aby wnioskować o dodatkowe fundusze na ograniczenie słabości objętych priorytetem.
6. **Powołanie Komisji oceny inwestycji i wprowadzenie zarządzania portfelem:** ustalenie priorytetów uzasadnień biznesowych organizacji w odniesieniu do wymagań i priorytetów CIO, a także ustalenie portfela inwestycji.
7. **Przedłożenie Załączników 300 i Załącznika 53[39] oraz zarządzanie programem:** zapewnienie włączenia zatwierdzonych Załączników 300 do treści organizacyjnego Załącznika 53; zapewnienie zarządzania inwestycjami w całym ich cyklu życia.

[38] Załącznik ten należy traktować jako przykład, który może zostać zaadaptowany ze stosownymi zmianami przez organizację.

[39] Tamże.

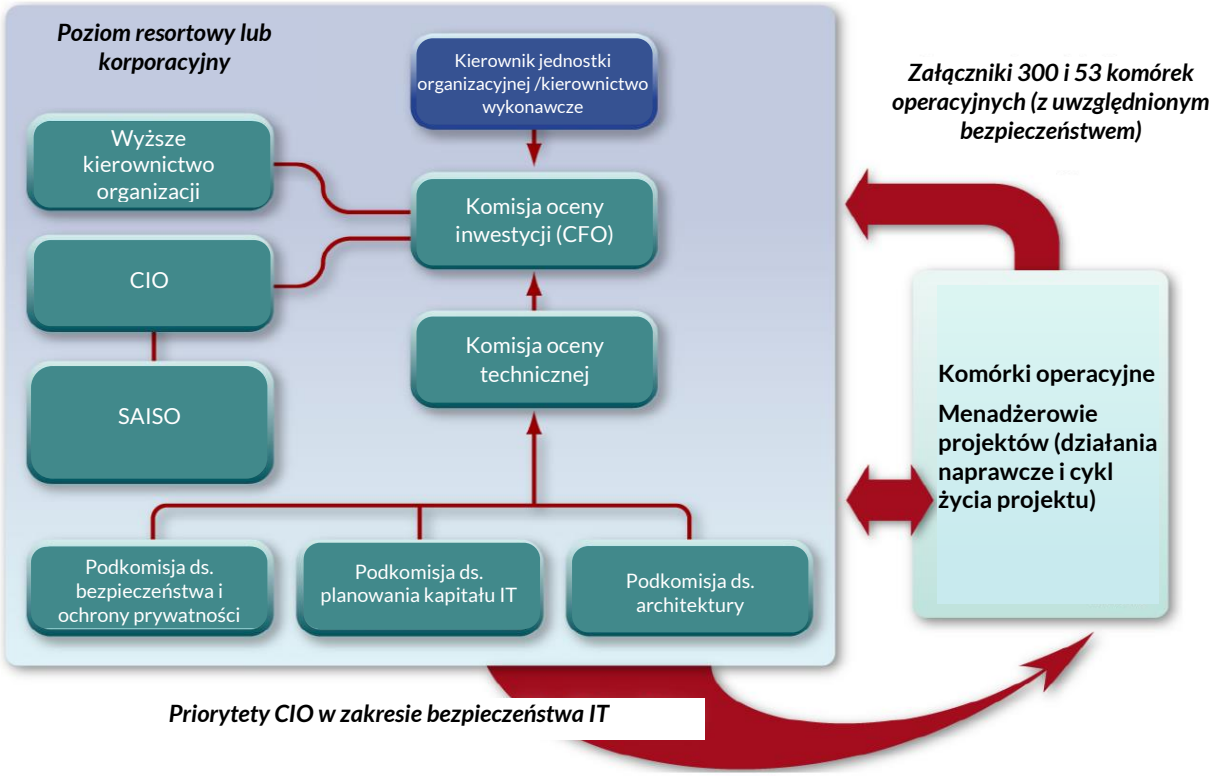


Rysunek 5-2. Integracja bezpieczeństwa informacji z procesem CPIC

W poniższych podrozdziałach przedstawiono przegląd integracji bezpieczeństwa informacji z procesem CPIC mającej na celu pomoc w zapewnieniu, aby działania naprawcze określone w rocznym sprawozdaniu na podstawie POA&M zostały włączone do procesu CPIC dla zmaksymalizowania bezpieczeństwa w ekonomiczny sposób.

5.3. ROLE I OBOWIĄZKI DOTYCZĄCE PLANOWANIA FINANSOWEGO I KONTROLI INWESTYCJI[40]

Integracja bezpieczeństwa informacji z procesem planowania finansowego i kontroli inwestycji (CPIC) wymaga wkładu i współpracy jednostek operacyjnych i biznesowych w całym cyklu życia inwestycji technologicznych. Rys. 5-3 pokazuje hierarchiczne podejście do procesu CPIC, w którym decyzje inwestycyjne są podejmowane zarówno na poziomie korporacji, jak i komórek operacyjnych.



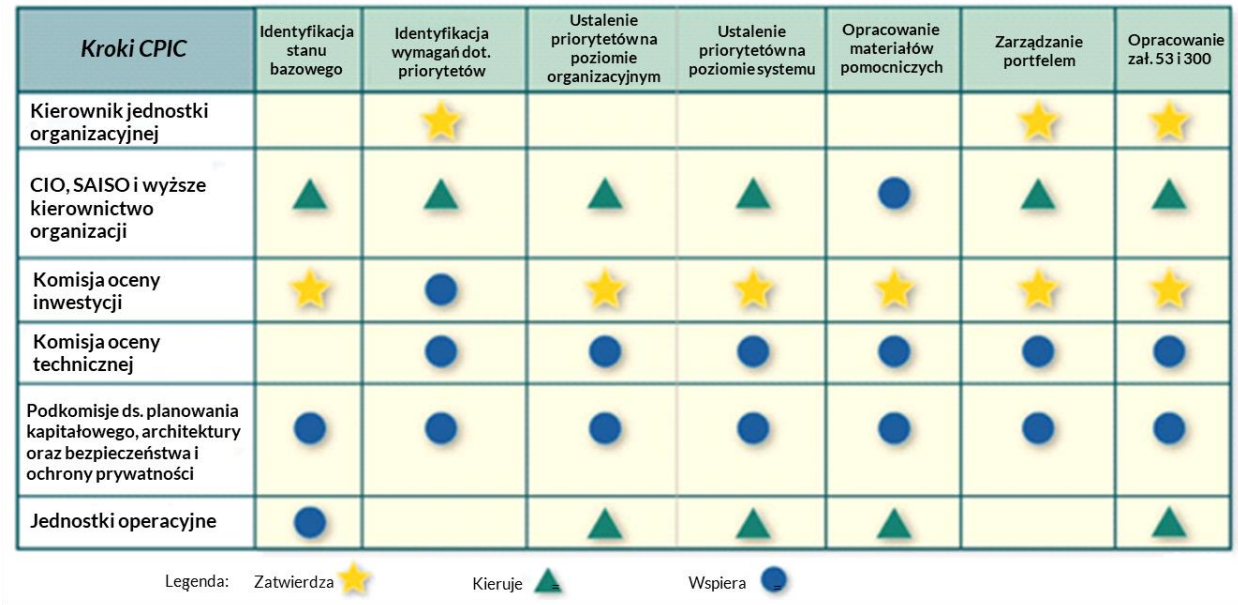
Rysunek 5-3. Hipotetyczna hierarchia zarządzania IT

[40] Dodatkowe wytyczne dotyczące ról i obowiązków, zob. Rozdział 2 „Zarządzanie bezpieczeństwem informacji", Rozdział 8 „Planowanie bezpieczeństwa", Rozdział 11 „Certyfikacja, akredytacja i oceny bezpieczeństwa" oraz Rozdział 14 „Zarządzanie konfiguracją" niniejszego podręcznika.

Chociaż konkretne praktyki zarządzania inwestycjami mogą się różnić na poziomie komórek operacyjnych z powodu różnic w zakresie misji, proces jest generalnie odzwierciedleniem na poziomie organizacji. CIO formułuje i artykułuje priorytety bezpieczeństwa informacji dla organizacji, które mają zostać rozważone w kontekście wszystkich inwestycji organizacji. Priorytety mogą opierać się na misji organizacji, wytycznych władzy wykonawczej, zaleceniach lub innych priorytetach zewnętrznych/wewnętrznych. Przykładowe priorytety w zakresie bezpieczeństwa to: certyfikacja i akredytacja wszystkich systemów czy wdrożenie infrastruktury klucza publicznego (*ang. Public Key Infrastructure, PKI*) w całej organizacji. Należy zauważyć, iż wytyczne władzy wykonawczej powinny mieć najwyższy priorytet spośród wyżej wymienionych.

Kiedy jednostki operacyjne sfinalizują już swoje portfele IT i wnioski budżetowe na dany rok budżetowy, przekazują je do decydentów na poziomie organizacji. Na tym poziomie, komisje oceniają portfele IT otrzymane od jednostek operacyjnych, co pokazano na rys. 5-3, a kulminacją tej oceny jest przegląd przez komisję oceny inwestycji (IRB). Następnie IRB podejmuje decyzję w sprawie portfela IT na poziomie organizacji i przekazuje zalecenia kierownikowi jednostki organizacyjnej celem zatwierdzenia. Po zatwierdzeniu organizacyjnego portfela IT przez kierownika jednostki organizacyjnej, wymagane Załączniki 300 Załącznik 53 są przekazywane do komórki ds. zarządzania i budżetu w celu rozpatrzenia finansowania.

Wielu różnych interesariuszy z obszarów kierownictwa zajmujących się bezpieczeństwem informacji, planowaniem finansowym i zarządzaniem wykonawczym odgrywa kluczowe role i podejmuje decyzje w zakresie integracji bezpieczeństwa informacji z procesem CPIC, przy czym ostatecznym celem jest stworzenie dobrze zbilansowanego portfela IT. Zaangażowanie na poziomie zarówno korporacji, jak i jednostek operacyjnych w całym procesie pozwala organizacjom zapewnić spełnienie celów i atrybutów CPIC i bezpieczeństwa informacji. Na rys. 5-4 określono typowe role przywódcze, pomocnicze lub zatwierdzające każdego z interesariuszy mające zastosowanie do integracji bezpieczeństwa z fazami procesu CPIC.



Rysunek 5-4. Role i obowiązki w procesie CPIC

5.4. IDENTYFIKACJA ZABEZPIECZEŃ BAZOWYCH

Pierwszym krokiem w integracji bezpieczeństwa informacji i procesu CPIC jest ocena zabezpieczeń bazowych[41] (*ang. security baseline*). Zabezpieczenia bazowe dają obraz zgodności organizacji z podstawowymi wymogami bezpieczeństwa (*ang. baseline security requirements - BLSR*) i mają zasadnicze znaczenie dla określenia mocnych i słabych stron bezpieczeństwa informacji. Wynik analizy zabezpieczeń bazowych umożliwia kierownictwu organizacji ocenę stanu bezpieczeństwa informacji i zidentyfikowanie obszarów, w których wymagana jest poprawa. Organizacje mogą określać swoje „bejslajny" dla inwestycji na poziomie organizacji lub systemu. Inwestycje na poziomie systemu to inwestycje w bezpieczeństwo mające wzmocnić stan bezpieczeństwa konkretnego systemu, np. wzmocnienie zabezpieczeń hasłowych czy przetestowanie planu awaryjnego konkretnego systemu. Inwestycje na poziomie organizacji to inwestycje w bezpieczeństwo, które dotyczą całej organizacji i mają poprawić jej ogólny stan bezpieczeństwa, np. nabycie zapory sieciowej lub systemu wykrywania włamań dla całej organizacji.

41 W potocznym języku technicznym – „bejslajny".

Publikacja NIST SP 800-55, *Security Metrics Guide for Information Technology Systems*, zawiera wytyczne w zakresie opracowywania i wdrażania programu metryk bezpieczeństwa informacji. Metryki mogą przedstawiać wartości procentowe dotyczące zgodności z poziomem bazowym wskazujące na istnienie odpowiednich zabezpieczeń, ukazujące słabości i identyfikujące rozbieżności między faktycznym i pożądanym stanem wdrożenia środków bezpieczeństwa informacji. Celem ustalenia linii bazowej stanu bezpieczeństwa jest umożliwienie personelowi organizacji zrozumienia mocnych i słabych punktów oraz podatności istniejących w zabezpieczeniach organizacji, a także pomoc w zidentyfikowaniu inwestycji, które są wymagane do zniwelowania słabości. Znalezione podatności i słabości służą następnie za materiał wejściowy dla kolejnego etapu procesu CPIC, czyli określenia kryteriów ustalania priorytetów.

5.5. OKREŚLENIE KRYTERIÓW USTALANIA PRIORYTETÓW

Dostępne fundusze nie zawsze pozwalają na niezwłoczne zajęcie się wszystkimi potrzebami w zakresie bezpieczeństwa zidentyfikowanymi podczas oceny zabezpieczeń bazowych. Dlatego priorytetowy charakter mają wymagania dotyczące najpilniejszych potrzeb inwestycyjnych z zakresu bezpieczeństwa. Szczegółowe kryteria dotyczące ustalania priorytetów będą różnić się w zależności od misji i celów danej organizacji oraz obowiązujących przepisów i uregulowań. Przykładowe priorytety w zakresie bezpieczeństwa informacji:

- spełnienie ustawowych wymagań prawnych;
- wdrożenie programu bezpieczeństwa opartego na ryzyku (rozporządzenia wykonawcze, pomocnicze normy i rekomendacje NSC); np. wdrożenie zabezpieczeń opisanych w publikacji NSC 800-53;
- ochrona narodowych i organizacyjnych aktywów o krytycznym znaczeniu dla misji;
- poprawa stanu programu bezpieczeństwa informacji; ukończenie certyfikacji i akredytacji bezpieczeństwa wszystkich systemów zgodnie z obowiązującymi normami i wydanymi rekomendacjami.

Kryteria ustalania priorytetów można zorganizować przy użyciu różnorodnych taksonomii, w tym kategorii zabezpieczeń podanych w NSC 200 lub innych kategorii specyficznych dla danej organizacji.

5.6. USTALENIE PRIORYTETÓW NA POZIOMIE SYSTEMU I ORGANIZACJI[42]

Kiedy już kierownictwo i interesariusze organizacji dojdą do porozumienia w sprawie priorytetów inwestycji, organizacja może rozpocząć proces ustalania priorytetów przez hierarchizowanie wymogów względem kryteriów priorytetyzacji. Celem tego działania jest zapewnienie finansowania w pierwszym rzędzie dla inwestycji o największym znaczeniu dla bezpieczeństwa. Kolejna warstwa finansowania powinna zostać przydzielona inwestycji, która jest następna pod względem znaczenia, itd. aż do całkowitego wyczerpania budżetu albo spełnienia priorytetów, zależnie od tego, co nastąpi wcześniej.

Przed ustaleniem priorytetów działań naprawczych, organizacja powinna przydzielić fundusze konieczne do zniwelowania niedociągnięć i zaspokojenia innych potrzeb, które w sposób oczywisty wymagają uwagi. Inicjatywy te powinny zostać następnie usunięte z procesu ustalania priorytetów, aby uniknąć dublowania działań.

Po określeniu bazowego stanu bezpieczeństwa i kryteriów ustalania priorytetów, organizacja może przystąpić do ustalania priorytetów działań naprawczych na dwóch poziomach:

1. Ustalenie priorytetów na poziomie systemu: uporządkowanie pod kątem ważności działań naprawczych dotyczących słabości i podatności na poziomie systemu stwierdzonych podczas oceny zabezpieczeń bazowych względem z góry ustalonych kryteriów ustalania priorytetów. Jest to wykonywane na poziomie jednostek operacyjnych przez właścicieli systemów i menadżerów programu[43].

---

[42] Informacje przedstawione w niniejszej publikacji stanowią przegląd procesu ustalania priorytetów. Szczegółowe objaśnienie sugerowanego systemu oraz korporacyjnych procedur w zakresie ustalania priorytetów, np. zob. NIST SP 800-65, str. 28–36.

[43] Dodatkowe wytyczne dotyczące ról i obowiązków w zakresie bezpieczeństwa, zob. Rozdział 8 „Planowanie bezpieczeństwa", Rozdział 10 „Zarządzanie ryzykiem", Rozdział 11 „Certyfikacja, akredytacja i oceny bezpieczeństwa" oraz Rozdział 14 „Zarządzanie konfiguracją" niniejszego podręcznika.

2. Ustalenie priorytetów na poziomie organizacji: uporządkowanie pod kątem ważności działań naprawczych na poziomie organizacji stwierdzonych podczas oceny zabezpieczeń bazowych względem z góry ustalonych kryteriów ustalania priorytetów. Jest to wykonywane na poziomie organizacji przez interesariuszy organizacji związanych z bezpieczeństwem informacji.

Metodologia ustalania priorytetów opiera się głównie na istniejących źródłach i danych wejściowych. Specyficzne dane wejściowe dla powyższych dwóch typów ustalania priorytetów przedstawiono w tabeli 5-1.

Tabela 5-1. Dane wejściowe do ustalania priorytetów

Dane	Źródło	Dostępność danych
Informacje na poziomie systemu		
Kategoryzacja systemu	Certyfikacja i akredytacja bezpieczeństwa system, plan bezpieczeństwa lub kategoryzacja wg. NSC 800-60 i NSC 199.	Certyfikacja i akredytacja bezpieczeństwa, plany bezpieczeństwa oraz kategoryzacja wg NSC 800-60/NSC 199 są zalecane w przypadku wszystkich systemów organizacji. Wymagane dane można łatwo pozyskać z odpowiedniej dokumentacji.
Zgodność w zakresie bezpieczeństwa	Metryki bezpieczeństwa informacji na poziomie systemu lub agregowane wartości procentowe dotyczące zgodności w zakresie bezpieczeństwa informacji z szacowania ryzyka, certyfikacji i akredytacji bezpieczeństwa lub innych źródeł, zorganizowane według kategorii kryteriów ustalania priorytetów.	Szacowanie ryzyka oraz działania z zakresu certyfikacji i akredytacji bezpieczeństwa są zalecane dla wszystkich organizacji. Niezbędne dane można łatwo zebrać w wymaganej formie.

Dane	Źródło	Dostępność danych
Koszt działania naprawczego	Plan i etapy działania (POA&M) systemu.	POA&M to działanie zalecane w przypadku wszystkich organizacji. Niezbędne dane można łatwo zebrać w wymaganej formie.
Informacje na poziomie organizacji		
Rankingi interesariuszy dotyczące inicjatyw prowadzonych na poziomie organizacji	Spotkania z osobami zaangażowanymi w bezpieczeństwo informacji w organizacji dotyczące ustalania priorytetów.	Nowe działanie – wymaga współpracy między osobami zaangażowanymi w bezpieczeństwo informacji w organizacji.
Status inicjatywy dotyczącej bezpieczeństwa informacji prowadzonej na poziomie organizacji	Metryki bezpieczeństwa informacji na poziomie organizacji lub agregowane wartości procentowe dotyczące zgodności w zakresie bezpieczeństwa informacji z szacowania ryzyka, certyfikacji i akredytacji bezpieczeństwa lub innych źródeł, zorganizowane według kategorii kryteriów ustalania priorytetów.	Szacowanie ryzyka oraz działania z zakresu certyfikacji i akredytacji bezpieczeństwa są wymagane dla wszystkich organizacji. Wymagane dane można łatwo zebrać w wymaganej formie.
Koszt wdrożenia pozostałych wymaganych zabezpieczeń dla inicjatyw prowadzonych na poziomie organizacji	POA&M programu	POA&M to działanie wymagane w przypadku wszystkich organizacji. Wymagane dane można łatwo zebrać w wymaganej formie.

Niektóre dane wejściowe trzeba bardziej szczegółowo opracować na potrzeby wsparcia procesu ustalania priorytetów działań naprawczych:

- **Luka zgodności:** różnica między pożądanym i faktycznym stopniem zgodności z wymaganiami bezpieczeństwa. Na przykład, jeżeli w danym systemie

informacyjnym ukończono 80 procent działań związanych z certyfikacją i akredytacją bezpieczeństwa, to luka zgodności dla tej inwestycji wynosi 20 procent (faktyczna zgodność wynosząca 80 procent odjęta o pożądanego stopnia zgodności wynoszącego 100 procent daje lukę zgodności wynoszącą 20 procent). Im mniejsza luka zgodności, tym wyższy stopień zgodności danego systemu lub zabezpieczenia organizacyjnego.

- **Wpływ działania naprawczego:** stosunek luki zgodności do kosztu działania naprawczego. Jak pokazano na rys. 5-5, wpływ działania naprawczego jest obliczany jako iloraz wartości procentowej luki zgodności i kosztu wdrożenia tego działania. Wynikiem jest proporcja rezultatu do kosztu. Im jest ona wyższa, tym większa będzie opłacalność przeprowadzonego działania naprawczego. Otrzymana proporcja jest mnożona przez 100 000 na potrzeby dalszych obliczeń.

$$\left(\frac{\text{Wartość procentowa luki zgodności po zrealizowaniu działania naprawczego}}{\text{Koszt działania naprawczego}} \right) \times 100{,}000$$

Rysunek 5-5. Obliczanie wpływu działania naprawczego

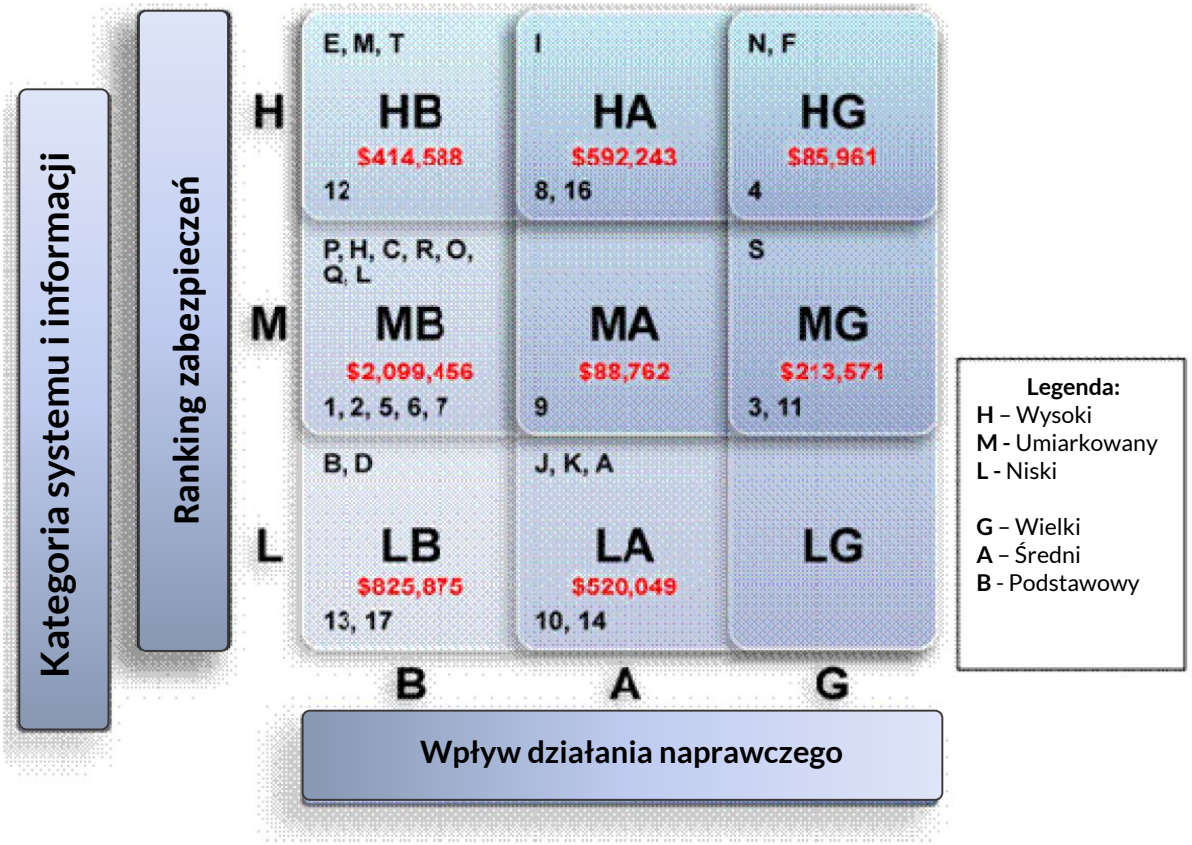
Po zebraniu danych wejściowych, proces ustalania priorytetów należy zakończyć wykonując następujące cztery czynności:

1. uporządkowanie ustalonych priorytetów dotyczących kategorii działań naprawczych według ich znaczenia dla organizacji,
2. uporządkowanie systemów organizacji według rangi,
3. obliczenie luk zgodności w zakresie bezpieczeństwa na poziomie organizacji i poszczególnych inwestycji;
4. obliczenie wpływu działań naprawczych na poziomie organizacji i poszczególnych inwestycji.

Należy przeprowadzić priorytetyzację zarówno na poziomie organizacji, jak i systemu, a następnie nałożyć wyniki tak, aby odpowiednie priorytety organizacji na pewno

uzyskały finansowanie współmierne do ich poziomów ryzyka. Ustalanie priorytetów ułatwić może wykorzystanie arkuszy kalkulacyjnych lub bardziej zaawansowanych narzędzi automatyzacji[44]. Wizualizacji wyników procesu ustalania priorytetów można użyć do ułatwienia procesu decyzyjnego.

Na rys. 5-6 przedstawiono przykład wizualizacji ustalania priorytetów działań naprawczych przy użyciu hipotetycznych danych. Z perspektywy systemu, rys. 5-6 nanosi kategorię systemu wzdłuż osi pionowej, natomiast wpływ działania naprawczego wzdłuż osi poziomej. Hipotetyczne systemy organizacji zostały oznaczone jako małe litery u góry każdego kwadratu. Na tym przykładzie uznano, że systemy „N" i „F" mają kategorię „wysoki" (*ang. high -H*), a wpływ działania naprawczego kategorię „wielki" (*ang. great - G*).



Rysunek 5-6. Połączone ustalanie priorytetów z kosztami

Z perspektywy organizacji, rys. 5-6 nanosi ustalone przez organizację zabezpieczenia wzdłuż osi pionowej, natomiast wpływ działania naprawczego wzdłuż osi poziomej.

[44] Na rys. 4-6 i 4-8 (odpowiednio) w publikacji NIST SP 800-65 pokazano przykłady sposobów wykorzystania arkuszy kalkulacyjnych do ułatwienia procesu ustalania priorytetów.

Liczby (1-17) przedstawiają siedemnaście kategorii zabezpieczeń określonych w publikacji NSC 800-53, których użyto w tym przykładzie. Obszar zabezpieczeń nr 12 został oceniony jako „wysoki" (H) pod względem znaczenia, ale ma wpływ działania naprawczego określony jako „podstawowy" (*ang. basic - B*).

Symbole dolara na rys. 5-6 przedstawiają całkowity koszt wdrożenia wszystkich działań naprawczych w danej komórce. Na przykład, patrząc na komórkę HG, organizacja wydałaby 85,961 $ na wdrożenie działań naprawczych dla systemów „N" i „F" kategorii zabezpieczeń nr „4." Po naniesieniu wszystkich swoich systemów, organizacja powinna przeprowadzić walidację rozmieszczenia różnych systemów, aby zapewnić spełnienie priorytetów interesariuszy.

Interesariusze organizacji związani z bezpieczeństwem informacji powinni dokonać przeglądu wyników ustalenia priorytetów, aby zapewnić, że zostały one odpowiednio ustalone. Należy im umożliwić ponowne ustalenie priorytetów, jeżeli wyniki procesu zostaną uznane za niezadowalające. Zakładając, że interesariusze organizacji zgodzili się, że wszystkie priorytety działań naprawczych są odpowiednie, jak pokazano na rys. 5-6, można przystąpić do analizy. Jak wskazują osie, realizacja działań naprawczych należy rozpocząć od komórki HG, a następnie iść po przekątnej do komórki LB, aby zapewnić, że organizacja wdroży najbardziej ekonomiczne działania naprawcze o wysokim wpływie.

Pozostając przy przywołanym przykładzie, załóżmy, że hipotetyczna organizacja posiada budżet w wysokości 2,000,000 $ na wdrożenie działań naprawczych z zakresu bezpieczeństwa informacji. Jak pokazano na rys. 5-6, zsumowanie trzech komórek o najwyższym priorytecie (HG, HA i MG) daje 891,775$, co stanowi niemal połowę budżetu na działania naprawcze. Organizacja następnie przeszłaby do kolejnego poziomu priorytetów, czyli komórek HB, MA i LG. Ich zsumowanie daje 503,350$, co w połączeniu z sumą kwot z komórek HG, HA i MG, daje 1,395,125$. Z kwotą 604,875 pozostającą w budżecie na działania naprawcze, organizacja przeszłaby następnie do komórek MB i LA. Ich zsumowanie daje 2,619,505$. Ponieważ kwota ta wyraźnie przekracza pozostały budżet, interesariusze będą musieli zdecydować, jak podzielić dostępne fundusze. Jeżeli ustalą, że decydująca jest kolejność wpływu działań naprawczych (G, A, B), to wdrożone zostaną działania naprawcze z komórki LA.

Natomiast jeżeli w ich opinii decydujące znaczenie ma kategoria systemu i zabezpieczenia (H, M, L), to wdrożone zostaną działania naprawcze z komórki MB aż do wyczerpania pozostałej w budżecie kwoty 604,875$[45].

5.7. OPRACOWANIE MATERIAŁÓW POMOCNICZYCH

Po ustaleniu priorytetów zgodnie z wymogami, jednostki operacyjne są gotowe do wybrania swoich inwestycji na dany rok budżetowy i rozpoczęcia procesu wnioskowania o fundusze na następny rok w celu wdrożenia działań naprawczych i zabezpieczeń.

Załącznik 300 to mechanizm gromadzący dane do wszystkich analiz i działań wymaganych w pełnym przeglądzie wewnętrznym (np. IRB, CIO). Co ważniejsze, Załącznik 300 jest dokumentem, z którego organizacja korzysta do oceny inwestycji i podejmowania ostatecznych decyzji o finansowaniu, a zatem powinien być przez organizacje wykorzystywany do wyraźnego uzasadnienia swoich corocznych wniosków dotyczących cyklu życia i finansowania. Załącznik 300 jest wypełniany w przypadku wszystkich nowych inwestycji IT i składany co roku w przypadku inwestycji o mieszanym cyklu życia i stałym stanie. Jednostki operacyjne powinny dokonywać oceny swoich priorytetów działań naprawczych i zabezpieczeń ustalonych w procesie priorytetyzacji i określić, czy wyniki tego procesu należy ująć w Załączniku 300 już realizowanej inwestycji, czy też trzeba stworzyć odrębny Załącznik 300 dla nowej inwestycji.

5.8. KOMISJA OCENY INWESTYCJI I ZARZĄDZANIE PORTFELEM

Komisja oceny inwestycji (IRB) dokonuje przeglądu i wyboru inwestycji do portfela organizacji w oparciu o Załączniki 300 przekazane przez jednostki operacyjne. Podobnie jak w przypadku ustalania priorytetów mającego miejsce na poziomie jednostki operacyjnej, IRB zazwyczaj wykorzystuje kryteria strategiczne do ustalenia hierarchii puli inwestycji i na ogół podejmuje decyzji w oparciu o misję i cele organizacji,

[45] Informacje przedstawione w niniejszej publikacji specjalnej stanowią przegląd procesu ustalania priorytetów. Szczegółowe objaśnienie sugerowanego systemu oraz korporacyjnych procedur w zakresie ustalania priorytetów, zob. NIST SP 800-65, str. 28–36.

nie tylko koszt. Chociaż bezpieczeństwo nie jest typowym motorem napędowym zarządzania portfelem, to stanowi ono jeden z kluczowych elementów strategii inwestycyjnej, ponieważ służy jako kwalifikator pozyskiwania funduszy i pomoc dla tych funkcji, które wspierają misję organizacji. Po ustaleniu priorytetów i zatwierdzeniu Załączników 300, IRB tworzy wniosek dotyczący portfela inwestycji do oceny przez komórkę ds. zarządzania i budżetu.

5.9. ZAŁĄCZNIKI 53 I 300 ORAZ ZARZĄDZANIE PROGRAMEM

Po naborze inwestycji do portfela, organizacja łączy treść Załączników 300 w Załącznik 53. Załącznik 53 umożliwia dokonanie ogólnego przeglądu całego portfela IT organizacji poprzez wyszczególnienie informacji o każdej inwestycji IT, cyklu życia i kosztach roku budżetowego.

Oprócz ujęcia wszystkich inwestycji opisanych w Załącznikach 300, Załącznik 53 zawiera również inwestycje IT, które nie wymagają Załącznika 300 (np. dotyczących już istniejących systemów z kosztami poniżej ustalonych dla organizacji progów). Komórka ds. zarządzania i budżetu dokonuje ewaluacji złożonych Załączników 53 i 300 i ustala odpowiednie kwoty finansowania na dany rok budżetowy w oparciu o uzasadnienie zawarte w Załącznikach 300. Organizacje otrzymują następnie środki budżetowe przydzielone na dany rok i muszą z nich wdrożyć lub utrzymać swoje inwestycje w tym roku.

Strony internetowe:[46]

Informacje na temat Załącznika 300:

http://www.whitehouse.gov/omb/circulars/a11/current yearZs300.pdf

www.csrc.nist.gov

[46] Dla zainteresowanych.

REFERENCJE:[47]

Federal Information Processing Standard 199, *Requirements for Security Categorization of Federal Information and Information Systems*, February 2004.

Federal Information Processing Standard 200, *Minimum Security Standards for Federal Information and Information Systems*, March 2006.

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

National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems (draft)*, April 2006.

National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

National Institute of Standards and Technology Special Publication 800-53, *Revision 1, Recommended Security Controls for Federal Information Systems*, February 2006.

National Institute of Standards and Technology Special Publication 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003.

National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.

National Institute of Standards and Technology Special Publication 800-65, *Integrating Information Security into the Capital Planning and Investment Control Process*, January 2005.

[47] Tamże.

ROZDZIAŁ 6

6. POŁĄCZENIA MIĘDZYSYSTEMOWE

Wzajemne połączenie systemów (połączenie międzysystemowe) jest definiowane jako połączenie co najmniej dwóch systemów informacyjnych w celu wymiany danych i innych zasobów informacyjnych. Podmioty decydują o łączeniu swoich systemów informacyjnych z różnych powodów w oparciu o swoje potrzeby organizacyjne. Może to być np. wymiana danych, współpraca przy wspólnych projektach lub bezpieczne przechowywanie danych i wykonywanie kopii zapasowych plików. To bezpośrednie połączenie między systemem jednej organizacji i innym systemem tej samej lub innej organizacji realizowane za pośrednictwem mechanizmu, który je łączy (czyli łącza, którym dane są udostępniane, wymieniane lub przekazywane). Łączem może być specjalna linia należąca do jednej z organizacji lub dzierżawiona od podmiotu trzeciego (np. cyfrowa sieć usług zintegrowanych [*ang. Integrated Services Digital Network*, *ISDN*], linia E1 lub E3). Systemy mogą też być połączone za pośrednictwem sieci publicznej (np. Internetu) z wykorzystaniem wirtualnej sieci prywatnej (*ang. Virtual Private Network - VPN*).

Rysunek 6-1 przedstawia koncepcję wzajemnego połączenia systemów informacyjnych.

Rysunek 6-1. Wzajemne połączenie systemów informacyjnych

Przykłady połączeń międzysystemowych:

- System A jest połączony z Systemem B linią abonencką dzierżawioną przez System A od Systemu B.

- System A jest podzielony w taki sposób, że System A1 jest zintegrowany z Systemem A, ale znajduje się pod inną kontrolą zarządczą (osobą autoryzującą).
- System B świadczy usługi przesyłu danych między Systemem A i Systemem C. W tym przypadku, System B uczestniczy w dwóch połączeniach wzajemnych z Systemem A i Systemem C.

Poziomy wzajemnych połączeń systemów mogą być różne. Przykładowo, niektóre organizacje mogą wybrać ograniczone połączenie wzajemne, w ramach którego użytkownicy mogą korzystać tylko z jednej aplikacji lub lokalizacji plików i podlegają zasadom regulującym dostęp. Inne organizacje mogą ustanowić szersze połączenie umożliwiające użytkownikom dostęp do wielu aplikacji lub baz danych. Jeszcze inne mogą ustanowić połączenie, które pozwala na pełną przejrzystość i dostęp wszystkim uczestniczącym stronom.

Wzajemne połączenie systemów informacyjnych może stwarzać ryzyko dla uczestniczących w nim organizacji. Jeżeli nie zostanie właściwie zaprojektowane, błędy zabezpieczeń mogą narazić połączone systemy lub dane na naruszenie. Podobnie, w przypadku naruszenia bezpieczeństwa jednego z połączonych systemów, wzajemne połączenie może zostać wykorzystane jako kanał naruszenie bezpieczeństwa drugiego systemu i jego danych.

Organizacje powinny zawierać umowy o bezpiecznym połączeniu systemów i uzyskać pisemną autoryzację zanim połączą swoje systemy informacyjne z innymi systemami w oparciu o wzajemnie akceptowany poziom ryzyka. Przykładowe zalecenia dotyczące wzajemnego łączenia systemów informacyjnych znajdują się w publikacji specjalnej NIST SP 800-47, *Security Guide for Interconnecting Information Technology Syste*ms.

6.1. ZARZĄDZANIE WZAJEMNYMI POŁĄCZENIAMI SYSTEMOWYMI

Organizacje powinny jednoznacznie odnieść się do kwestii wzajemnych połączeń systemów informacyjnych poprzez zawieranie formalnych umów precyzujących wymagania dotyczące połączenia w zakresie techniki i bezpieczeństwa, a także określających obowiązki stron i zasady regulujące połączenie.

Oprócz wymogu uzyskania pisemnego upoważnienia przed połączeniem systemów informacyjnych, zaleca się, aby organizacje postępowały zgodnie z np. treścią publikacji NIST SP 800-47 w celu zapewnienia zgodności w przypadku połączeń z systemami spoza organizacji.

Właściwe zarządzanie połączonymi systemami daje organizacjom dodatkowe korzyści w postaci większej wydajności, scentralizowanego dostępu do danych oraz większej funkcjonalności. Zabezpieczenia każdego z połączonych systemów należy poddać ocenie. Muszą one wzajemnie spełniać swoje wymagania w zakresie środków bezpieczeństwa odpowiednich dla danego połączenia. Obie organizacje powinny określić swoje wymagania dotyczące zabezpieczeń, które mają zostać wdrożone zgodnie z NSC 200 oraz NSC 800-53.

Każdy system uczestniczący w połączeniu powinien być zarządzany przez osobę autoryzującą formalnie odpowiedzialną za użytkowanie systemu na dopuszczalnym poziomie ryzyka. Publikacja NSC 800-53 szczegółowo określa zabezpieczenia połączeń systemów informacyjnych (wyszczególnione w tabeli 6-1), jakie organizacje powinny wdrożyć w oparciu o dokonaną kategoryzację bezpieczeństwa systemu informacyjnego. Ponieważ kategorie i wytyczne, o których mowa mają zastosowanie do poszczególnych systemów, organizacje powinny starannie rozważyć ryzyko towarzyszące łączeniu systemów różniących się od siebie konfiguracją lub zabezpieczeniami.

Tabela 6-1. Zabezpieczenie połączeń systemów informacyjnych wg NSC 800-53

Identyfikator zabezpieczenia	Nazwa	Zabezpieczenie
CA-3	Wymiana informacji	Organizacja autoryzuje wszystkie połączenia z systemu informacyjnego do innych systemów informacyjnych poza granicami akredytacji i regularnie monitoruje/kontroluje wzajemne połączenia. Umowy o połączeniu systemów informacyjnych są zatwierdzane przez odpowiednie osoby w organizacji.

Kluczowe jest, aby obie organizacje utrzymywały efektywne kanały komunikacji w celu:

- zapewnienia właściwego zarządzania połączeniem i skuteczności zabezpieczeń;
- usprawnienie skutecznego zarządzanie modyfikacjami poprzez ułatwienie obu stronom wymiany zawiadomień o planowanych zmianach systemowych mogących mieć wpływ na połączenie;
- umożliwienia obu stronom niezwłocznego zawiadamiania o incydentach bezpieczeństwa i zakłóceniach systemów, a w razie konieczności, ułatwienia skoordynowanej reakcji.

Identyfikowanie i wdrażanie zabezpieczeń są niezbędne dla ochrony poufności, integralności i dostępności połączonych systemów i danych, które są między nimi przesyłane. Jeżeli zabezpieczenia nie zostaną wdrożone albo właściwie skonfigurowane, ustanowienie wzajemnego połączenia może narazić systemy informacyjne na nieautoryzowany dostęp. Organizacje mogą wybierać zabezpieczenia spośród podanych w publikacji NSC 800-53, w oparciu o kategoryzację bezpieczeństwa systemów uczestniczących w połączeniu podaną w NSC 199, oraz NSC 800-60. Zabezpieczenia powinny zostać dobrane odpowiednio do podłączanego systemu i środowiska, w którym będą zestawione połączenia międzysystemowe.

Jedna albo obydwie organizacje powinny przeprowadzić przegląd zabezpieczeń połączeń międzysystemowych co najmniej raz w roku albo w przypadku każdej znaczącej zmiany w którymkolwiek z systemów lub w środowisku operacyjnym. Celem tego przeglądu jest zapewnienie, aby wszystkie zabezpieczenia działały właściwie i niezmiennie zapewniały wymagany poziom bezpieczeństwa systemu i danych[48].

6.2. PODEJŚCIE OPARTE NA ZARZĄDZANIU CYKLEM ŻYCIA

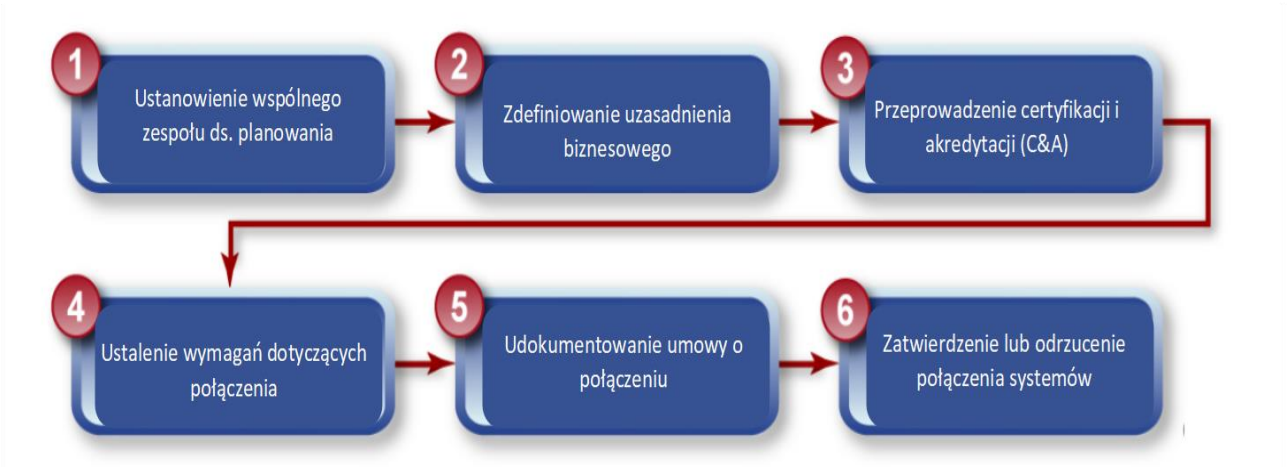
[48] Dodatkowe wytyczne w zakresie przeglądów zabezpieczeń, zob. NSC 800-30, a także Rozdział 10 „Zarządzanie ryzykiem" oraz Rozdział 11 „Certyfikacja, akredytacja i oceny bezpieczeństwa" niniejszego podręcznika.

Publikacja NIST SP 800-47 szczegółowo opisuje podejście do łączenia systemów informacyjnych składające się z czterech faz i związane z cyklem życia systemu, które podkreśla zwrócenie odpowiedniej uwagi na bezpieczeństwo informacji:

- faza 1: planowanie połączenia,
- faza 2: ustanowienie połączenia,
- faza 3: utrzymanie połączenia
- faza 4: rozłączenie.

6.2.1. FAZA 1: PLANOWANIE POŁĄCZENIA

Proces łączenia dwóch lub więcej systemów informacyjnych zaczyna się od fazy planowania, w której uczestniczące organizacje wykonują wstępne czynności i badają wszystkie istotne kwestie techniczne, administracyjne oraz dotyczące bezpieczeństwa. Dzięki fazie planowania połączenie będzie działać w sposób najbardziej wydajny i bezpieczny z możliwych. Zaleca się, aby planowanie połączenia systemów składało się z sześciu kroków. Poszczególne kroki procesu planowania połączenia systemów przedstawiono na rys. 6-2. Bardziej szczegółowe podejście opisano w następnych podrozdziałach.



Rysunek 6-2. Kroki planowania połączenia systemów

Krok 1: Ustanowienie wspólnego zespołu ds. planowania

Organizacje powinny rozważyć ustanowienie wspólnego zespołu ds. planowania złożonego z odpowiedniego personelu technicznego i zarządczego, w którego skład wejdą menadżerowie, osoby odpowiedzialne za bezpieczeństwo systemu, administratorzy systemu, administratorzy sieci i architekci systemu. Wspólny zespół ds. planowania zazwyczaj odpowiada za koordynowanie wszystkich aspektów procesu planowania i zapewnienie istnienia jednoznacznego kierunku oraz wystarczających zasobów. Musi również uzyskać zgodę i wsparcie ze strony właścicieli systemu i danych oraz innych osób z wyższego kierownictwa.

Krok 2: Określ uzasadnienie biznesowe

Obie organizacje powinny wspólnie określić cel połączenia, ustalić sposób, w jaki będzie ono wspierało wymagania ich misji, a także zidentyfikować ewentualne koszty i ryzyko. Określenie uzasadnienia biznesowego stworzy podstawę połączenia i ułatwi proces planowania. Czynniki, jakie należy rozważyć to: szacunkowe koszty (np. personel, sprzęt, obiekty), oczekiwane korzyści (np. lepsza wydajność) oraz ewentualne ryzyko (np. techniczne, prawne i finansowe).

Krok 3: Przeprowadzenie certyfikacji i akredytacji

Ustanowienie połączenia może stanowić znaczącą zmianę dla łączonych systemów. Przed wykonaniem dalszych działań, każda z organizacji powinna rozważyć ponowną certyfikację i akredytację swojego systemu/swoich systemów w celu sprawdzenia czy zabezpieczenia nadal są akceptowalne. Pełna certyfikacja i akredytacja mogą nie być konieczne, jeżeli system nadal będzie działać w granicach akceptowalnego poziomu ryzyka. W takim przypadku, wystarczy skrócona certyfikacja i akredytacja[49].

Krok 4: Ustalenie wymagań dotyczących połączenia

Wspólny zespół ds. planowania powinien zidentyfikować i zbadać wszystkie istotne wymagania dotyczące techniki, bezpieczeństwa i administracji związane z proponowanym połączeniem.

Krok 5: Przygotowanie umowy o połączeniu systemów

[49] Dodatkowe zalecenia w zakresie certyfikacji i akredytacji, zob. NSC 800-37, a także Rozdział 11 „Certyfikacja, akredytacja i oceny bezpieczeństwa" niniejszego podręcznika.

Umowa o bezpiecznym połączeniu systemów (*ang. Interconnection Security Agreement - ISA*) to dokument bezpieczeństwa określający wymogi w zakresie techniki i bezpieczeństwa dotyczące ustanowienia, użytkowania i utrzymania połączenia. Potwierdza ona również protokół uzgodnień (*ang. Memorandum of Understanding - MOU*) /porozumienie o współpracy (*ang. Memorandum of agreement - MOA*) między organizacjami. W szczególności, ISA dokumentuje wymagania dotyczące łączenia systemów informacyjnych, opisuje zabezpieczenia, jakie zostaną zastosowane do ochrony systemów i danych, a także zawiera rysunek topologiczny połączenia i podpisy stron.

Wspólny zespół ds. planowania powinien opracować umowę regulującą połączenie oraz warunki, jakich będą przestrzegać organizacje. Umowa powinna opierać się na przeprowadzonym przez zespół przeglądzie wszystkich istotnych wymagań w zakresie techniki, bezpieczeństwa i administracji zidentyfikowanych i zbadanych podczas realizacji Kroku 4.

MOU/MOA dokumentuje warunki wymiany zasobów danych i informacji. Definiuje cel połączenia, identyfikuje stosowne organy, precyzuje obowiązki każdej z organizacji, określa podział kosztów oraz ustala harmonogram zakończenia lub ponownej autoryzacji połączenia. Aby stać się instrumentem, który organizacja będąca stroną połączenia może egzekwować, MOU/MOA musi zostać podpisane przez osobę prawnie umocowaną w organizacji. Wreszcie, ponieważ ISA i MOU/MOA mogą zawierać wrażliwe informacje, oryginał dokumentu i wszelkie jego kopie powinny być chronione przed nieautoryzowanym ujawnieniem lub modyfikacją, uszkodzeniem lub zniszczeniem.

Krok 6: Zatwierdzenie lub odrzucenie połączenia systemów

Wspólny zespół ds. planowania powinien przesłać ISA oraz MOU/MOA do osoby autoryzującej w każdej z organizacji, z wnioskiem o zatwierdzenie połączenia. Po otrzymaniu dokumentu, odpowiednie osoby autoryzujące powinny dokonać przeglądu ISA, MOU/MOA oraz innych istotnych dokumentów lub działań. Jeżeli ISA i MOU/MOA wchodzą w zakres kompetencji tej samej osoby autoryzującej, organizacje mogą łączyć te dokumenty dla uproszczenia procesów zarządzania i ograniczenia

biurokracji. Łącząc ISA i MOU/MOA, organizacje muszą dopilnować, aby treść oraz cel obydwu dokumentów pozostały niezmienione.

Na podstawie tego przeglądu, osoby autoryzujące powinny zdecydować o:

- zatwierdzeniu połączenia,
- udzieleniu zatwierdzenia tymczasowego lub
- odrzuceniu połączenia.

6.2.2. FAZA 2: USTANOWIENIE POŁĄCZENIA

Po zaplanowaniu i zatwierdzeniu połączenia systemów, można przystąpić do jego wdrożenia. Zalecane kroki dotyczące ustanowienia połączenia systemów przedstawiono na rys. 6-3.

Rysunek 6-3. Zalecane kroki dotyczące ustanowienia połączenia

Krok 1: Opracowanie planu wdrożenia

Aby zapewnić właściwe i bezpieczne połączenie systemów informacyjnych, wspólny zespół ds. planowania powinien opracować plan wdrożenia połączenia. Plan taki powinien co najmniej:

- opisywać systemy informacyjne, które zostaną połączone,
- identyfikować poziom wrażliwości lub niejawności danych, które będą podlegać udostępnieniu, wymianie lub przekazywanych jednostronnie w ramach połączenia,
- identyfikować personel, który ustanowi i będzie utrzymywać połączenie, a także określić jego obowiązki,
- identyfikować zadania i procedury wdrożenia,
- identyfikować i opisywać zabezpieczenia, jakie zostaną zastosowane do ochrony poufności, integralności i dostępności połączonych systemów i danych,
- przewidywać procedury testowania i kryteria pomiarowe w celu zapewnienia

właściwego i bezpiecznego działania połączenia,

- określać wymagania w zakresie szkolenia użytkowników, w tym harmonogram szkoleń,
- przywoływać lub zawierać wszystkie istotne dokumenty, takie jak plany bezpieczeństwa systemu, specyfikacja projektowa i standardowe procedury operacyjne.

Krok 2: Wykonanie planu wdrożenia

Opracowany plan wdrożenia powinien zostać poddany ocenie i zatwierdzeniu przez członków wyższego kierownictwa zespołu ds. planowania, a następnie zostać wykonany. Lista zalecanych zadań w zakresie ustanowienia połączenia obejmuje:

- wdrożenie lub konfigurację zabezpieczeń,
- zainstalowanie lub skonfigurowanie sprzętu komputerowego i oprogramowania,
- zintegrowanie aplikacji,
- przeprowadzenie ocen operacyjnych i ocen bezpieczeństwa,
- przeprowadzenie uświadamiania i szkoleń w zakresie bezpieczeństwa,
- zaktualizowanie planów bezpieczeństwa systemu,
- przeprowadzenie ponownej certyfikacji i akredytacji.

Procedury związane z każdym z powyższych zadań powinny zostać opisane w planie wdrożenia.

Krok 3: Uruchomienie połączenia

Obie strony powinny uruchomić połączenie po wykonaniu planu wdrożenia. Każda z organizacji powinna starannie i często badać dzienniki audytu i rodzaje pomocy, o jaką zwracają się w tym czasie użytkownicy, aby zapewnić właściwe i bezpieczne działanie systemu. Wreszcie, organizacja powinna niezwłocznie dokumentować i niwelować wszelkie słabości i problemy dotyczące bezpieczeństwa.

6.2.3. FAZA 3: UTRZYMANIE POŁĄCZENIA

Po ustanowieniu połączenia, uczestniczące organizacje muszą aktywnie je utrzymywać w celu zapewnienia jego właściwego i bezpiecznego działania. Zalecane są następujące działania dotyczące utrzymania połączenia:

- obsługa sprzętu,
- zarządzanie profilami użytkowników,
- przeprowadzenie przeglądów bezpieczeństwa,
- analizowanie dzienników audytu,
- zgłaszanie incydentów bezpieczeństwa i reagowanie na nie,
- koordynowanie działań z zakresu planowania awaryjnego,
- zarządzanie zmianami
- utrzymanie planów bezpieczeństwa systemu.

6.2.4. FAZA 4: ROZŁĄCZENIE

Rozłączenie systemów może być planowe lub wynikać z sytuacji nagłej. Organizacje mogą chcieć przywrócić tylko niektóre z rozłączonych elementów.

6.3. LIKWIDACJA POŁĄCZENIA MIĘDZYSYSTEMOWEGO

Organizacja może mieć różnorodne powody, aby zlikwidować zestawione połączenie międzysystemowe, np. zmienione potrzeby biznesowe, kwestie związane z kosztami lub zmiany w konfiguracji systemu. Decyzja o likwidacji połączenia powinna zostać podjęta przez właściciela systemu po zasięgnięciu rady odpowiedniego personelu zarządczego i technicznego. Przed zakończeniem połączenia, strona inicjująca powinna pisemnie zawiadomić stronę odbierającą zawiadomienie. Strona odbierająca powinna otrzymanie tego zawiadomienia potwierdzić. Zawiadomienie powinno opisywać powód/powody likwidacji, podawać proponowane ramy czasowe rozłączenia oraz identyfikować personel zarządczy i techniczny, który przeprowadzi rozłączenie.

Harmonogram likwidacji połączenia międzysystemowego powinien dawać rozsądny termin na planowanie wewnętrzne, aby obie strony mogły poczynić odpowiednie

uzgodnienia. Dodatkowo, personel obu organizacji powinien wspólnie ustalić kwestie logistyczne wyłączenia i rozporządzenia wspólnymi danymi, w tym w zakresie skasowania i nadpisania danych wrażliwych. Wyłączenie należy przeprowadzić, kiedy jego wpływ na użytkowników będzie minimalny. Po likwidacji, każda z organizacji powinna zaktualizować swój plan bezpieczeństwa systemu i powiązane z nim dokumenty.

6.3.1. ROZŁĄCZENIE AWARYJNE

W przypadku gdy jedna lub obie organizacje wykryją atak, próbę włamania lub inną sytuację awaryjną stanowiącą wykorzystanie lub zagrożenie połączonych systemów lub znajdujących się w nich danych, konieczne może być nagłe rozłączenie bez udzielenia pisemnego zawiadomienia drugiej stronie. Ten nadzwyczajny środek powinien być stosowany wyłącznie w skrajnych okolicznościach i tylko po konsultacji z odpowiednim personelem technicznym i kierownictwem wyższego szczebla.

Decyzja o rozłączeniu awaryjnym powinna zostać podjęta przez właściciela systemu (lub wyznaczonego członka personelu) i wykonana przez personel techniczny. Właściciel systemu lub wyznaczona osoba powinni niezwłocznie udzielić drugiej stronie stosownego zawiadomienia i uzyskać potwierdzenie jego odbioru. Obie strony powinny wspólnie odizolować i zbadać incydent zgodnie z procedurami reagowania na incydenty. W razie konieczności należy zawiadomić organy ścigania i zabezpieczyć materiał dowodowy.

Strona inicjująca powinna przedstawić drugiej stronie pisemne zawiadomienie w odpowiednim terminie (zgodnie z zawartą umową). W zawiadomieniu należy opisać charakter incydentu, wyjaśnić powody i sposób rozłączenia połączenia oraz określić działania podjęte w celu odizolowania i zbadania incydentu. Zawiadomienie powinno również precyzować, kiedy i na jakich warunkach połączenie może zostać przywrócone (w stosownych przypadkach).

6.3.2. PRZYWRÓCENIE POŁĄCZENIA

Obie organizacje mogą zdecydować o przywróceniu zakończonego połączenia systemów. Decyzja o przywróceniu połączenia powinna być uzależniona od przyczyny i czasu trwania rozłączenia. Na przykład, jeżeli systemy rozłączono z powodu ataku, włamania lub innej sytuacji awaryjnej, obie strony powinny wdrożyć odpowiednie środki przeciwdziałania zapobiegające powtórzeniu się problemu. W razie konieczności, strony powinny również zmodyfikować treść ISA i MOU/MOA tak, aby uwzględniała ona kwestie wymagające uwagi. Ewentualnie, jeżeli połączenie zostało zakończone, każda ze stron powinna oszacować ryzyko dla swojego systemu i zbadać wszelkie istotne wymagania w zakresie planowania i wdrożenia, w tym opracować nową ISA oraz MOU/MOA.

W załączniku 6.A przedstawiona została przykładowa treść MOU/MOA.

Załącznik 6.B zawiera podstawowe listy kontrolnej ISA.

Załącznik 6.A Przykład MOU/MOA

Niniejszy załącznik zawiera przykładowy wzór MOU/MOA, który organizacje mogą wykorzystać jako punkt wyjścia do opracowania własnych MOU/MOA. Wzór nie uwzględnia wszystkich możliwych scenariuszy i służy jedynie jako przykład.

DO UŻYTKU SŁUŻBOWEGO

PROTOKÓŁ UZGODNIEŃ/POROZUMIENIE O WSPÓŁPRACY

NINIEJSZY DOKUMENT ZASTĘPUJE

(*Tytuł i data ewentualnego dokumentu*[50])

WSTĘP

Celem niniejszego protokołu/porozumienia jest zawarcie przez „*Organizację A*" i „*Organizację B*" umowy o zarządzaniu w zakresie opracowania, zarządzania, użytkowania i zabezpieczenia połączenia między „*Systemem A*", którego właścicielem jest *Organizacja A*, oraz „*Systemem B*", którego właścicielem jest *Organizacja B*. Umowa ta będzie regulować relacje między *Organizacją A* i *Organizacją B*, w tym wyznaczenie personelu zarządczego i technicznego w przypadku braku wspólnego kierownictwa.

UPOWAŻNIENIE

Podstawą upoważnienia do zawarcia niniejszych uzgodnień jest „*Obwieszczenie A*" wydane przez *kierownika jednostki organizacyjnej (data).*

TŁO

Intencją stron niniejszej umowy jest połączenie następujących systemów informacyjnych w celu wymiany danych między „*bazą danych ABC*" i „*bazą danych XYZ*". *Organizacja A* wymaga korzystania z bazy danych *ABC Organizacji B*, a *Organizacja B* wymaga korzystania z bazy danych *XYZ Organizacji A* zgodnie z zatwierdzeniem i zaleceniem przez *kierownika jednostki organizacyjnej* zawartym w *Obwieszczeniu A.*

[50] Kursywą zaznaczona pola, które organizacje powinny wypełnić zgodnie z poczynionymi ustaleniami dzień zawierania umowy.

Spodziewana korzyść z połączenia to przyspieszenie przetwarzania danych związanych z *„Projektem R”* w przewidzianych terminach. Każdy z przedmiotowych systemów informacyjnych opisano poniżej:

SYSTEM A:

- nazwa,
- funkcja,
- lokalizacja,
- opis danych, w tym podanie wrażliwości i poziomu niejawności oraz kategoryzacji bezpieczeństwa/poziomu wpływu.

SYSTEM B:

- nazwa,
- funkcja,
- lokalizacja,
- opis danych, w tym podanie wrażliwości i poziomu niejawności oraz kategoryzacji bezpieczeństwa/poziomu wpływu.

KOMUNIKACJA MIĘDZY STRONAMI

Częsta wymiana oficjalnych informacji między stronami jest niezbędna do zapewnienia skutecznego zarządzania połączeniem i użytkowania go. Strony zgadzają się utrzymywać linie komunikacji między wyznaczonymi pracownikami zarówno na poziomie zarządczym, jak i technicznym. O ile nie stwierdzono inaczej, wszelka komunikacja opisana w niniejszym dokumencie musi być prowadzona w formie pisemnej. Właściciele *Systemu A* i *Systemu B* zgadzają się wyznaczyć kierowników technicznych swoich systemów i udostępnić ich dane kontaktowe, a także ułatwić kontakty między tymi osobami w celu wsparcia zarządzania i użytkowania zestawionego połączenia międzysystemowego. Dla ochrony poufności, integralności i dostępności połączonych systemów i danych w nich przechowywanych, przetwarzanych i przesyłanych, strony zgadzają się zgłaszać określone zdarzenia w poniższych terminach:

Incydenty bezpieczeństwa: Personel techniczny niezwłocznie zawiadomi swoich odpowiedników telefonicznie lub pocztą elektroniczną o wykryciu incydentu / incydentów bezpieczeństwa, aby umożliwić drugiej stronie podjęcie działań zmierzających do ustalenia, czy jej system został naruszony oraz wdrożenie odpowiednich środków bezpieczeństwa. Właściciel systemu zostanie formalnie zawiadomiony na piśmie w terminie do *pięciu (5) dni roboczych* od wykrycia incydentu/incydentów.

Katastrofy i inne sytuacje awaryjne: Personel techniczny niezwłocznie zawiadomi swoich wyznaczonych odpowiedników, telefonicznie lub pocztą elektroniczną, o wystąpieniu katastrofy lub innej sytuacji awaryjnej, która zakłóca normalne działanie jednego lub obydwu połączonych systemów.

Istotne zmiany w konfiguracji systemu: Planowane zmiany techniczne w architekturze systemu będą zgłaszane personelowi technicznemu przed ich wdrożeniem. Strona inicjująca zgadza się przeprowadzić oszacowanie ryzyka w oparciu o nową architekturę systemu oraz zmodyfikować i ponownie podpisać ISA w terminie *jednego (1) miesiąca* od wdrożenia zmian.

Nowe połączenia: Strona inicjująca zawiadomi drugą stronę na co najmniej *jeden miesiąc* przed połączeniem swojego systemu informacyjnego z jakimikolwiek innymi systemami, w tym systemami, które należą i są użytkowane przez podmioty trzecie.

Zmiany w składzie personelu: Strony zgadzają się zawiadamiać o odejściu lub długiej nieobecności swojego właściciela systemu lub kierownika technicznego. Ponadto, obie strony będą zawiadamiać o wszelkich zmianach w informacjach dotyczących punktu kontaktowego. Obie strony będą również zawiadamiać o zmianach profili użytkowników, w tym użytkowników, którzy ponownie obejmują lub zmieniają swoje obowiązki.

UMOWA O BEZPIECZNYM POŁĄCZENIU SYSTEMÓW

Szczegóły techniczne połączenia zostaną udokumentowane w Umowie o bezpiecznym połączeniu systemów (ISA). Strony zgadzają się wspólnie opracować ISA, która musi zostać podpisana przez obydwie strony przed uruchomieniem połączenia. Proponowane zmiany któregokolwiek systemu lub medium połączenia będą podlegać

przeglądowi i ocenie w celu ustalenia ich ewentualnego wpływu na połączenie. ISA zostanie renegocjowana przed wprowadzeniem zmian. ISA zostanie podpisana przez osoby autoryzujące każdego systemu.

BEZPIECZEŃSTWO

Obydwie strony zgadzają się współpracować dla zapewnienia wspólnego bezpieczeństwa połączonych systemów oraz danych, które są w nich przechowywane, przetwarzane i przesyłane, zgodnie z postanowieniami ISA. W oparciu o publikację NSC 800-53, obie strony powinny autoryzować wszystkie połączenia z systemu informacyjnego do innych systemów informacyjnych poza granicami akredytacji oraz na bieżąco monitorować i kontrolować wzajemne połączenia systemowe. Każda ze stron powinna określić środki bezpieczeństwa zastosowane do podłączania w oparciu o kategoryzację bezpieczeństwa informacji i poziom wpływu każdego z systemów oraz uzgodnić zestaw wzajemnych zabezpieczeń. Każda ze stron zaświadcza, że jej system jest zaprojektowany, zarządzany i użytkowany zgodnie z wszelkimi stosownymi przepisami, rozporządzeniami i zaleceniami oraz zapewni utrzymanie odpowiednich zabezpieczeń przez cały okres obowiązywania niniejszego MOU/MOA.

WYMAGANIA DOTYCZĄCE OCHRONY PRYWATNOŚCI

Obie strony zgadzają się zbadać kwestie ochrony prywatności związane z danymi, które będą podlegać wymianie lub przekazaniu za pośrednictwem połączenia, a także ustalą, czy takie wykorzystanie podlega ograniczeniom na mocy obowiązujących ustaw, rozporządzeń lub przyjętych polityk. Wśród danych, które mogą podlegać ograniczeniom są takie dane osobowe, jak *nazwiska*, *PESEL i adresy*, czy takie poufne informacje biznesowe, jak *stawki ofertowe wykonawców i tajemnice handlowe*. Każda ze stron powinna skonsultować się ze swoim *inspektorem ochrony danych* lub *radcą prawnym w* celu ustalenia czy informacje takie mogą zostać udostępniane lub przesyłane. Zezwolenie na wymianę lub przesył informacji powinno zostać udokumentowane wraz z zobowiązaniem do ochrony takich danych.

UZGODNIENIA FINANSOWE

Obie strony zgadzają się w równym stopniu dzielić kosztami mechanizmu i/lub mediów połączenia, przy czym poniesienie wszelkich związanych z tym wydatków lub

zobowiązań finansowych wymaga pisemnej zgody obu stron. Odpowiedzialność za dokonanie zmian systemowych niezbędnych do obsługi połączenia spoczywa na organizacji odpowiedniego właściciela systemu.

RAMY CZASOWE

Niniejsza umowa obowiązuje przez jeden *(1) rok* od daty złożenia ostatniego podpisu w polu poniżej. Niniejsza umowa wygasa, jeżeli po upływie *jednego (1) roku* nie zostaną podjęte dalsze działania. Jeżeli strony zechcą przedłużyć niniejszą umowę, mogą to uczynić poprzez dokonanie jej przeglądu, aktualizacji i ponownej autoryzacji. Nowo podpisana umowa powinna w sposób wyraźny zastępować niniejszą umowę, którą należy w takim przypadku zidentyfikować tytułem i datą. Jeżeli jedna lub obie strony zechcą rozwiązać niniejszą umowę przed datą upływu jej ważności, mogą to zrobić z zachowaniem *trzydziestodniowego* okresu wypowiedzenia albo w przypadku wystąpienia incydentu bezpieczeństwa wymagającego niezwłocznej reakcji.

OSOBY UPOWAŻNIONE DO PODPISANIA DOKUMENTU

Zgadzam się z postanowieniami niniejszego Protokołu uzgodnień/Porozumienia o współpracy.

(Osoba upoważniona Organizacji A) ***(Osoba upoważniona Organizacji B)***

_____ _____

(Podpis Data) (Podpis Data)

Załącznik 6.B Lista kontrolna umowy o bezpiecznym połączeniu systemów

Niniejszy załącznik zawiera ogólną listę kontrolną, z której organizacje mogą skorzystać przy opracowywaniu swoich umów o bezpiecznym połączeniu systemów (ISA), aby upewnić się, że uwzględniono wszystkie wymagania przedstawione w tym rozdziale.

LISTA KONTROLNA ISA[51]		TAK	NIE
1	**Wymagania dotyczące ISA:**		
A	Czy istnieje formalny wymóg i uzasadnienie połączenia dwóch systemów?		
B	Czy połączenie dotyczy dwóch systemów? • Jeżeli tak, czy zostały one określone? • Jeżeli nie, obydwa systemy należy określić.		
C	Czy istnieje lista korzyści z wymaganego połączenia/wymaganych połączeń?		
D	Czy podano nazwę lub organizację organizacji, która zainicjowała wymóg połączenia?		
2	**Kwestie związane z bezpieczeństwem systemu:**		
A	Czy przeprowadzono certyfikację i akredytację bezpieczeństwa systemu?		
B	Czy zweryfikowano status certyfikacji i akredytacji bezpieczeństwa?		
C	Czy wprowadzono zabezpieczenia chroniące poufność, integralność i dostępność łączonych systemów i danych?		
D	Czy kategorię bezpieczeństwa każdego z systemów określono zgodnie z NSC 199?		
E	Czy dla każdego z systemów określono minimalne zabezpieczenia zgodnie z NSC 800-53?		
F	Czy obie strony odpowiedziały na każdą pozycję, niezależnie od tego, czy dany punkt dotyczy tylko jednej strony?		

[51] Kursywą zaznaczona pola, które organizacje powinny wypełnić zgodnie z poczynionymi ustaleniami w dniu zawierania umowy.

LISTA KONTROLNA ISA[51]		TAK	NIE
	Jeżeli nie, obie strony muszą się cofnąć i odpowiedzieć na każdą z nich.		
G	Czy istnieje ogólny opis informacji/danych, które będą podlegać udostępnieniu, wymianie lub przekazaniu?		
H	Czy opisano usługi informacyjne (np. e-mail, protokół transferu plików, zapytania do bazy danych, zapytania o pliki, ogólne usługi obliczeniowe) świadczone przez każdą z uczestniczących organizacji za pośrednictwem połączonego systemu?		
I	Czy zidentyfikowano użytkowników systemu i czy wydano odpowiednie zatwierdzenie?		
J	Czy opisano wszystkie usługi techniczne związane z bezpieczeństwem systemu dotyczące bezpiecznej wymiany informacji/danych między przedmiotowymi systemami?		
K	Czy udokumentowano zasady zachowania obowiązujące użytkowników każdego z systemów objętych połączeniem?		
L	Czy istnieją zapisy formalnej polityki bezpieczeństwa, które regulują każdy system?		
M	Czy istnieją procedury obsługi incydentów dotyczących połączenia?		
N	Czy istnieją wymagania dotyczące audytów?		
3	**Topologia połączenia międzysystemowego:**		
A	Czy sporządzono opisową specyfikację techniczną połączeń?		
4	**Osoby upoważnione do podpisania dokumentu: ISA pozostaje ważna przez *rok od daty* złożenia ostatniego podpisu w polu poniżej. W tym czasie będzie ona poddawana przeglądowi, w razie konieczności aktualizowana, a także poddawana ponownej walidacji. Niniejszą umowę można rozwiązać z zachowaniem *trzydziestodniowego* okresu wypowiedzenia albo w przypadku wystąpienia wyjątku związanego z bezpieczeństwem, który wymagałby niezwłocznej reakcji.**		

REFERENCJE:

Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

Federal Information Processing Standard 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

National Institute of Standards and Technology, Information Technology Laboratory (ITL) Bulletin: *Secure Interconnections for Information Technology Systems*, February 2003.

National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

National Institute of Standards and Technology Special Publication 800-42, *Guidelines on Network Security Testing*, October 2003.

National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.

National Institute of Standards and Technology Special Publication 800-53, *Revision 1*, *Recommended Security Controls for Federal Information System*, February 2006.

National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.

ROZDZIAŁ 7

7. MIARY WYNIKÓW

Program miar wyników daje organizacjom wiele korzyści organizacyjnych i finansowych. Organizacje mogą opracować metryki bezpieczeństwa informacji mierzące skuteczność swoich programów bezpieczeństwa oraz zapewnić menadżerom i właścicielom systemów dane do analizy i wykorzystania w celu wyodrębnienia problemów, uzasadniania wniosków inwestycyjnych oraz kierowania funduszy dokładnie do obszarów wymagających poprawy. Dzięki wykorzystaniu metryk do kierowania środków do inwestycji w bezpieczeństwo, organizacje mogą uzyskać najlepszą wartość z dostępnych funduszy. Typowy program zarządzania wydajnością informacji zazwyczaj składa się z czterech współzależnych komponentów: wsparcie ze strony wyższego kierownictwa, zasady i procedury bezpieczeństwa, wymierne metryki wyników oraz analizy.

Zdecydowane wsparcie ze strony wyższego kierownictwa sprawia, że bezpieczeństwo znajduje się w centrum uwagi na najwyższych szczeblach organizacji. Bez solidnego fundamentu (np. czynnego wsparcia ze strony osób na stanowiskach dających kontrolę nad zasobami informacyjnymi), program metryk bezpieczeństwa może zawieść, jeżeli znajdzie się pod presją polityki i ograniczeń budżetowych. Drugim komponentem skutecznego programu metryk bezpieczeństwa są praktyczne zasady i procedury bezpieczeństwa wsparte upoważnieniami niezbędnymi do egzekwowania zgodności. Nie jest łatwo uzyskać metryki, kiedy nie ma stosownych polityk i procedur. Trzecim komponentem jest opracowanie i ustanowienie metryk wyników wychwytujących i dostarczających istotnych dane o wynikach. Aby uzyskane dane były istotne, wymierne metryki wyników muszą zostać oparte na celach i atrybutach bezpieczeństwa informacji oraz być łatwe do uzyskania, powtarzalne, istotne i możliwe do zmierzenia. Wreszcie, sam program metryk bezpieczeństwa musi kłaść nacisk na konsekwentne, okresowe analizowanie danych pochodzących z metryk. Wyniki tej analizy są wykorzystywane do stosowania wyciągniętych wniosków, poprawy skuteczności istniejących zabezpieczeń i planowania przyszłych zabezpieczeń w celu spełnienia pojawiających się nowych wymagań w zakresie bezpieczeństwa.

Jeżeli zebrane dane mają być istotne dla zarządzania i ułatwienia usprawnienia ogólnego planu bezpieczeństwa, to priorytetem dla interesariuszy i użytkowników musi być zbieranie dokładnych danych.

Szereg obowiązujących przepisów, zasad i regulacji wymienia pomiary efektywności technologii informacyjnych (IT) jako wymagania ogólne, a pomiary efektywności bezpieczeństwa informacji jako wymagania szczególne.

Publikacja specjalna NIST SP 800-55, *Security Metrics Guide for Information Technology Systems*, dostarcza wskazówek w zakresie wykorzystywania metryk przez organizację do określania adekwatności już wdrożonych zabezpieczeń, polityk i procedur. Publikacja przedstawia podejście, które ma pomóc kierownictwu w decydowaniu, gdzie dokonywać inwestycji w dodatkowe zabezpieczenia albo w jaki sposób identyfikować i oceniać zabezpieczenia, które są bezproduktywne. NIST SP 800-55 wyjaśnia proces opracowywania i wdrażania metryk, a także sposobu ich wykorzystania do odpowiedniego uzasadniania inwestycji w zabezpieczenia. Wyniki skutecznego programu metryk mogą dostarczyć danych przydatnych w przydzielaniu zasobów bezpieczeństwa informacji i powinny uprościć sporządzanie sprawozdań dotyczących wydajności.

Ograniczenia budżetowe i warunki rynkowe zmuszają organizację i branżę do funkcjonowania w warunkach zmniejszonych budżetów. W takim środowisku trudno jest uzasadnić szeroko zakrojone inwestycje w infrastrukturę bezpieczeństwa informacji. W ujęciu historycznym, argumenty za inwestowaniem w konkretne obszary bezpieczeństwa informacji są za mało szczegółowe i w nieadekwatny sposób łagodzą konkretne ryzyka systemowe. Metryki bezpieczeństwa informacji mogą ułatwić proces planowania budżetowego i kontroli inwestycji przez dostarczenie wymiernych informacji na potrzeby opracowywania uzasadnień biznesowych[52]. Metryki bezpieczeństwa informacji mogą również wspomóc ustalania skuteczności wdrożonych procesów, procedur i środków bezpieczeństwa informacji poprzez odniesienie

[52] Dodatkowe informacje w zakresie opracowywania uzasadnień biznesowych, zob. NIST SP 800-65, *Integrating Security into the Capital Planning and Investment Control* Process, a także Rozdział 5 „Planowanie finansowe" niniejszego podręcznika.

wyników działań z zakresu bezpieczeństwa informacji (np. danych o incydentach, przychodów utraconych w wyniku cyberataków) do odpowiednich wymagań oraz inwestycji w bezpieczeństwo informacji.

Organizacje mogą też wykazać zgodność z obowiązującymi przepisami, zasadami i regulacjami poprzez wdrożenie i utrzymanie programu metryk bezpieczeństwa informacji zgodnie z treścią niniejszego podręcznika. Metryki bezpieczeństwa informacji pomogą w spełnieniu wymogu składania sprawozdań poprzez zapewnienie infrastruktury do zorganizowanego zbierania, analizy i raportowania danych. Mogą być też wykorzystywane jako dane wejściowe dla audytów przeprowadzanych stosowne podmioty.

7.1. RODZAJE METRYK

Metryki to narzędzia wspierające podejmowanie decyzji. Podobnie jak doświadczenie, uprawnienia zewnętrzne i strategie, metryki stanowią element zestawu narzędzi menadżera służący uzasadnianiu decyzji. Metryki są wykorzystywane do odpowiedzi na trzy podstawowe pytania:

- *„Czy wdrażam zadania, za które jestem odpowiedzialny?”* Rozważmy przykład menadżera programu odpowiedzialnego za 250 systemów informacyjnych. Do jego obowiązków należy m.in. certyfikacja i akredytacja bezpieczeństwa tych systemów. Powszechnie stosowaną metryką wdrożeniową dla certyfikacji i akredytacji bezpieczeństwa jest odsetek akredytowanych systemów.
- *„Jak wydajnie i skutecznie realizuję te zadania?”* Metryki często odpowiadają na bardziej złożone pytania po pełnym wykonaniu zadania. Na przykład, przepisy wymagają, aby po znaczącej zmianie systemu przeprowadzić certyfikację i akredytację bezpieczeństwa. Wydajność programu certyfikacji i akredytacji bezpieczeństwa można zmierzyć poprzez ustalenie czasu, jaki upływa między każdą znaczącą zmianą systemu i ponowną akredytacją tego systemu. Skuteczność programu certyfikacji i akredytacji bezpieczeństwa można też zmierzyć ustalając liczbę akredytowanych systemów, w przypadku których proces certyfikacji obejmował stworzenie planu bezpieczeństwa systemu.

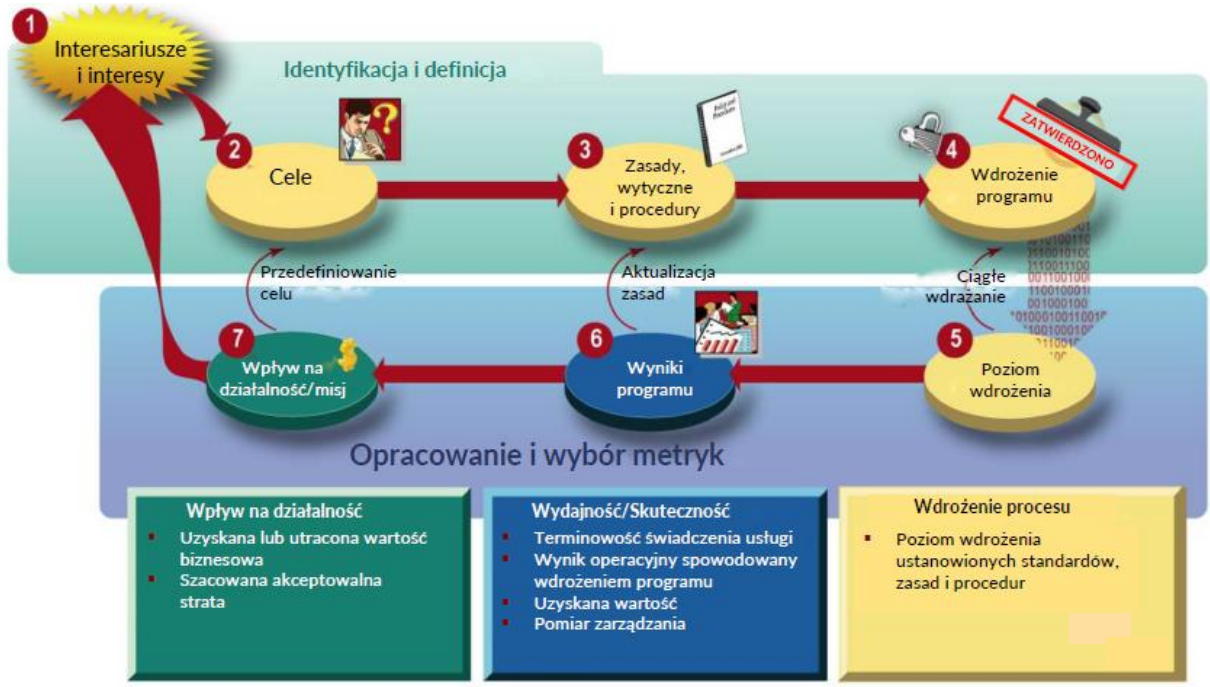
- *„Jaki jest wpływ tych zadań na misję?”* Działania są początkowo wybierane z założeniem, że przyczynią się do realizacji misji. Po wykazaniu pełnej realizacji działania, menadżerowie muszą potwierdzić, czy daje ono oczekiwane korzyści. Te metryki najtrudniej wygenerować. Wpływ procesu certyfikacji i akredytacji bezpieczeństwa można wykazać przez pokazanie mniejszej liczby zakłóceń lub przypadków utraty danych z powodu incydentów bezpieczeństwa występujących w prawidłowo akredytowanych systemach w porównaniu z systemami akredytowanymi nieprawidłowo lub nieakredytowanymi wcale.

7.2. OPRACOWANIE METRYK I PODEJŚCIE DO WDROŻENIA

Ustanowieniem i funkcjonowaniem programu metryk bezpieczeństwa informacji kierują dwa procesy: opracowanie metryk i wdrożenie metryk. Proces rozwoju metryki skutkuje ustanowieniem początkowego zbioru metryk i wyborem podzbioru metryk, który jest odpowiedni dla danej organizacji w danym czasie. Proces wdrażania programu metryki wykorzystuje metrykę, która jest z natury iteracyjna i zapewnia pomiar odpowiednich aspektów bezpieczeństwa informacji w określonym czasie.

7.3. PROCES OPRACOWANIA METRYK

Rysunek 7-1 przedstawia umiejscowienie metryk bezpieczeństwa informacji w szerszym kontekście organizacyjnym i demonstruje, że mogą one być wykorzystane do stopniowego pomiaru wdrażania, wydajności, skuteczności i wpływu działań z zakresu bezpieczeństwa informacji w obrębie organizacji lub konkretnych systemów.



Rysunek 7-1. Proces opracowywania metryk bezpieczeństwa informacji

Na proces opracowania metryki bezpieczeństwa informacji składają się dwa główne działania:

1. zidentyfikowanie i zdefiniowanie aktualnego programu bezpieczeństwa informacji;
2. opracowanie i dobór konkretnych metryk do pomiaru wdrażania, wydajności, skuteczności i wpływu środków bezpieczeństwa.

Etapy procesu nie muszą następować po kolei. Proces przedstawiony na rys. 7-1 zapewnia ramy dla rozważań o metrykach i pomaga w identyfikacji metryk, które trzeba opracować dla każdego systemu. Rodzaj metryk zależy od miejsca, w jakim system znajduje się w swoim cyklu życia oraz od zaawansowaniu programu bezpieczeństwa systemu informacyjnego. Ramy te ułatwiają dostosowanie metryk do konkretnej organizacji i różnych grup interesariuszy obecnych w każdej organizacji.

Przedstawione na rys. 7-1 fazy 5, 6 i 7 obejmują opracowanie metryk mierzących stopień realizacji procesu, a także jego skuteczność i wydajność oraz wpływ na misję. To na jakim konkretnym aspekcie bezpieczeństwa informacji skupią się metryki w danym momencie będzie zależeć od stopnia dojrzałości programu bezpieczeństwa

informacji. Charakter materiału dowodowego z procesu wdrożenia, wymaganego do wykazania osiągnięcia wyższych poziomów skuteczności, będzie różny, począwszy od ustanowienia istnienia zasad i procedur, przez kwantyfikację ich wdrożenia, aż po identyfikację wpływu tego wdrożenia na misję organizacji.

Na podstawie istniejących zasad i procedur, uniwersum możliwych metryk może być nadmiernie rozległy. Organizacje powinny zatem ustalić priorytety metryk, aby zapewnić, że ich ostateczny zestaw wybrany do wstępnego wdrożenia ma następujące cechy:

- ułatwia wdrożenie zabezpieczeń o wysokim priorytecie. Wysoki priorytet może być określony w najnowszych sprawozdaniach, wynikach oceny ryzyka lub w wewnętrznych celach organizacji;
- wykorzystuje dane, które można realnie uzyskać z istniejących procesów i repozytoriów danych;
- mierzy procesy, które już istnieją i są stosunkowo stabilne. Mierzenie nieistniejących lub niestabilnych procesów nie da istotnych informacji na temat wydajności bezpieczeństwa, a zatem nie przyda się w kierowaniu uwagi na konkretne aspekty tej wydajności. Z drugiej strony, próby wykonania takich pomiarów nie muszą być całkowicie bezcelowe, ponieważ takie metryki z pewnością wykażą słabą wydajność, tym samym wskazując na obszar, który wymaga poprawy.

Metryki można wyprowadzić z istniejących źródeł danych, w tym certyfikacji i akredytacji bezpieczeństwa, ocen bezpieczeństwa, planu i etapów działania, statystyk dotyczących incydentów oraz przeglądów niezależnych lub zainicjowanych przez organizację[53]. Organizacje mogą zdecydować o zastosowaniu skali wag do odróżnienia znaczenia wybranych metryk i zapewnienia, aby wyniki dokładnie odzwierciedlały istniejące priorytety programu bezpieczeństwa. Proces obejmowałby przypisanie wartości każdej metryce na podstawie jej znaczenia w kontekście ogólnego programu

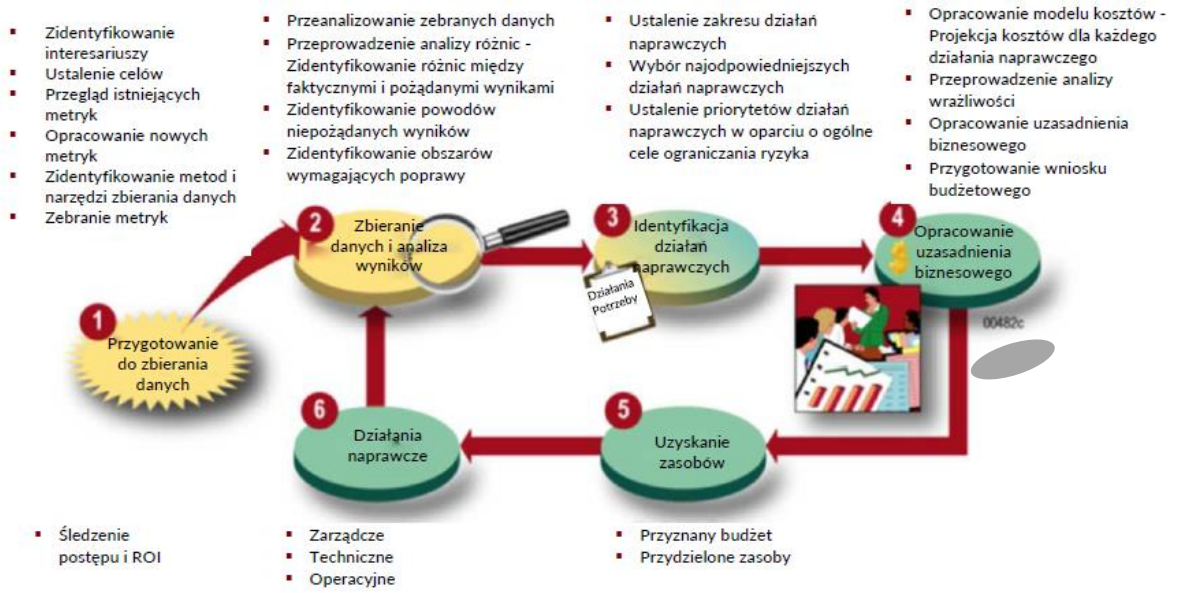
[53] Dodatkowe wytyczne w zakresie ocen bezpieczeństwa, zob. NSC 800-30, a także Rozdział 10 „Zarządzanie ryzykiem" i Rozdział 11 „Certyfikacja, akredytacja i oceny bezpieczeństwa" niniejszego podręcznika.

bezpieczeństwa. Waga metryk powinna opierać się na ogólnych celach w zakresie mitygacji ryzyka. Prawdopodobnie odzwierciedli większą krytyczność inicjatyw realizowanych na poziomie organizacji od inicjatyw o mniejszej skali, a także jest przydatnym narzędziem ułatwiającym integrację bezpieczeństwa informacji z procesem planowania finansowego w organizacji.

Stopniowe podejście może być wymagane do identyfikowania metryk krótko-, średnio- i długoterminowych, w przypadku których czasowe ramy wdrożenia zależą od połączenia skuteczności na poziomie systemu, priorytetów w zakresie metryk, dostępności danych i stabilności systemu. Po zidentyfikowaniu stosownych metryk zawierających wyżej opisane cechy, należy je udokumentować przy użyciu takich szczegółów pomocniczych, jak częstotliwość zbierania danych, źródło danych, formuła obliczania, dowody wdrożenia dla mierzonego działania oraz wskazówki do interpretacji danych metryki. Pozostałe informacje na temat każdej z metryk można określić w oparciu o wymagania organizacji w zakresie przetwarzania oraz wymagania biznesowe.

7.4. WDROŻENIE PROGRAMU METRYK

Metryki bezpieczeństwa informacji powinny być wykorzystywane do monitorowania wydajności zabezpieczeń oraz inicjowania działań ją poprawiających. Ten powtarzający się proces składa się z sześciu faz, co przedstawiono na rys. 7-2.



Rysunek 7-2. Proces wdrożenia programu metryk bezpieczeństwa informacji

7.4.1. PRZYGOTOWANIE DO ZBIERANIA DANYCH

Faza 1 procesu, czyli przygotowanie do zbierania danych, obejmuje działania, które są kluczowe do ustanowienia kompleksowego programu metryk bezpieczeństwa informacji. Do działań tych należy zidentyfikowanie, zdefiniowanie, opracowanie i dobór metryk bezpieczeństwa informacji oraz opracowanie planu wdrożenia programu metryk.

Po zidentyfikowaniu metryk, należy zdefiniować konkretne kroki dotyczące sposobu ich zbierania, analizowania i raportowania. Kroki te powinny zostać udokumentowane w planie wdrożenia programu metryk. W planie można uwzględnić następujące elementy:

- role i obowiązki w zakresie metryk, w tym obowiązki w zakresie zbierania danych (zarówno dotyczące występowania o nie, jak i dostarczania), analizy i sprawozdawczości;
- adresaci planu;
- proces zbierania, analizy i raportowania metryk dostosowany do konkretnej struktury organizacyjnej, procesów, polityk i procedur;
- szczegóły dotyczące koordynacji z CIO, np. w zakresie szacowania ryzyka, certyfikacji i akredytacji bezpieczeństwa oraz sprawozdawczości;
- szczegóły dotyczące koordynacji między CIO i innymi funkcjami w organizacji zewnętrznymi wobec CIO (np. w zakresie wiarygodności informacji, jeżeli nie mieści się to w zakresie kompetencji CIO, bezpieczeństwo fizyczne, bezpieczeństwo osobowe oraz ochrona infrastruktury kluczowej) w celu zapewnienia sprawnego i nieinwazyjnego zbierania danych;
- stworzenie lub dobór narzędzi zbierania i śledzenia danych;
- modyfikacje narzędzi zbierania i śledzenia danych;
- format raportowania podsumowania metryk.

7.4.2. ZBIERANIE DANYCH I ANALIZA WYNIKÓW

Faza 2 procesu, czyli zbieranie danych i analiza wyników, obejmuje działania niezbędne dla zapewnienia, aby gromadzone metryki służyły zrozumieniu bezpieczeństwa systemu oraz identyfikowaniu odpowiednich działań doskonalących. Ta faza obejmuje:

- gromadzenie metryk zgodnie z procesami zdefiniowanymi w planie programu wdrożenia metryk,
- skonsolidowanie zebranych danych i przechowanie ich w formacie sprzyjającym analizie i raportowaniu (tzn. baza danych lub arkusz kalkulacyjny),
- przeprowadzenie analizy luk, porównanie zebranych pomiarów z celami (o ile takowe zdefiniowano) oraz zidentyfikowanie luk między faktycznymi pożądanymi wynikami,
- zidentyfikowanie przyczyn słabych wyników,
- zidentyfikowanie obszarów wymagających poprawy.

Przyczyny słabych wyników często można zidentyfikować przy użyciu danych pochodzących z więcej niż jednej metryki. Na przykład, ustalenie, że odsetek zatwierdzonych planów bezpieczeństwa jest niedopuszczalnie niski nie byłoby pomocne w ustaleniu sposobu naprawy problemu. Aby ustalić powód niskiego poziomu zgodności należy zebrać informacje o przyczynach niskiej zgodności (np. brak wytycznych, niewystarczająca wiedza specjalistyczna lub sprzeczne priorytety). Te informacje można zebrać jako oddzielne metryki lub dowody wdrożenia dotyczące odsetka zatwierdzonych planów bezpieczeństwa. Po zebraniu i skompilowaniu tych informacji organizacja powinna opracować plan naprawczy dotyczący źródłowej przyczyny problemu.

Przyczyny źródłowe wadliwego bezpieczeństwa tworzą szeroką gamę – od zaawansowanych technicznie kwestii złej konfiguracji aż po brak wyszkolenia albo przestarzałe polityki lub praktyki. Poniżej przedstawiono przykłady czynników przyczynowo-skutkowych leżących u podstaw słabego wdrożenia i skuteczności zabezpieczeń:

- zasoby—niewystarczające zasoby ludzkie, finansowe lub inne;

- szkolenie—brak odpowiednich szkoleń dla personelu instalacyjnego, administrującego, utrzymującego lub użytkującego systemy;
- modernizacja systemu—poprawki bezpieczeństwa, które zostały usunięte, ale nie zastąpione podczas modernizacji systemu operacyjnego;
- praktyki z zakresu zarządzania konfiguracją—nowe lub zmodernizowane systemy, których nie skonfigurowano przy użyciu wymaganych ustawień i poprawek bezpieczeństwa;
- kompatybilność oprogramowania—poprawki bezpieczeństwa lub modernizacje, które są niekompatybilne z aplikacjami obsługiwanymi przez system;
- świadomość i zaangażowanie—brak świadomości i/lub zaangażowania w zakresie bezpieczeństwa ze strony kierownictwa;
- zasady i procedury—brak zasad i procedur wymaganych do zapewnienia istnienia, użytkowania i audytów wymaganych funkcji bezpieczeństwa;
- architektura—słaba infrastruktura systemowa i bezpieczeństwa, która sprawia, że systemy są podatne na ataki;
- niewydajne procesy—niewydajne procesy planowania i komunikacji mające wpływ na metryki.

7.4.3. IDENTYFIKACJA DZIAŁAŃ NAPRAWCZYCH

Faza 3 procesu, czyli identyfikacja działań naprawczych, obejmuje opracowanie planu, który będzie mapą drogową sposobu załatania luki wdrożeniowej zidentyfikowanej w Fazie 2. Ta faza obejmuje:

- **Ustalenie zakresu działań naprawczych.** Na podstawie wyników i czynników przyczynowo-skutkowych należy zidentyfikować działania naprawcze, które można zastosować do każdego z problemów. Działania naprawcze mogą polegać na zmianie konfiguracji systemu, przeszkoleniu personelu odpowiedzialnego za bezpieczeństwo, administratorów systemu lub zwykłych użytkowników, zakupie narzędzi bezpieczeństwa, zmianie architektury systemu, ustanowienia nowych procesów i procedur oraz aktualizacji zasad bezpieczeństwa.

- **Ustalenie priorytetów działań naprawczych w oparciu o ogólne cele mitygacji ryzyka.** Do jednego problemu z wydajnością zastosowanie może mieć kilka działań naprawczych. Niektóre z nich mogą być jednak niewłaściwe, jeżeli nie odpowiadają skali problemu lub są zbyt drogie. Należy ustalić priorytety stosownych działań naprawczych dla każdego z problemów z wydajnością, porządkując je od najniższego do najwyższego kosztu oraz od najwyższego do najniższego wpływu. Do ustalenia priorytetów działań naprawczych należy wykorzystać proces zarządzania ryzykiem, opisany w publikacji NSC 800-30[54]. W przypadku przypisania wag do metryk w Fazie 1 (przygotowania do zbierania danych), wagi te powinny zostać użyte do ustalenia priorytetów dla działań naprawczych. Ewentualnie, wagi można przypisać do działań naprawczych w Fazie 3 (*Identyfikacja działań naprawczych*) na podstawie newralgiczności wdrożenia poszczególnych działań naprawczych, ich kosztu oraz siły wpływu na stan bezpieczeństwa organizacji.
- **Wybór najodpowiedniejszych działań naprawczych.** Do przeprowadzenia analizy kosztów i korzyści należy wybrać do trzech działań naprawczych z listy najwyższych priorytetów. Wybór powinien być odpowiednio odzwierciedlony w POA&M organizacji lub systemu.

7.4.4. OPRACOWANIE UZASADNIENIA BIZNESOWEGO I POZYSKANIE ZASOBÓW

Fazy 4 i 5, czyli opracowanie uzasadnienia biznesowego i pozyskanie zasobów, dotyczą cyklu budżetowania wymaganego do pozyskania zasobów potrzebnych do wdrożenia działań naprawczych, o których mowa w Fazie 3. Kroki opracowania uzasadnienia biznesowego opierają się na praktykach branżowych i zaleconych wytycznych. Wynik trzech wcześniejszych faz należy włączyć do uzasadnienia biznesowego jako dowody potwierdzające. Wkład osób zawodowo zajmujących się bezpieczeństwem w proces CPIC oraz role pełnione przez te osoby w głównym procesie planowania przedstawiono w publikacji NIST SP 800-55.

---

[54] Dodatkowe wytyczne w zakresie ustalania priorytetów działań naprawczych, zob. też Rozdział 10 „Zarządzanie ryzykiem” i Rozdział 11 „Certyfikacja, akredytacja i oceny bezpieczeństwa” niniejszego podręcznika.

W tej fazie każda organizacja powinna postępować zgodnie z właściwymi dla niej wytycznymi w zakresie uzasadnienia biznesowego. Ukończenie wewnętrznych i zewnętrznych wniosków budżetowych zazwyczaj staje się łatwiejsze, jeżeli wykorzystane zostaną elementy i analiza działalności. Dokładna analiza uzasadnienia biznesowego będzie wsparciem i ułatwieniem podczas pozyskiwania zasobów.

7.4.5. ZASTOSOWANIE DZIAŁAŃ NAPRAWCZYCH

Faza 6 procesu, czyli zastosowanie działań naprawczych, polega na wdrożeniu tych działań zgodnie z ustaleniami poczynionymi w wyniku analizy danych oraz według stosownego uzasadnienia biznesowego lub POA&M. Po zastosowaniu działań naprawczych, cykl sam się kończy i rozpoczyna od nowa ze zbieraniem i analizą kolejnych danych. Wielokrotne zbieranie, analizowanie i raportowanie danych będzie umożliwiać śledzenie postępu realizacji działań naprawczych poprzez POA&M oraz identyfikowanie obszarów do dalszej poprawy, które zostaną włączone do planów taktycznych, planów zarządzania programem lub innych organizacyjnych mechanizmów planowania. Powtarzalny charakter cyklu zapewnia, że proces jest monitorowany, a działania naprawcze mają wpływ na wdrażanie zabezpieczeń systemu w sposób zgodny z zamierzeniami. Częste pomiary wydajności zapewnią, że w przypadku niewdrożenia działań naprawczych zgodnie z planem albo gdy ich faktyczny skutek nie jest zgodny z pożądanym, organizacja będzie mogła sama szybko skorygować kierunek, tym samym unikając ujawnienia problemów podczas zewnętrznych audytów, działań z zakresu certyfikacji i akredytacji bezpieczeństwa lub innych podobnych działań.

REFERENCJE:

National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

National Institute of Standards and Technology Special Publication 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003.

ROZDZIAŁ 8

8. PLANOWANIE BEZPIECZEŃSTWA

Dzisiejsze szybko zmieniające się środowisko techniczne wymaga od organizacji przyjęcia minimalnego zestawu zabezpieczeń w celu ochrony swoich informacji i systemów informacyjnych. Celem planu bezpieczeństwa systemu jest przedstawienie przeglądu wymagań bezpieczeństwa systemu i opisanie zabezpieczeń, które zostały wprowadzone lub zaplanowane do wprowadzenia w celu spełnienia tych wymagań. Plan bezpieczeństwa systemu określa również obowiązki i oczekiwane zachowanie wszystkich osób uzyskujących dostęp do systemu. Powinien odzwierciedlać wkład różnych menedżerów odpowiedzialnych za system, w tym właścicieli informacji, właściciela systemu oraz kluczowej osoby w jednostce organizacyjnej odpowiedzialnej za bezpieczeństwo informacji (*ang. Senior Agency Information Security Officer - SAISO*). Organizacje mogą według własnego uznania zawierać w ogólnym planie dodatkowe informacje oraz rozszerzać jego treść o dodatkowe rozdziały, o ile główne rozdziały opisane w niniejszym dokumencie zostaną odpowiednio ujęte i będą łatwe do zidentyfikowania.

Menedżerowie programów, właściciele systemów i personel ochrony w organizacji muszą zrozumieć proces planowania bezpieczeństwa systemu. Ponadto z procesem planowania bezpieczeństwa systemu powinni zapoznać się użytkownicy systemu informacyjnego i osoby odpowiedzialne za określenie wymagań systemowych, ponieważ plan bezpieczeństwa systemu jest ważnym produktem w procesie cyklu życia systemu (*SDLC*)[55]. Osoby odpowiedzialne za wdrażanie systemów informacyjnych i zarządzanie nimi muszą brać udział w podejmowaniu decyzji o ustanowieniu zabezpieczeń, które mają być stosowane w ich systemach.

Standard NSC 200 wer. 2 określa minimalne wymagania bezpieczeństwa dla informacji i systemów informacyjnych w dwudziestu kategoriach bezpieczeństwa. Organizacje powinny spełniać minimalne wymagania bezpieczeństwa określone w NSC 200

[55] Dodatkowe wytyczne w zakresie cyklu życia systemu, zob. NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*, a także Rozdział 3 „Cykl życia systemu" niniejszego podręcznika.

poprzez zastosowanie zabezpieczeń znajdujących się w publikacji NSC 800-53 oraz NSC 800-18, która w Załączniku A prezentuje wzór planu bezpieczeństwa systemu. Przedstawione poniżej wytyczne dostarczają podstawowych informacji o tym, jak przygotować plan bezpieczeństwa systemu zgodnie ze stosownymi wymaganiami. Można je łatwo dostosować do różnych struktur organizacyjnych.

8.1. APLIKACJE GŁÓWNE, SYSTEMY OGÓLNEGO WSPARCIA I APLIKACJE POMOCNICZE

Wszystkie systemy informacyjne muszą być objęte planem bezpieczeństwa systemu i skategoryzowane jako aplikacja główna (*ang. Major Application - MA*)[56] lub system ogólnego wsparcia (*ang. General Support System - GSS*)[57]. Dla aplikacji pomocniczych[58] nie są wymagane specjalne plany bezpieczeństwa systemu, ponieważ zabezpieczenia dla tych aplikacji są zazwyczaj zapewniane przez GSS lub MA w ramach, których działają. W przypadkach, gdzie aplikacja pomocnicza nie jest połączona z MA ani GSS, powinna ona zostać pokrótce opisana w planie GSS, który albo ma wspólną lokalizację fizyczną albo jest obsługiwany przez tę samą organizację.

8.2. ROLE I OBOWIĄZKI ZWIĄZANE Z PLANOWANIEM BEZPIECZEŃSTWA

Organizacje powinny opracować polityki dotyczące procesu planowania bezpieczeństwa systemu. Plany bezpieczeństwa systemu to żywe dokumenty, które wymagają okresowego przeglądu, modyfikacji oraz planów i etapów działania w celu wdrożenia zabezpieczeń. Powinny istnieć procedury określające, kto dokonuje przeglądu planów, utrzymuje plan na bieżąco i monitoruje zaplanowane zabezpieczenia. Ponadto procedury powinny wymagać opracowania i przeglądu

---

56 Aplikacja główna – aplikacja, która wymaga szczególnej ochrony ze względu na ryzyko i skalę szkód wynikających z utraty, niewłaściwego użycia lub nieautoryzowanego dostępu lub modyfikacji informacji w aplikacji.

57 System ogólnego wsparcia – połączony zestaw zasobów informacyjnych pod tą samą bezpośrednią kontrolą zarządczą, posiadający wspólną funkcjonalność. Zwykle obejmuje sprzęt, oprogramowanie, informacje, dane, aplikacje, środki telekomunikacji i personel.

58 Aplikacja pomocnicza -aplikacja inna niż aplikacja główna, która wymaga zwrócenia uwagi na bezpieczeństwo ze względu na ryzyko i skalę szkód wynikających z utraty, niewłaściwego użycia lub nieautoryzowanego dostępu do informacji w aplikacji lub ich modyfikacji. Aplikacje pomocnicze są zazwyczaj włączane jako część GSS.

planów bezpieczeństwa systemu przed przystąpieniem do procesu certyfikacji bezpieczeństwa i akredytacji systemu.

Podczas procesu certyfikacji i akredytacji bezpieczeństwa plan bezpieczeństwa systemu jest analizowany, aktualizowany i akceptowany. Organ certyfikacji potwierdza, że zabezpieczenia opisane w planie bezpieczeństwa systemu są zgodne z kategorią bezpieczeństwa NSC 199, określoną dla systemu informacyjnego oraz że identyfikacja zagrożeń, podatności i wstępne określenie ryzyka są zidentyfikowane oraz udokumentowane w planie bezpieczeństwa systemu, ocenie ryzyka lub równoważnym dokumencie. Wyniki certyfikacji bezpieczeństwa są wykorzystywane do ponownej oceny ryzyka, opracowania planu i etapów działania (*POA&M*), które są wymagane do śledzenia działań zaradczych i aktualizacji planu bezpieczeństwa systemu, zapewniając tym samym podstawę merytoryczną dla osoby autoryzującej do wydania decyzji o akredytacji bezpieczeństwa[59].

Role i obowiązki w tej sekcji dotyczą planowania bezpieczeństwa systemu informacyjnego. Uznając, że organizacje mają bardzo różne misje i struktury organizacyjne, mogą występować różnice w konwencjach nazewnictwa dla ról związanych z planowaniem bezpieczeństwa oraz w sposobie podziału powiązanych obowiązków między personelem organizacji (np. wiele osób pełniących jedną rolę lub jedna osoba pełniąca wiele ról)[60,61].

---

59 Dodatkowe wytyczne w zakresie procesu certyfikacji i akredytacji, zob. NSC 800-37, a także Rozdział 11 „Certyfikacja, akredytacja i oceny bezpieczeństwa" niniejszego podręcznika.

60 Należy zachować ostrożność w przypadku pełnienia wielu funkcji przez jedną osobę, zapewniając tej osobie zachowanie odpowiedniej niezależności i brak konfliktu interesów.

61 Dodatkowe wytyczne dotyczące ról i obowiązków w zakresie bezpieczeństwa, zob. Rozdział 2 „Zarządzanie", Rozdział 5 „Planowanie finansowe", Rozdział 11 „Certyfikacja, akredytacja i oceny bezpieczeństwa" oraz Rozdział 14 „Zarządzanie konfiguracją" niniejszego podręcznika.

8.2.1. CHIEF INFORMATION OFFICER - CIO

CIO (*ang. Chief Information Officer*)[62] to kluczowa osoba, która w organizacji odpowiada za opracowanie i utrzymanie obejmującego całą organizację programu bezpieczeństwa informacji. Przypisane obowiązki w zakresie planowania bezpieczeństwa systemu:

- wyznaczenie SAISO (*ang. Senior Agency Information Security Officer*), który będzie realizował zadania CIO w zakresie planowania bezpieczeństwa systemu;
- opracowanie i utrzymanie zasad bezpieczeństwa informacji, procedur i technik zabezpieczeń w celu uwzględnienia planowania bezpieczeństwa systemu;
- zarządzanie identyfikacją, wdrażaniem i oceną zabezpieczeń;
- zapewnienie przeszkolenia personelu odpowiedzialnego za plany bezpieczeństwa systemu;
- pomoc kierownikom komórek organizacyjnych w organizacji w wypełnianiu ich planów bezpieczeństwa systemu;
- identyfikowanie i opracowywanie zabezpieczeń w organizacji.

8.2.2. WŁAŚCICIEL SYSTEMU INFORMACYJNEGO

Właściciel systemu informacyjnego[63] (*ang. Information System Owner*) jest osobą w organizacji odpowiedzialną za zamówienia, rozwój, integrację, modyfikację lub obsługę i utrzymanie systemu informacyjnego. Właściciel systemu informacyjnego ma następujące obowiązki związane z planami bezpieczeństwa systemu:

- opracowanie planu bezpieczeństwa systemu w koordynacji z właścicielami informacji, administratorem systemu, ISSO (*ang. Information System Security Officer*), SAISO oraz użytkownikami końcowymi;

---

[62] W przypadku, gdy organizacja nie wyznaczyła formalnego stanowiska CIO, wymagane jest, aby związane z tym stanowiskiem obowiązki były pełnione przez osobę o porównywalnej randze w organizacji.

[63] Rolę właściciela systemu informacyjnego można interpretować na wiele sposobów w zależności od konkretnej organizacji i fazy SDLC w jakiej znajduje się system informacyjny. Niektóre organizacje mogą nazywać właścicieli systemu informacyjnego menadżerami programu lub właścicielami działalności/aktywów/misji.

- utrzymanie planu bezpieczeństwa systemu i zapewnienie, aby system był wdrażany i obsługiwany zgodnie z uzgodnionymi wymogami bezpieczeństwa;
- zapewnienie, aby użytkownicy systemu i personel pomocniczy zostali odpowiednio przeszkoleni w zakresie bezpieczeństwa (np. zgodnie z instrukcją dotyczącą zasad zachowania) oraz pomoc w identyfikacji, wdrażaniu i ocenie zabezpieczeń.

8.2.3. WŁAŚCICIEL INFORMACJI

Właściciel informacji (*ang. Information Owner*) jest osobą w organizacji posiadającą uprawnienia ustawowe, zarządcze lub operacyjne w zakresie określonych informacji oraz jest odpowiedzialny za ustanowienie polityki i procedur regulujących ich wytwarzanie, gromadzenie, przetwarzanie, rozpowszechnianie i usuwanie. Właściciel informacji ma następujące obowiązki związane z planami bezpieczeństwa systemu:

- ustanawianie zasad właściwego wykorzystania i ochrony danych/informacji organizacji (zasady zachowania)[64],
- dostarczanie właścicielom systemów informacyjnych informacji dotyczących wymagań bezpieczeństwa i zabezpieczeń systemów informacyjnych, w których przetwarzane są informacje,
- decydowanie, kto ma dostęp do systemu informacyjnego oraz z jakiego rodzaju przywilejami lub prawami dostępu, pomoc w identyfikacji i ocenie ogólnych zabezpieczeń systemów, w których znajdują się informacje.

8.2.4. SENIOR AGENCY INFORMATION SECURITY OFFICER - SAISO

SAISO jest osobą w organizacji pełniącą funkcję głównego łącznika CIO z właścicielami systemu informacyjnego i ISSO w organizacji. SAISO ma następujące obowiązki związane z planami bezpieczeństwa systemu:

- realizowanie zadań CIO w zakresie planowania bezpieczeństwa systemu,

[64] Właściciel informacji zachowuje tę odpowiedzialność nawet jeżeli te dane/informacje są udostępniane innym organizacjom.

- koordynacja opracowywania, przeglądu i akceptacji planów bezpieczeństwa systemu z właścicielami systemów informacyjnych, ISSO i osobą autoryzującą,
- koordynacja identyfikacji, wdrażania i oceny zabezpieczeń wspólnych,
- posiadanie kwalifikacji zawodowych, w tym przeszkolenia i doświadczenia, wymaganych do opracowania i przeglądu planów bezpieczeństwa systemu.

8.2.5. INFORMATION SYSTEM SECURITY OFFICER - ISSO

ISSO to osoba w organizacji, której SAISO, osoba autoryzująca, osoba zarządzająca lub właściciel systemu informacyjnego przypisali odpowiedzialność za zapewnienie utrzymania odpowiedniego poziomu bezpieczeństwa operacyjnego dla systemu informacyjnego. ISSO ma następujące obowiązki związane z planami bezpieczeństwa systemu:

- pomoc SAISO w identyfikacji, wdrażaniu i ocenie zabezpieczeń,
- odgrywanie aktywnej roli w opracowywaniu i utrzymaniu planu bezpieczeństwa systemu, a także koordynowaniu z właścicielem systemu informacyjnego wszelkich zmian w systemie i ocenie wpływu tych zmian na bezpieczeństwo.

8.3. ZASADY ZACHOWANIA

Zasady zachowania[65], które są również formą środków bezpieczeństwa zawartych w NSC 800-53, powinny jasno określać obowiązki i oczekiwane zachowanie wszystkich osób mających dostęp do systemu. Zasady powinny określać konsekwencje niespójnego zachowania lub niezgodności i być udostępniane każdemu użytkownikowi przed otrzymaniem autoryzacji na dostęp do systemu. Wymagane jest, aby zasady zawierały stronę podpisu dla każdego użytkownika potwierdzającą otrzymanie, wskazującą, że przeczytał, zrozumiał i zgodził się przestrzegać zasad zachowania. Podpisy elektroniczne są dopuszczalne do stosowania w uznaniu zasad zachowania.

W tabeli 8-1 przedstawiono zaczerpnięte z Załącznika do Okólnika OMB A-130 przykłady, co należy objąć typowymi zasadami postępowania. Są to tylko przykłady i organizacje mają

[65] Zasady zachowania stanowią rodzaj umowy dostępu dla użytkowników organizacyjnych. Przykładowo dla zainteresowanych- wymagane zgodnie z treścią Załącznika III do wydanego przez OMB Okólnika A-130.

swobodę w zakresie szczegółów i treści zasad zachowania. Opracowując zasady zachowania, należy pamiętać, że celem tego dokumentu jest uczynienie wszystkich użytkowników odpowiedzialnymi za swoje działania, potwierdzając, że przeczytali, zrozumieli i zgadzają się przestrzegać zasad zachowania. Zasady nie powinny być kompletną kopią przewodnika dotyczącego polityki bezpieczeństwa lub procedur, ale powinny obejmować, na wysokim poziomie, niektóre elementy zabezpieczeń opisane w tabeli 8-1. Na koniec należy zaznaczyć, że organizacje mogą włączać do treści zasad zachowania, w drodze odniesienia, własne polityki i procedury regulujące bezpieczeństwo informacji, a także inne stosowne zasady.

Tabela 8-1. Przykłady zasad zachowania

Przykłady zabezpieczeń zawartych w zasadach zachowania
• Określ obowiązki, oczekiwane sposoby wykorzystania systemu i zachowanie wszystkich użytkowników. • Opisz odpowiednie ograniczenia dotyczące wzajemnych kontaktów. • Zdefiniuj świadczone usługi i priorytety ich przywracania. • Wyraźnie informuj o konsekwencjach zachowania niezgodnego z zasadami. • Obejmij zasadami następujące zagadnienia: ✓ praca w domu, ✓ dostęp telefoniczny, ✓ dostęp do internetu, ✓ wykorzystanie dzieła chronionego prawem autorskim. ✓ nieoficjalne użycie sprzętu służbowego, ✓ przypisanie i ograniczenia uprawnień systemowych oraz indywidualnej odpowiedzialności, ✓ użycie hasła, ✓ przeszukiwanie baz danych i ujawnianie informacji.

8.4. ZATWIERDZENIE PLANU BEZPIECZEŃSTWA SYSTEMU

Zasady organizacyjne powinny jasno określać, kto jest odpowiedzialny za zatwierdzenie planu bezpieczeństwa systemu i opracowane procedury przedkładane wraz z planem lub inną dokumentacją wymaganą przez organizację. Przed procesem certyfikacji i akredytacji bezpieczeństwa plan jest zazwyczaj zatwierdzany przez osobę autoryzującą, niezależną od właściciela systemu.

8.4.1. ANALIZA GRANIC SYSTEMU I ŚRODKI BEZPIECZEŃSTWA

Przed opracowaniem planu bezpieczeństwa systemu, system informacyjny i informacje się w nim znajdujące muszą zostać skategoryzowane na podstawie analizy wpływu zakłócenia zgodnie z NSC 199[66]. Następnie można ustalić, które posiadane systemy można logicznie pogrupować w aplikacje główne lub systemy ogólnego wsparcia. Podczas wyznaczania granic systemu oraz doboru początkowego zestawu zabezpieczeń (np. zabezpieczeń bazowych) należy rozważyć poziomy wpływu podane w NSC 199. Zabezpieczenia bazowe można następnie dostosować w oparciu o ocenę ryzyka i lokalne uwarunkowania, w tym wymagania bezpieczeństwa właściwe dla organizacji, informacje o konkretnym zagrożeniu, analizy kosztów i korzyści, dostępność zabezpieczeń kompensacyjnych lub szczególnych okoliczności.

Przed opracowaniem planu bezpieczeństwa systemu należy zidentyfikować zabezpieczenia wspólne, które są jednym z aspektów dostosowywania, aby zidentyfikować i uwzględnić zabezpieczenia poczynione na poziomie organizacji (np. zabezpieczenia fizyczne i środowiskowe), które nie są specyficzne dla systemu. Zabezpieczenia wspólne można następnie włączyć do planu bezpieczeństwa systemu przez odniesienie się do nich. Na rys. 8-1 przedstawiono możliwe rozbicie dużego GSS na potrzeby planowania bezpieczeństwa.

Proces jednoznacznego przypisywania zasobów informacyjnych[67] do systemu informacyjnego określa granicę bezpieczeństwa dla tego systemu. Organizacje mają dużą elastyczność w określaniu, co stanowi system informacyjny (tj. MA lub GSS). Jeżeli

---

66 Pomocnicze wytyczne w zakresie kategoryzacji systemu, zob. NSC 800-60.

67 Na zasoby informacyjne składają się informacje i powiązane zasoby, takie jak personel, sprzęt, fundusze czy technologia informatyczna.

zbiór zasobów informacyjnych zostanie zidentyfikowany jako system informacyjny, zasoby powinny zasadniczo podlegać tej samej bezpośredniej kontroli zarządczej (*ang. direct management control*).

Bezpośrednia kontrola zarządcza[68] niekoniecznie wyklucza interwencje w te zasoby. System informacyjny może również zawierać wiele podsystemów. Podsystem jest głównym podziałem lub komponentem systemu informacyjnego składającym się z informacji, technologii informatycznej (IT) i personelu wykonującego jedną lub więcej określonych funkcji.

8.4.2. ZABEZPIECZENIA

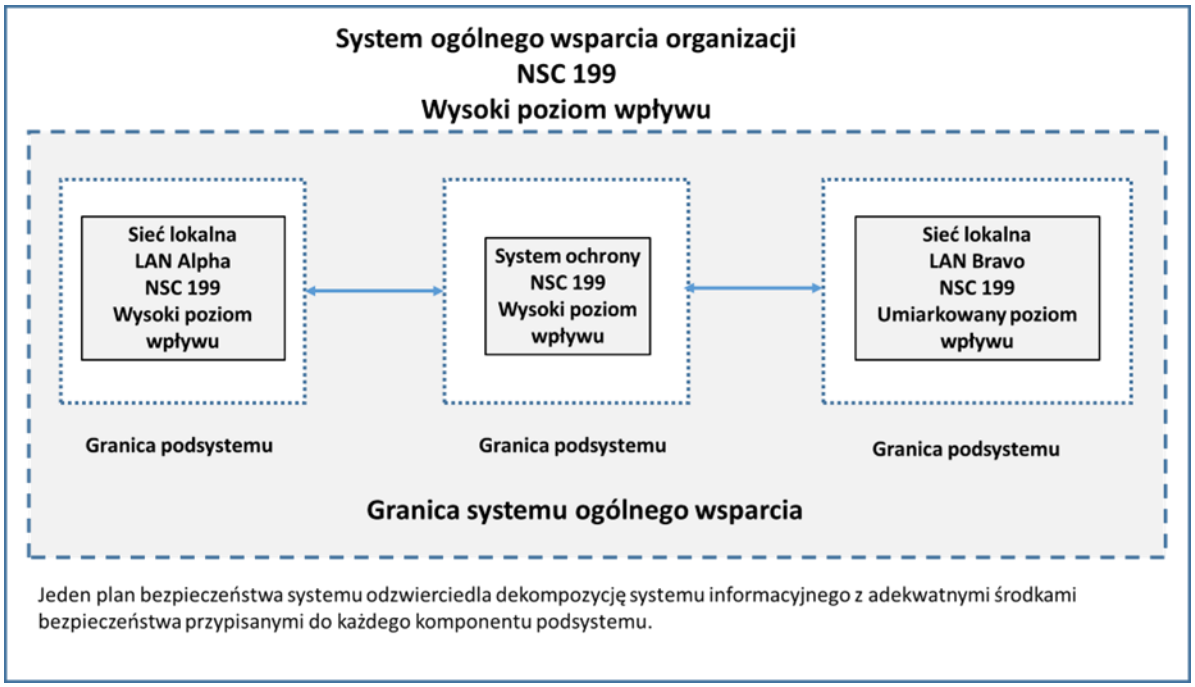
NSC 200 ustanawia dwadzieścia minimalnych kategorii bezpieczeństwa dla informacji i systemów informacyjnych. Wymagania te stanowią szeroko zakrojony, zrównoważony program bezpieczeństwa informacji, który dotyczy zarządzania oraz działań operacyjnych i technicznych w zakresie ochrony poufności, integralności i dostępności informacji i systemów informacyjnych. Organizacja powinna spełniać minimalne wymagania bezpieczeństwa określone w tym standardzie, stosując zabezpieczenia wybrane zgodnie z NSC 800-53 i wyznaczonymi poziomami wpływu na systemy informacyjne. Organizacja ma swobodę w dostosowywaniu zabezpieczeń bazowych zgodnie z postanowieniami standardu. Działania dostosowawcze obejmują: (1) procedury ustalania zakresu działania systemu, (2) specyfikację zabezpieczeń kompensacyjnych oraz (3) specyfikację zdefiniowanych przez organizację parametrów zabezpieczeń, tam, gdzie jest to dozwolone. Wszystkie działania dostosowawcze należy udokumentować w planie bezpieczeństwa systemu.

8.4.3. PROCEDURY USTALANIA ZAKRESU DZIAŁANIA SYSTEMU

Podsystemy zazwyczaj podlegają temu samemu organowi zarządzającemu i są objęte

[68] Bezpośrednia kontrola zarządcza zwykle obejmuje uprawnienia budżetowe, programowe lub operacyjne oraz związaną z tym odpowiedzialność. W przypadku nowych systemów informacyjnych kontrolę zarządczą można interpretować jako posiadanie władzy budżetowej / programowej i odpowiedzialności za rozwój i wdrażanie systemów informacyjnych. W przypadku systemów informacyjnych znajdujących się obecnie w eksploatacji, kontrolę zarządczą można interpretować jako posiadanie uprawnień budżetowych / operacyjnych do codziennych operacji i utrzymania systemów informacyjnych.

jednym planem bezpieczeństwa systemu. Rysunek 8-1 przedstawia przykład systemu ogólnego wsparcia z trzema podsystemami. Procedury ustalania zakresu działania systemu (*ang. scoping guidance*) zapewniają organizacji wsparcie w zakresie stosowania i wdrażania podstawowych zabezpieczeń określonych w NSC 800-53. Opisane poniżej uwagi mogą potencjalnie wpłynąć na sposób, w jaki organizacja zastosuje zabezpieczenia bazowe. Plany bezpieczeństwa systemu powinny jasno określać, które zabezpieczenia wynikają z wytycznych dotyczących ustalania zakresu działania systemu oraz zawierać opis rodzaju podjętych przedsięwzięć. Zastosowanie procedur ustalania zakresu działania systemu musi zostać sprawdzone i zatwierdzone przez osobę autoryzującą dla danego systemu informacyjnego.



Rysunek 8-1. Dekompozycja dużych i złożonych systemów informacyjnych (przykład).

8.4.4. ZABEZPIECZENIA KOMPENSACYJNE

Zabezpieczenia kompensacyjne (*ang. compensating controls*) to zabezpieczenia zarządcze, operacyjne lub techniczne, stosowane przez organizację zamiast zalecanych zabezpieczeń bazowych dla niskich, umiarkowanych lub wysokich poziomów wpływu zakłócenia opisanych w NSC 800-53, które zapewniają równoważną lub porównywalną ochronę systemu informacyjnego, jak zabezpieczenia bazowe.

Zabezpieczenia kompensacyjne dla systemu informacyjnego mogą być stosowane przez organizację tylko pod następującymi warunkami: (1) organizacja wybiera zabezpieczenia kompensacyjne z katalogu zabezpieczeń znajdujących się w standardzie NSC 800-53; (2) organizacja przedstawia kompletne i przekonujące uzasadnienie, w jaki sposób zabezpieczenia kompensacyjne zapewniają równoważne bezpieczeństwo lub poziom ochrony systemu informacyjnego; oraz (3) organizacja ocenia i formalnie akceptuje ryzyko związane z zastosowaniem zabezpieczeń kompensacyjnych w systemie informacyjnym. Zastosowanie zabezpieczeń kompensacyjnych musi zostać przejrzane, udokumentowane w planie bezpieczeństwa systemu i zatwierdzone przez osobę autoryzującą.

8.4.5. ZABEZPIECZENIA OGÓLNE SYSTEMU

Ogólne spojrzenie organizacji na bezpieczeństwa informacji ułatwia identyfikację zabezpieczeń ogólnych systemu (*ang. common security controls*)[69], które można zastosować do jednego lub więcej systemów informacyjnych organizacji. Zabezpieczenia te mogą mieć zastosowanie do: (1) wszystkich systemów informacyjnych organizacji; (2) grupy systemów informacyjnych w określonej lokalizacji (czasami w związku z terminami certyfikacji/akredytacji lokalizacji); lub (3) wspólnych systemów informacyjnych, podsystemów lub aplikacji (tj. wspólny sprzęt komputerowy, oprogramowanie i/lub oprogramowanie sprzętowe) wdrożone w wielu lokalizacjach operacyjnych (czasami związane z terminami certyfikacji/akredytacji). Zabezpieczenia ogólne systemu, zwykle identyfikowane podczas procesu obejmującego całą organizację, z udziałem CIO, SAISO, AO, właścicieli systemów informacyjnych i ISSO (oraz przez kierowników programów rozwojowych w przypadku zabezpieczeń wspólnych dla wspólnego sprzętu, aplikacji i/lub oprogramowana układowego), mają następujące właściwości:

[69] Definicja – patrz: NSC 7298.

- opracowanie, wdrożenie i ocenę zabezpieczeń ogólnych systemu można przypisać do upoważnionego personelu organizacji lub komórek organizacyjnych (innych niż właściciele systemów informacyjnych, których systemy będą wdrażać lub wykorzystywać te wspólne środki bezpieczeństwa);
- wyniki oceny zabezpieczeń wspólnych można wykorzystać do wsparcia procesów certyfikacji bezpieczeństwa i akredytacji systemów informacyjnych organizacji, w których zastosowano te zabezpieczenia.

W celu zwiększenia skuteczności opracowywania planów bezpieczeństwa systemu należy udokumentować zabezpieczenia wspólne, a następnie wprowadzić je do każdego planu bezpieczeństwa systemu informacyjnego w obrębie organizacji. Skuteczne maksymalizowanie zastosowania zabezpieczeń wspólnych w procesie planowania bezpieczeństwa systemu zależy od następujących czynników:

- organizacja opracowała, udokumentowała i przekazała szczegółowe wytyczne dotyczące identyfikacji zabezpieczeń wspólnych;
- organizacja przypisała odpowiedzialność za koordynację identyfikacji i przeglądu zabezpieczeń wspólnych oraz uzyskanie konsensusu w sprawie tych zabezpieczeń osobie zarządzającej, np. CIO lub SAISO, której obowiązki dotyczą programu bezpieczeństwa.
- właściciele systemów zostali poinformowani o procesie planowania bezpieczeństwa systemu, w tym o stosowaniu zabezpieczeń wspólnych;
- w ramach tego procesu skonsultowano się z ekspertami organizacji w zidentyfikowanych wspólnych obszarach zabezpieczeń.

Chociaż koncepcja podziału zabezpieczeń na zabezpieczenia wspólne i zabezpieczenia specyficzne dla systemu jest prosta i intuicyjna, zastosowanie tej zasady w organizacji wymaga planowania, koordynacji i wytrwałości. Jeżeli organizacja dopiero zaczyna wdrażać to podejście lub tylko częściowo wdrożyła to podejście, uzyskanie maksymalnych korzyści z podziału zabezpieczeń i związanego z nim ponownego wykorzystania dowodów oceny może zająć trochę czasu. Ze względu na potencjalną zależność od zabezpieczeń wspólnych w wielu systemach informacyjnych organizacji,

nieprawidłowe zastosowanie takich zabezpieczeń wspólnych może spowodować znaczny wzrost ryzyka na poziomie organizacji – pojawia się ryzyko dla każdego systemu zależnego od tych zabezpieczeń.

8.5. DOBÓR ZABEZPIECZEŃ

Organizacja powinna spełniać minimalne wymagania bezpieczeństwa określone w NSC 199, wybierając odpowiednie środki bezpieczeństwa i zapewnienia wiarygodności opisane w dokumencie NSC 800-53. Proces wyboru odpowiednich środków bezpieczeństwa i wiarygodności w zakresie zapewnienia bezpieczeństwa dla systemu informacyjnego organizacji w celu osiągnięcia *odpowiedniego bezpieczeństwa*[70] jest działaniem wieloaspektowym, opartym na szacowaniu ryzyka, w który w ramach organizacji zaangażowani są kierownictwo i personel operacyjny. Pierwszym krokiem w procesie zarządzania ryzykiem jest kategoryzacja bezpieczeństwa informacji i systemów informacyjnych zgodnie z wymaganiami podanymi w NSC 199[71]. Po przeprowadzeniu procesu kategoryzacji bezpieczeństwa, organizacja musi dokonać wyboru odpowiedniego zestawu zabezpieczeń dla swoich systemów informacyjnych, który spełni minimalne wymagania bezpieczeństwa określone w NSC 200. Wybrany zestaw zabezpieczeń musi być jednym z trzech zestawów zabezpieczeń bazowych wymienionych w NSC 800-53 (zob. tabela 8-2) związanych z poziomami wpływu na systemy informacyjne organizacji wyznaczonymi podczas procesu kategoryzacji bezpieczeństwa.

- W przypadku systemów informacyjnych o *niskim wpływie*, organizacje powinny co najmniej stosować odpowiednio dostosowane zabezpieczenia bazowe zdefiniowane w standardzie NSC 800-53B, jako *niski poziom wpływu* na atrybuty bezpieczeństwa informacji. Organizacje powinny mieć pewność, że minimalne

---

70 Odpowiednie bezpieczeństwo - bezpieczeństwo współmierne do ryzyka i skali szkód wynikających z utraty, niewłaściwego użycia lub nieautoryzowanego dostępu do informacji lub ich modyfikacji.

71 Kategoryzacja bezpieczeństwa musi zostać zrealizowana jako działanie na poziomie organizacji, w którym udział biorą osoby z wyższego kierownictwa organizacji, w tym m.in. CIO, SAISO, osoby autoryzujące (nazywane też organami akredytującymi), właściciele systemów informacyjnych i właściciele informacji. W publikacji NSC 800-60 przedstawiono wytyczne w zakresie wdrażania NSC 199.

wymagania zapewnione przez zastosowanie zabezpieczeń poziomu niskiego, są wystarczające.

- W przypadku systemów informacyjnych o *umiarkowanym wpływie*, organizacje powinny co najmniej stosować odpowiednio dostosowane zabezpieczenia bazowe zdefiniowane w standardzie NSC 800-53B jako *umiarkowany poziom wpływu* na atrybuty bezpieczeństwa informacji. Organizacje powinny mieć pewność, że minimalne wymagania zapewnione przez zastosowanie zabezpieczeń poziomu umiarkowanego, są wystarczające.
- W przypadku systemów informacyjnych o *wysokim wpływie*, organizacje powinny co najmniej stosować odpowiednio dostosowane zabezpieczenia bazowe) zdefiniowane w standardzie NSC 800-53B jako *wysoki poziom wpływu* na atrybuty bezpieczeństwa informacji. Organizacje powinny mieć pewność, że minimalne wymagania zapewnione przez zastosowanie zabezpieczeń poziomu wysokiego, są wystarczające.

Tabela 8-2. Kategoryzacja poziomów wpływu na atrybuty bezpieczeństwa informacji wg NSC 199.

ATRYBUT BEZPIECZEŃSTWA	POTENCJALNY WPŁYW		
	NISKI	**UMIARKOWANY**	**WYSOKI**
POUFNOŚĆ Zapewnienie stosowania zatwierdzonych ograniczeń w zakresie ujawniania i dostępu do informacji, w tym środków ochrony prywatności i informacji osobistych.	Można oczekiwać **ograniczonego** negatywnego wpływu nieuprawnionego ujawnienia informacji na działalność organizacji, jej zasoby lub osoby fizyczne.	Można oczekiwać **poważnego** negatywnego wpływu nieuprawnionego ujawnienia informacji na działalność organizacji, jej zasoby lub osoby fizyczne.	Można oczekiwać **drastycznie lub katastrofalnie** negatywnego wpływu nieuprawnionego ujawnienia informacji na działalność organizacji, jej zasoby lub osoby fizyczne.
INTEGRALNOŚĆ Ochrona przed niewłaściwą modyfikacją lub zniszczeniem informacji, w tym zapewnienie niezaprzeczalności	Można oczekiwać **ograniczonego** negatywnego wpływu nieuprawnionej modyfikacji lub zniszczenia informacji na działalność	Można oczekiwać **poważnego** negatywnego wpływu nieuprawnionej modyfikacji lub zniszczenia informacji na	Można oczekiwać **drastycznie lub katastrofalnie** negatywnego wpływu nieuprawnionej modyfikacji lub zniszczenia informacji na działalność organizacji, jej

ATRYBUT BEZPIECZEŃSTWA	POTENCJALNY WPŁYW		
	NISKI	**UMIARKOWANY**	**WYSOKI**
i autentyczności informacji.	organizacji, jej zasoby lub osoby fizyczne.	działalność organizacji, jej zasoby lub osoby fizyczne.	zasoby lub osoby fizyczne.
DOSTĘPNOŚĆ Zapewnienie terminowego i niezawodnego dostępu i możliwości wykorzystania informacji.	Można oczekiwać **ograniczonego** negatywnego wpływu zaburzenia dostępu lub możliwości wykorzystania informacji na działalność organizacji, jej zasoby lub osoby fizyczne.	Można oczekiwać **poważnego** negatywnego wpływu zaburzenia dostępu lub możliwości wykorzystania informacji na działalność organizacji, jej zasoby lub osoby fizyczne.	Można oczekiwać **drastycznie lub katastrofalnie** negatywnego wpływu zaburzenia dostępu lub możliwości wykorzystania informacji na działalność organizacji, jej zasoby lub osoby fizyczne.

8.6. TERMINY UKOŃCZENIA I ZATWIERDZENIA

Należy podać datę zakończenia opracowywania planu bezpieczeństwa systemu. Data zakończenia powinna być aktualizowana za każdym razem, gdy plan jest okresowo sprawdzany i aktualizowany. Plan bezpieczeństwa systemu powinien również zawierać datę zatwierdzenia planu przez osobę autoryzującą lub wyznaczony organ zatwierdzający. Dokumentacja zatwierdzenia planu, np. dokument akredytacyjny, powinna znajdować się w aktach lub być dołączona jako część planu.

8.7. BIEŻĄCE UTRZYMANIE PLANU BEZPIECZEŃSTWA SYSTEMU

Po zatwierdzeniu planu bezpieczeństwa systemu informacyjnego ważne jest, aby okresowo oceniać plan, przeglądać wszelkie zmiany stanu systemu, funkcjonalności, projektu itp. oraz upewnić się, że plan nadal odzwierciedla prawidłowe informacje o systemie. Ta dokumentacja i jej dokładność są kluczowe dla działań z zakresu ponownej certyfikacji i akredytacji systemu. Wszystkie plany należy poddawać przeglądowi i w stosowanych przypadkach aktualizacji co najmniej raz w roku. Niektóre elementy do uwzględnienia w przeglądzie to:

- zmiana właściciela systemu informacyjnego,
- zmiana przedstawiciela ds. bezpieczeństwa informacji,
- znacząca zmiana w architekturze systemu,
- zmiana statusu systemu,
- dodania/usunięcia wzajemnych połączeń systemowych,
- zmiana zakresu systemu,
- zmiana osoby autoryzującej.

Celem planowania bezpieczeństwa systemu jest poprawienie ochrony zasobów systemu informacyjnego. Wszystkie systemy organizacyjne mają pewien poziom wrażliwości i wymagają ochrony w ramach dobrej praktyki zarządzania. Ochrona systemu musi być udokumentowana w planie bezpieczeństwa systemu.

W celu odpowiedniego odzwierciedlania przez plany ochrony zasobów, właściwy członek kierownictwa organizacji musi autoryzować system do przetwarzania informacji lub działania. To upoważnienie zapewnia istotne zabezpieczenie jakości. Autoryzując przetwarzanie w systemie, osoba autoryzująca akceptuje związane z tym ryzyko.

Autoryzacja powinna opierać się na ocenie zabezpieczeń zarządczych, operacyjnych i technicznych. Ponieważ plan bezpieczeństwa systemu ustanawia i dokumentuje zabezpieczenia, powinien stanowić podstawę autoryzacji uzupełnioną raportem z oceny i POA&M. Ponadto niezbędny jest okresowy przegląd zabezpieczeń na potrzeby przyszłych autoryzacji. Ponowna autoryzacja powinna nastąpić przed znaczącą zmianą w przetwarzaniu, ale nie rzadziej niż co trzy lata.

REFERENCJE:

Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

Federal Information Processing Standard 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

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

National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

National Institute of Standards and Technology Special Publication 800-53, *Revision 1*, *Recommended Security Controls for Federal Information System*, February 2006.

National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.

National Institute of Standards and Technology Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle*, Rev. 1 June 2004.

ROZDZIAŁ 9

9. PLANOWANIE AWARYJNE W ZAKRESIE IT

Planowanie awaryjne w zakresie IT to modułowy element szerszego procesu planowania awaryjnego (*ang. contingency planning - CP*) i planu kontynuacji operacji (*ang. continuity of operations planning - COOP*) obejmującego IT, procesy biznesowe, zarządzanie ryzykiem, zarządzanie finansowe, komunikację kryzysową, bezpieczeństwo personelu i mienia oraz ciągłość zarządzania. Każdy z tych elementów funkcjonuje samodzielnie, ale razem tworzą one skoordynowaną synergię, która skutecznie i wydajnie chroni całą organizację[72].

Planowanie awaryjne dla systemów informacyjnych to proces wymagany w przypadku tworzenia systemów ogólnego wsparcia (*ang. General Support System - GSS*) i aplikacji głównych (*ang. Major Application - MA*) z odpowiednimi metodami wykonywania kopii zapasowych i procedurami odzyskiwania i odtwarzania systemu z uwzględnieniem ryzyka IT[73]. Ryzyko dla systemów informacyjnych może mieć charakter naturalny, technologiczny lub ludzki. Na planowanie awaryjne składa się proces odzyskiwania i dokumentacja procedur odzyskiwania. Publikacja NSC 800-34 szczegółowo przedstawia składającą się z siedmiu kroków metodologię opracowywania procesu i planu awaryjnego w zakresie IT. Pierwszych sześć z siedmiu tych kroków dotyczy planowania, wdrażania i testowania strategii awaryjnej, natomiast przedmiotem ostatniego kroku są dokumentowanie planu, ustanowienie procedur oraz organizacja personelu wdrażającego strategię. NSC 800-34 zawiera również aspekty techniczne dotyczące opracowywania strategii odzyskiwania.

---

[72] Wszystkie organizacje powinny posiadać plany awaryjne w zakresie IT dotyczące ich certyfikowanych i akredytowanych systemów, a także mają obowiązek posiadania organizacyjnego planu kontynuacji operacji dotyczącego ich kluczowych funkcji.

[73] Dodatkowe wytyczne w zakresie ustalania klasyfikacji systemu, zob. NSC 199, NSC 800-60, a także Rozdział 8 „Planowanie bezpieczeństwa" niniejszego podręcznika.

Na rysunku 9-1 przedstawiono działania z zakresu planowania awaryjnego realizowane w każdym z tych siedmiu kroków, które należy uwzględnić w każdej z faz cyklu życia systemu (*ang. System Development Life Cycle - SDLC*)[74].

Zdolność do odzyskania i odtworzenia danych powinna być integralną częścią koncepcji projektu systemu informacyjnego w fazie inicjacji. Strategie odzyskiwania powinny zostać wbudowane w architekturę GSS lub MA podczas fazy opracowywania. Procesy awaryjne powinny być testowane i utrzymywane podczas fazy wdrożenia, natomiast plany awaryjne powinny być realizowane i utrzymywane podczas fazy eksploatacji/utrzymania. Po osiągnięciu przez system informacyjny fazy wycofania, dotychczas eksploatowany system powinien pozostać nienaruszony i sprawny, jako wariant awaryjny, co najmniej do czasu, aż nowy system zostanie wystarczająco przetestowany. W pewnym momencie dotychczasowy system może już dłużej nie obsługiwać potrzeb organizacji, a wtedy może nastąpić przejście z dotychczasowej strategii odzyskiwania do nowej, stworzonej podczas fazy opracowywania nowego systemu.

Rysunek 9-1. Siedem kroków procesu planowania awaryjnego w zakresie IT

[74] Zobacz Rozdział 3 „Cykl życia systemu" niniejszego podręcznika. Dla zainteresowanych - dodatkowe wytyczne w zakresie cyklu życia systemu, zob. NIST SP 800-64.

9.1. KROK 1: OPRACOWANIE DEKLARACJI POLITYKI PLANOWANIA AWARYJNEGO

Pierwszym krokiem podczas opracowywania planu awaryjnego w zakresie IT jest ustanowienie polityki planowania awaryjnego, która będzie obowiązywała w ramach organizacji. Może ona istnieć na poziomie komórki, organizacji i/lub programu organizacji. Dokument powinien definiować ogólne cele planowania awaryjnego oraz identyfikować kierownictwo, role i obowiązki, wymagania dotyczące zasobów, harmonogramy testów, szkolenia i ćwiczeń, a także zawierać grafiki konserwacji i minimalne wymagania dotyczące częstotliwości wykonywania kopii zapasowych.

9.2. KROK 2: PRZEPROWADZENIE ANALIZY WPŁYWU NA DZIAŁALNOŚĆ

Analiza wpływu na działalność (*ang. Business Impact Analysis - BIA*) to kluczowy krok ku zrozumieniu komponentów, współzależności i wpływu potencjalnych przestojów w systemach informacyjnych. Strategię i procedury planu awaryjnego należy projektować z uwzględnieniem wyników BIA.

Przykład zasobów krytycznych w BIA

Rejestracja dostępności i czasu pracy może wymagać wykorzystania serwera lokalnej sieci komputerowej (ang. Local Area Network - LAN), dostępu do rozległej sieci informatycznej (ang. Wide Area Network - WAN), poczty elektronicznej oraz serwera poczty elektronicznej.

Analiza wpływu na działalność jest wykonywana poprzez identyfikację krytycznych zasobów systemu. Każdy kluczowy zasób jest następnie badany w celu ustalenia jak długo jego funkcjonalność może pozostawać niedostępna w systemie informacyjnym zanim wystąpi nieakceptowalny wpływ.

Przykład wpływu na zasób w BIA

Zakłócenie sieci LAN wykorzystywanej w systemie rejestracji dostępności i czasu pracy przez 8 godzin może spowodować opóźnienie w przetwarzaniu kart czasu pracy.

Wpływ może materializować się z upływem czasu albo można go prześledzić w powiązanych zasobach lub podporządkowanych systemach (np. kaskadowy efekt domina). Podany czas to maksymalny dopuszczalny czas przestoju (*ang. Maximum Allowable Outage - MAO*). W oparciu o potencjalny wpływ, jest to czas przez jaki system

informacyjny może pozostawać bez kluczowego zasobu; jest on wykorzystywany jako priorytet odzyskiwania będący dla organizacji podstawą planowania działań z zakresu odzyskiwania. Czas odzyskiwania (*ang. Recovery Time Objective - RTO*) systemu informacyjnego jest ustalany w oparciu o punkt równowagi między MAO i kosztem odzyskania. Strategie odzyskiwania należy tworzyć tak, aby spełnić wymóg RTO.

Przykład czasu odzyskiwania w BIA

Serwer LAN musi zostać odzyskany w ciągu 8 godzin, aby uniknąć opóźnienia w przetwarzaniu kart czasu pracy.

Strategia musi również uwzględniać odzyskiwanie krytycznych komponentów systemu informacyjnego w ramach danego priorytetu, zgodnie z ich RTO.

9.3. KROK 3: IDENTYFIKACJA ZABEZPIECZEŃ PREWENCYJNYCH

W niektórych przypadkach wdrożenie zabezpieczeń prewencyjnych może złagodzić skutki przestoju określone w BIA. Zabezpieczenia prewencyjne to środki, które wykrywają, uniemożliwiają i/lub ograniczają wpływ zakłócenia na system. Tam, gdzie jest to opłacalne, zapobieganie takiemu wpływowi jest bardziej pożądane niż wdrażanie strategii odzyskiwania, które stwarza ryzyko utraty danych i wpływu na organizację. Środki zapobiegawcze są specyficzne dla poszczególnych komponentów i środowiska, w których te komponenty działają. Wśród powszechnie stosowanych zabezpieczeń są:

- zasilanie bezprzerwowe (*ang. Uninterruptible Power Supply - UPS*);
- systemy przeciwpożarowe
- agregaty prądotwórcze;
- systemy klimatyzacji o nadwyżce wydajności pozwalającej zniwelować wpływ awarii niektórych elementów;
- odporne na ciepło i wodoodporne pojemniki na nośniki kopii zapasowych;
- zapisy nieelektroniczne;
- częste, planowe wykonywanie kopii zapasowych.

9.4. KROK 4: OPRACOWANIE STRATEGII ODZYSKIWANIA

W przypadku wystąpienia zakłócenia mimo wdrożenia środków zapobiegawczych, konieczna jest strategia odzyskiwania umożliwiająca odzyskanie i przywrócenie danych i operacji systemu w przewidzianych RTO. Strategia odzyskiwania jest projektowana jako połączenie metod, które razem uwzględniają pełne spektrum ryzyka dla systemów informacyjnych. W fazie rozwoju można ocenić kilka możliwości, przy czym, w oparciu o potencjalny wpływ, wybrać i zintegrować z architekturą systemu informacyjnego i procedurami operacyjnymi należy najbardziej opłacalną z nich.

Wskazówka dotycząca strategii odzyskiwania

Wybrana strategia musi być również skoordynowana z planami awaryjnymi w zakresie IT powstałymi dla współzależnych systemów oraz planami ciągłości działalności powstałymi dla procesów biznesowych.

Dane systemowe powinny być regularnie przenoszone do kopii zapasowych. Wszystkie plany awaryjne w zakresie IT powinny zatem zawierać metodę i częstotliwość tworzenia kopii zapasowych. Częstotliwość tworzenia kopii zapasowych (dzienna lub tygodniowa, przyrostowa lub pełna) należy wybrać w oparciu o krytyczność systemu i to, kiedy wprowadzane są nowe informacje. Wybrana metoda tworzenia kopii zapasowych powinna opierać się na wymaganiach dotyczących dostępności i integralności systemu i danych (zdefiniowanych w BIA). W zależności od krytyczności systemu, może wystąpić potrzeba przechowywania zapasowych kopii danych poza siedzibą organizacji i dokonywania częstej rotacji nośników.

Wskazówka dotycząca strategii odzyskiwania

Przechowywane dane powinny być rutynowo testowane, aby potwierdzić ich integralność.

Poważne zakłócenia operacji systemu mogą wymagać podjęcia działań przywracających w alternatywnym miejscu przetwarzania. Wybór rodzaju miejsca alternatywnego musi opierać się na wymaganiach RTO i ograniczeniach budżetowych. Sprzęt przeznaczony do przywrócenia i/lub wymiany systemu informacyjnego należy zapewnić w ramach strategii odzyskiwania. Ustalając sposób zapewnienia niezbędnego sprzętu należy wziąć pod uwagę czynniki związane z kosztem, czasem dostawy

i kompatybilnością. Organizacje muszą również zaplanować takie alternatywne miejsce przetwarzania, które zapewnia co najmniej miejsce do pracy dla całego personelu realizującego plan awaryjny oraz sprzęt i odpowiednią infrastrukturę informatyczną niezbędną do realizacji planu awaryjnego w zakresie IT i działań w zakresie odzyskiwania systemu.

Poziom gotowości operacyjnej alternatywnego miejsca przetwarzania to ważna cecha, którą należy ustalić podczas opracowywania strategii odzyskiwania. Przegląd powszechnych rodzajów alternatywnych miejsc przetwarzania przedstawiono w dokumencie NSC 800-34.

Strategia odzyskiwania wymaga, aby personel wdrożył procedury i przetestował operacyjność. Do uruchomienia planu i kierowania całością operacji odzyskiwania wybierany jest zazwyczaj członek wyższego kierownictwa organizacji. Spośród personelu ustanawiane są odpowiednie zespoły (składające się z co najmniej dwóch osób, tak aby zapewnić możliwość realizacji procedur albo przez osobę główną, albo zmiennika) odpowiedzialne za realizację poszczególnych elementów planu.

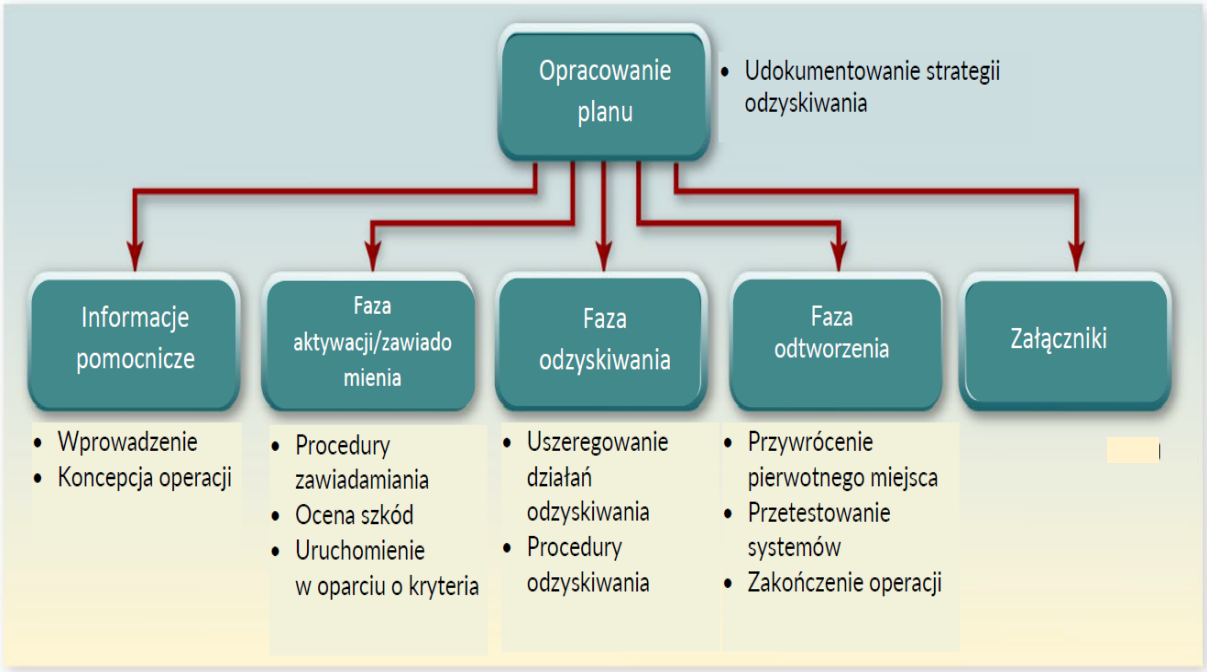
Członkowie zespołów powinni być dobierani w oparciu o ich normalne obowiązki, znajomość systemu i dostępność „na wezwanie” w razie wystąpienia konieczności odzyskania systemu. Należy określić porządek zastępstw, aby zapewnić obecność osoby mogącej przejąć kierowniczą rolę w przypadku, gdy osoba kierująca planem nie jest w stanie zareagować.

Na koniec, po dokonaniu wyboru każdego elementu strategii odzyskiwania, należy rozważyć kwestię kosztów. Strategia odzyskiwania musi spełniać wymagania dotyczące krytyczności, dostępności i RTO, a jednocześnie mieścić się w budżecie. W ocenie należy uwzględnić również mniej oczywiste koszty, takie jak przesyłki, programy uświadamiania, testy i ćwiczenia, przejazdy, godziny pracy oraz zakontraktowane usługi.

9.5. KROK 5: OPRACOWANIE PLANU AWARYJNEGO W ZAKRESIE IT

Procedury realizacji strategii odzyskiwania zostają nakreślone w planie awaryjnym w zakresie IT. Plan musi zostać napisany w formacie, który zapewni użytkownikom

(kierownictwu i członkom zespołu odzyskiwania) kontekst, w jakim należy wdrożyć plan, a także bezpośrednie procedury, jakie należy wykonać (w podziale na role). Plany awaryjne w zakresie IT są konstruowane z pięciu komponentów przedstawionych na rysunku 9-2.



Rysunek 9-2. Struktura planu awaryjnego

Procedury są dokumentowane w fazach zawiadomienia/uruchomienia, odzyskiwania i odtworzenia. Informacje pomocnicze i załączniki dostarczają uzupełniających informacji koniecznych do zrozumienia kontekstu, w którym plan ma być realizowany oraz dodatkowych informacji, które mogą być konieczne do wykonania procedur (np. dane kontaktowe w sytuacjach awaryjnych oraz BIA).

9.6. KROK 6: TESTOWANIE PLANU, SZKOLENIA I ĆWICZENIA

Personel wybrany do wykonywania planu awaryjnego w zakresie IT musi zostać przeszkolony w realizacji procedur, plan musi zostać przećwiczony, a strategia systemu przetestowana.

Planowanie testów powinno obejmować:

- odzyskiwanie systemu z zapasowych nośników na alternatywnej platformie,
- koordynację między zespołami ds. odzyskiwania,

- łączność wewnętrzną i zewnętrzną,
- działanie systemu z wykorzystaniem alternatywnego sprzętu,
- przywrócenie normalnego działania,
- procedury zawiadamiania.

Szkolenie personelu powinno obejmować:

- cel programu,
- koordynację i komunikację między zespołami,
- procedury raportowania,
- wymagania bezpieczeństwa,
- procesy właściwe dla danego zespołu,
- obowiązki indywidualne.

Ćwiczenia w zakresie testowania planu powinny być projektowane indywidualnie, a następnie zbiorczo badać różne komponenty całego planu. Ćwiczenia można prowadzić w warunkach sali lekcyjnej i polegać na omówieniu konkretnych komponentów planu i/lub zagadnień dotyczących wpływu, albo też mieć postać ćwiczeń funkcjonalnych symulujących odzyskiwanie przy użyciu faktycznego sprzętu i danych zastępczych oraz alternatywnych miejsc.

9.7. KROK 7: UTRZYMANIE PLANU

Plan awaryjny w zakresie IT musi być zawsze utrzymywany w stanie gotowości do użycia niezwłocznie po zawiadomieniu. Plan musi być poddawany okresowym przeglądom pod kątem aktualności informacji na temat kluczowego personelu i kluczowych dostawców, komponentów i współzależności systemu, strategii odzyskiwania, istotnych zapisów oraz wymagań operacyjnych. Chociaż niektóre z nich mogą być oczywiste (np. rotacja personelu czy zmiany wśród dostawców), inne będą wymagały analizy. BIA powinna być poddawana okresowym przeglądom i aktualizowana o nowe informacje w celu zidentyfikowania nowych wymagań i priorytetów awaryjnych. Zmiany wprowadzone do planu są odnotowywane w wykazie

zmian, opatrywane datą i podpisywane lub parafowane przez osobę, która je wprowadziła. Zmieniony plan lub odpowiednie jego rozdziały są rozpowszechniane wśród osób, których obowiązki obejmują realizację planu. Z powodu wpływu, jaki zmiany planu mogą mieć na współzależne procesy biznesowe lub systemy informacyjne, zmiany te należy w sposób wyraźny komunikować i odnotowywać na początku dokumentu.

REFERENCJE:

Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

National Institute of Standards and Technology Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.

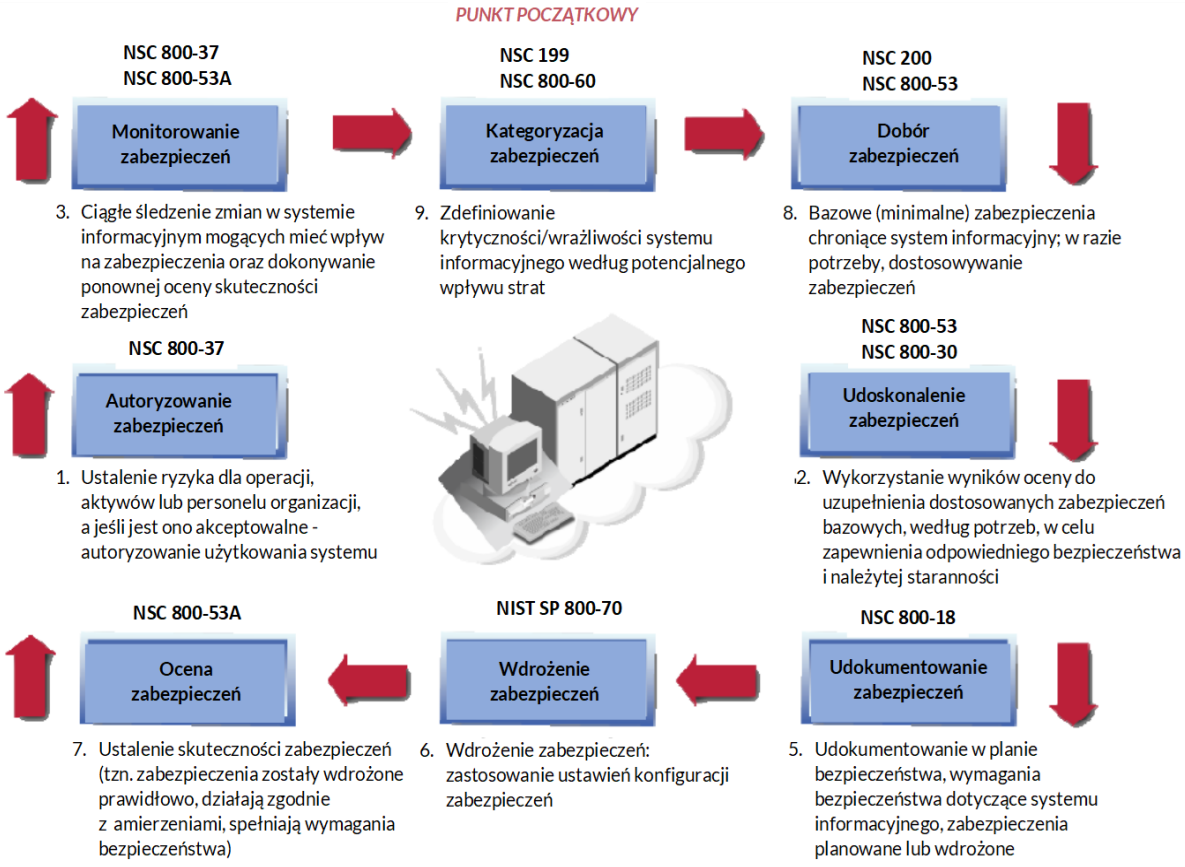
National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.

National Institute of Standards and Technology Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle*, Rev. 1 June 2004.

ROZDZIAŁ 10

10. ZARZĄDZANIE RYZYKIEM

Skuteczny proces zarządzania ryzykiem jest ważnym komponentem udanego programu bezpieczeństwa informacji. Głównym celem procesu zarządzania ryzykiem w organizacji jest ochrona organizacji i jej zdolności do realizacji misji, a nie tylko jej zasobów informacyjnych. Dlatego procesu zarządzania ryzykiem nie należy traktować głównie jako funkcji technicznej realizowanej przez specjalistów ds. bezpieczeństwa informacji, którzy użytkują system informacyjny i nim zarządzają, ale kluczową funkcję zarządczą organizacji, która jest ściśle powiązana z cyklem życia systemu (SDLC)[75], jak pokazano na rysunku 10-1.



Rysunek 10-1. Zarządzanie ryzykiem w cyklu życia systemu

[75] Dodatkowe informacje na temat cyklu SDLC można znaleźć w publikacji NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle* oraz w rozdziale 3 tego przewodnika, *Cykl życia systemu*.

Ponieważ ryzyka nie można wyeliminować całkowicie, proces zarządzania ryzykiem pozwala menadżerom programu bezpieczeństwa informacji zrównoważyć operacyjne i ekonomiczne koszty środków bezpieczeństwa i osiągnąć korzyści w obszarze zdolności do realizacji misji. Stosując praktyki i procedury stworzone w celu wspierania świadomych decyzji, organizacje pomagają chronić swoje systemy informacyjne i dane, które wspierają ich własne misje.

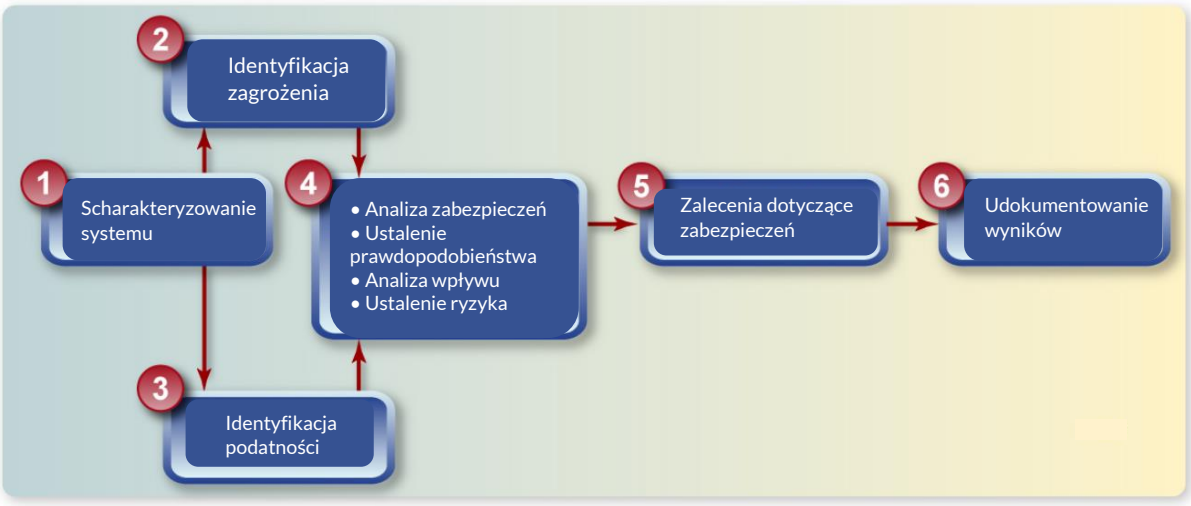
Zarządzanie ryzykiem to połączenie trzech procesów mających swoje korzenie w przepisach, regulacjach i wytycznych. Te trzy procesy to: szacowanie ryzyka, mitygacja ryzyka oraz ocena i ewaluacja. Kiedy zostaną zastosowane odpowiednio oraz z należytą starannością, procesy te pozwalają na „zapewnienie środków bezpieczeństwa informacji współmiernych do ryzyka i skali szkód wynikających z nieautoryzowanego dostępu, użytkowania, ujawnienia, zakłócenia, modyfikacji lub zniszczenia informacji i systemów informacyjnych" zbieranych/użytkowanych przez organizacje, a także „zapewnienie, że procesy zarządzania bezpieczeństwem informacji zostały zintegrowane z realizowanymi przez organizację procesami planowania strategicznego i operacyjnego".

10.1. SZACOWANIE RYZYKA

Do zrozumienia procesu szacowania ryzyka niezbędne jest zdefiniowanie pojęcia ryzyka. Publikacja NSC 800-30 definiuje ryzyko jako „funkcję prawdopodobieństwa wykorzystania potencjalnej podatności przez dane źródło zagrożenia i wpływu tego negatywnego zdarzenia na organizację". Innymi słowy, ryzyko jest obecne tam, gdzie zagrożenie spotyka się z podatnością. Przy tak zdefiniowanym ryzyku, celem procesu szacowania ryzyka jest identyfikacja i oszacowanie ryzyka dla danego środowiska. Szczegółowość oszacowania ryzyka może być bardzo różna i zależy od krytyczności i wrażliwości systemu w odniesieniu do jego poufności, integralności i dostępności, co zostało szczegółowo opisane w publikacji NSC 199.

Osiągnięcie celu szacowania ryzyka wymaga realizacji składającego się z dziewięciu kroków procesu, który opisano w publikacji NSC 800-30 i podsumowano w tym rozdziale. Dla pewnego uproszczenia procesu, dziewięć kroków opisanych w NSC 800-30 zredukowano do sześciu, łącząc Kroki 4, 5 i 6 w jeden - analizę ryzyka

(patrz: rysunki 10-2 i 10-3). Na rysunku 10-2 poniżej przedstawiono ogólny zarys procesu szacowania ryzyka.



Rysunek 10-2. Proces szacowania ryzyka

Prawdopodobieństwo, że dane zagrożenie skutecznie wykorzysta daną podatność jest szacowane poprzez ocenę motywacji źródła zagrożenia, okazji i sposobów wykorzystania tej podatności. Wpływ udanego wykorzystania podatności szacowany jest poprzez analizę skutku, jaki to wykorzystanie może mieć na poufność, integralność i dostępność systemu i przetwarzanych w nim danych. Krytyczność i wrażliwość systemu pod względem jego poufności, integralności i dostępności są ustalane przez zastosowanie koncepcji i procesów, które zostały szczegółowo omówione w NSC 199.

Proces szacowania ryzyka powinien być potarzany co jeden rok[76]. Jednakże szacowanie ryzyka powinno być wykonywane, a także zintegrowane z cyklem życia systemów informacyjnych nie dlatego, że jest wymagane przepisami prawa lub regulacjami, ale dlatego, że jest to dobra praktyka, która stanowi wsparcie celów biznesowych i misji organizacji.

[76] Wynika to z rocznego okresu wykonywania audytów, a nie przeprowadzi się audytu z wynikiem pozytywnym, jeśli nie będzie przeprowadzone szacowanie ryzyka.

10.1.1. KROK 1 - CHARAKTERYSTYKA SYSTEMU

Scharakteryzowanie systemu informacyjnego wyznacza zakres działań dotyczących szacowania ryzyka, wyznacza granice upoważnienia operacyjnego (lub akredytacji) i dostarcza informacji (np. dotyczących sprzętu komputerowego, oprogramowania, łączności z siecią oraz odpowiedzialnych działów i personelu wsparcia). Ten krok rozpoczyna się od zidentyfikowania granic, zasobów i informacji systemu informacyjnego.

Podczas charakteryzowania systemu, krytyczność i wrażliwość misji (zidentyfikowane uprzednio wg. NSC 199 w celu ustalenia odpowiedniej kategoryzacji bezpieczeństwa systemu) są opisywane tak, aby stworzyć podstawę dla zakresu szacowania ryzyka. Poziom wysiłku i ziarnistości (tzn. poziom szczegółowości badania systemu informacyjnego) szacowania ryzyka opiera się na kategoryzacji bezpieczeństwa podanej w NSC 199. Na przykład, system, którego wpływ ustalono jako niski może nie wymagać praktycznego testowania i oceny bezpieczeństwa. Do zbierania informacji potrzebnych do pełnego scharakteryzowania systemu można użyć różnych technik, takich jak kwestionariusze, wywiady, przeglądy dokumentacji czy zautomatyzowane narzędzia skanujące. W wariancie minimalnym, charakterystyka systemu opisuje następujące komponenty systemu:

- sprzęt komputerowy (np. komputery IBM typu „mainframe" z systemem operacyjnym z/OS, serwery Dell działające pod Windows 2012);
- oprogramowanie (np. serwery www Oracle, Apache, serwery Microsoft Internet Information Server [IIS]);
- zewnętrzne interfejsy z innymi systemami;
- dane;
- personel.

Oprócz opisów komponentów, charakterystyka systemu opisuje pozostałe czynniki mogące wpływać na bezpieczeństwo systemu, takie jak:

- wymagania funkcjonalne systemu;
- zasady i architektura bezpieczeństwa organizacji;

- topologia sieciowa systemu;
- przepływy informacji w systemie;
- zabezpieczenia zarządcze, operacyjne i techniczne wdrożone lub zaplanowane do wdrożenia w systemie;
- mechanizmy bezpieczeństwa fizycznego i środowiskowego.

Ponieważ ten krok stanowi podstawę dla pozostałych kroków, dokładność uzyskanych w nim wyników jest kluczowa dla uzyskania jak najlepszego obrazu profilu ryzyka ocenianego systemu. Niedokładność na tym etapie będzie przenoszona dalej i doprowadzi do kaskady błędów analitycznych w dalszym toku procesu.

10.1.2. KROK 2 - IDENTYFIKACJA ZAGROŻENIA

Identyfikacja zagrożenia polega na zidentyfikowaniu źródeł zagrożenia mogących wykorzystać słabości systemu. Kulminacją tego kroku powinno być opracowanie „deklaracji zagrożeń", czyli kompleksowej listy potencjalnych źródeł zagrożenia. Deklaracja zagrożeń musi być dostosowana do konkretnej organizacji i jej środowiska przetwarzania (np. zwyczajów obliczeniowych użytkowników końcowych), co wykonuje się poprzez przeprowadzenie oceny zagrożeń na podstawie charakterystyki systemu w celu ustalenia zdolności spowodowania szkód w systemie.

Istnieją powszechne zagrożenia, które zazwyczaj występują niezależnie od tego, jaki system jest poddawany ocenie. Zagrożenia te można sklasyfikować w trzech obszarach: (1) zagrożenia naturalne (np. powodzie, trzęsienia ziemi, wichury, osunięcia ziemi, lawiny, burze z wyładowaniami elektrycznymi), (2) zagrożenia ludzkie (zamierzone i niezamierzone) oraz (3) zagrożenia środowiskowe (np. awaria zasilania). Zasadniczo, informacje o zagrożeniach naturalnych (np. powodziach, trzęsieniach ziemi, burzach) powinny być łatwo dostępne, ponieważ znane zagrożenia zostały już zidentyfikowane przez wiele organizacji sektora państwowego i prywatnego. Coraz bardziej rozpowszechnione są narzędzia do wykrywania włamań, a organizacje publiczne i branżowe ciągle gromadzą dane na temat zdarzeń związanych z bezpieczeństwem, tym samym zwiększając zdolność do realnej oceny zagrożeń. Do źródeł informacji należą m.in.:

- Rządowe Centrum Bezpieczeństwa,
- Zespół Reagowania na Incydenty Komputerowe (*ang. Computer Emergency Response Team -CERT*) dostępny pod adresem CERT Polska),
- środki masowego przekazu, w tym zasoby internetowe.

10.1.3. KROK 3 - IDENTYFIKACJA PODATNOŚCI

Publikacja NSC 800-30 definiuje podatność jako „wadę lub słabość procedur bezpieczeństwa, projektu, wdrożenia lub zabezpieczeń wewnętrznych systemu, którą można wykorzystać (przypadkowo lub w sposób zamierzony) i która skutkuje naruszeniem bezpieczeństwa lub złamaniem zasad bezpieczeństwa". Podatności można identyfikować przy użyciu połączenia szeregu technik i źródeł. Proces identyfikacji podatności można rozpocząć od przeglądu takich źródeł, jak wcześniejsze oszacowania ryzyka, sprawozdania z audytów, listy podatności (np. prowadzona przez NIST baza danych National Vulnerability Database - NVD, wcześniej znana pod nazwą I-CAT, dostępna na stronie nvd.nist.gov) oraz ostrzeżenia dotyczące bezpieczeństwa. Do uzupełnienia źródłowych przeglądów podatności i zidentyfikowania podatności niestwierdzonych wcześniej w innych źródłach można użyć testowania bezpieczeństwa systemu takimi metodami, jak zautomatyzowane narzędzia skanowania podatności; badanie bezpieczeństwa, testowanie i ocenianie (*ang. Security, Test and Evaluation - ST&E*)[77]; czy testowanie penetracyjne.

Dodatkowo, całościowe sprawdzenie systemu można przeprowadzić poprzez opracowanie listy kontrolnej wymagań bezpieczeństwa opartej na wymaganiach określonych podczas fazy konceptualnej, projektowej i wdrożeniowej SDLC. Listę kontrolną można przygotować przy użyciu wskazówek podanych w NSC 800-53A oraz NSC 800-53, aby zapewnić uwzględnienie odpowiednich pytań z obszarów zabezpieczeń zarządczych, operacyjnych i technicznych. Wyniki listy można wykorzystać jako dane wejściowe do oceny zgodności i jej braku, co z kolei prowadzi do zidentyfikowania słabości systemowych, procesowych i proceduralnych stanowiących potencjalne podatności.

[77] Badanie i analiza zabezpieczeń wymaganych do ochrony systemu informacyjnego, zastosowanych w środowisku operacyjnym, w celu określenia stanu bezpieczeństwa tego systemu.

10.1.4. KROK 4 - ANALIZA RYZYKA

Analiza ryzyka to ustalenie (lub oszacowanie) ryzyka dla systemu, co wymaga rozważenia ściśle powiązanych czynników takich, jak zabezpieczenia wdrożone w badanym systemie, prawdopodobieństwo, że zabezpieczenia te okażą się niewystarczające lub nieskuteczne do ochrony systemu oraz wpływ tej okoliczności. Innymi słowy, oszacowanie poziomu ryzyka stwarzanego przez udane wykorzystanie danej podatności jest niemożliwe bez rozważenia skuteczności zabezpieczeń, które zostały lub mają zostać wdrożone w celu ograniczenia lub wyeliminowania możliwości takiego wykorzystania. Dotyczy to również oszacowania motywacji, możliwości i zdolności zagrożenia, które przyczyniają się do prawdopodobieństwa udanego ataku, a także oszacowania wpływu na system i organizację w przypadku udanego wykorzystania podatności. Przedstawione poniżej cztery kroki—analiza zabezpieczeń, ustalenie prawdopodobieństwa, analiza wpływu i ustalenie ryzyka—są w sensie praktycznym wykonywane jednocześnie lub niemal jednocześnie, ponieważ są ze sobą bardzo blisko związane.

10.1.4.1. ANALIZA ZABEZPIECZEŃ

Jak stwierdzono powyżej, analiza zabezpieczeń wdrożonych w celu ochrony systemu może zostać wykonana przy użyciu listy kontrolnej lub kwestionariusza, zgodnie z wymaganiami bezpieczeństwa systemu określonymi w publikacji NSC 800-53. Dane analityczne można dopracować stosując publikację NSC 800-53A, która podaje wytyczne w zakresie testowania zabezpieczeń zaczerpnięte z NSC 800-53. Wyniki służą lepszemu ustaleniu prawdopodobieństwa udanego wykorzystania konkretnej podatności przez dane zagrożenie.

10.1.4.2. USTALENIE PRAWDOPODOBIEŃSTWA

Ustalenie prawdopodobieństwa uwzględnia posiadaną przez źródło zagrożenia motywację i zdolność do wykorzystania podatności, charakter tej podatności, istnienie zabezpieczeń oraz skuteczność zabezpieczeń ograniczających. Oceny prawdopodobieństwa są opisywane w kategoriach jakościowych jako wysokie, umiarkowane i niskie, i służą do opisu prawdopodobieństwa udanego wykorzystania podatności przez dane zagrożenie. Na przykład, jeżeli zagrożenie ma wysoką

motywację i wystarczające zdolności, a zabezpieczenia wdrożone w celu ochrony podatności są nieskuteczne, to powodzenie ataku jest wysoce prawdopodobne. W tym scenariuszu, prawdopodobieństwo zostałoby ocenione jako wysokie. Prawdopodobieństwo umiarkowane i niskie są określane podobnie i odpowiadają niższym stopniom.

10.1.4.3. ANALIZA WPŁYWU

Trzecim czynnikiem używanym do ustalenia poziomu ryzyka dla systemu jest wpływ. Właściwa ogólna analiza wpływu uwzględnia następujące czynniki: wpływ na systemy, dane i misję organizacji. Dodatkowo, powinna one uwzględnić również krytyczność i wrażliwość systemu i jego danych.

W NSC 199 przedstawiono spójny i ukierunkowany proces kategoryzacji krytyczności i wrażliwości systemu w trzech domenach: poufności, integralności i dostępności. Użycie NSC 199 do ustalenia kategorii bezpieczeństwa oraz przeprowadzenie oceny misji organizacji i systemu z wykorzystaniem takich narzędzi, jak raporty o wpływie na misję, raporty z ceny krytyczności aktywów czy analizy wpływu na działalność prowadzi do oceny opisującej szacowany wpływ na system i organizację w przypadku udanego wykorzystania podatności przez zagrożenie. Chociaż wpływ można opisać w kontekście systemów informacyjnych i danych przy zastosowaniu podejścia ilościowego lub jakościowego, to zwykle robi się to w kategoriach jakościowych. Podobnie jak w przypadku ratingów opisujących prawdopodobieństwo, poziom wpływu jest opisywany jako wysoki, umiarkowany lub niski.

Definicje wpływu wysokiego, umiarkowanego i niskiego znajdują się w publikacji NSC 800-30.

10.1.4.4. USTALENIE RYZYKA

Po ustaleniu ratingu prawdopodobieństwa i wpływu w oparciu o odpowiednie analizy, poziom ryzyka dla systemu i organizacji można uzyskać mnożąc te ratingi przez siebie. W tabeli 10-1 pokazano sposób obliczania ogólnego ryzyka w matrycy 3x3 przy użyciu danych wejściowych z kategorii prawdopodobieństwa i wpływu zagrożenia.
W zależności od wymagań systemu i ziarnistości szacowania ryzyka, można też użyć matryc 4x4 i 5x5. W przypadku ostatniej z nich, można użyć bardzo niskiego/bardzo

wysokiego prawdopodobieństwa zagrożenia i bardzo niskiego/bardzo wysokiego wpływu zagrożenia do wygenerowania bardzo niskiego/bardzo wysokiego poziomu ryzyka. Bardzo wysoki poziom ryzyka może wymagać ewentualnego zamknięcia systemu lub wstrzymania wszelkich działań dotyczących integracji i testowania systemu informacyjnego.

Tabela 10-1. Matryca poziomu ryzyka

	**Wpływ**		
Prawdopodobieństwo zagrożenia	**Niski (10)**	**Umiarkowany (50)**	**Wysoki (100)**
Wysokie (1,0)	10 x 1,0 = 10	50 x 1,0 = 50	100 x 1,0 = 100
Umiarkowane (0,5)	10 x 0,5 = 5	50 x 0,5 = 25	100 x 0,5 = 50
Niskie (0,1)	10 x 0,1 = 1	50 x 0,1 = 5	100 x 0,1 = 10
Skala ryzyka: Wysokie (>50 do 100)	Umiarkowane (>10 do 50)		Niskie (1 do 10)

Ponieważ ustalenie ratingów ryzyka dla wpływu i prawdopodobieństwa zagrożenia jest w dużym stopniu subiektywne, dla ułatwienia obliczeń najlepiej jest przypisać każdemu ratingowi wartość liczbową. Przesłanki stojące za tym uzasadnieniem można wyjaśnić w kategoriach prawdopodobieństwa przypisanego do każdego poziomu prawdopodobieństwa zagrożenia i wartości przypisanej każdemu poziomowi wpływu. Na przykład:

- Prawdopodobieństwo przypisany każdemu poziomowi prawdopodobieństwa zagrożenia wynosi 1,0 dla wysokiego, 0,5 dla umiarkowanego i 0,1 dla niskiego.
- Wartość przypisana każdemu poziomowi wpływu wynosi 100 dla wysokiego, 50 dla umiarkowanego i 10 dla niskiego.

W tabeli 10-2 opisano poziomy ryzyka przedstawione w powyższej matrycy. Skala ryzyka - z ocenami ryzyka: wysokie, umiarkowane i niskie - przedstawia stopień ryzyka, na jaki narażony może zostać system informacyjny, obiekt lub procedura w przypadku wykorzystania danej podatności. Opisuje ona również rodzaj działania, jakie wyższe kierownictwo musi podjąć dla każdego poziomu ryzyka.

Tabela 10-2. Skala ryzyka i konieczne działanie zarządcze

Poziom ryzyka	Opis ryzyka i koniecznego działania zarządczego
Wysoki	Jeżeli obserwacja lub ustalenie zostaje ocenione jako wysokie ryzyko, to istnieje uzasadniona potrzeba wdrożenia środków naprawczych. Istniejący system może dalej działać, ale jak najszybciej należy wdrożyć plan działań naprawczych.
Umiarkowany	Jeżeli obserwacja zostaje oceniona jako umiarkowane ryzyko, to potrzebne są działania naprawcze i w rozsądnym terminie należy opracować uwzględniający je plan.
Niski	Jeżeli obserwacja zostaje opisana jako niskie ryzyko, to osoba autoryzująca w systemie musi ustalić, czy potrzebne są działania naprawcze lub zdecydować o akceptacji ryzyka.

10.1.5. KROK 5 - ZALECENIA DOTYCZĄCE ZABEZPIECZEŃ

Celem zaleceń dotyczących zabezpieczeń jest obniżenie poziomu ryzyka dla systemu informacyjnego i jego danych do poziomu, który organizacja uznaje za akceptowalny. Zalecenia stanowią niezbędny materiał wejściowy dla procesu mitygacji ryzyka, podczas którego zalecane zabezpieczenia proceduralne i techniczne są oceniane, szeregowane pod względem priorytetu i wdrażane. Ten krok ma pomóc organizacjom w identyfikacji i wyborze zabezpieczeń odpowiednich dla operacji i misji organizacji, które mogą ograniczyć lub wyeliminować ryzyka zidentyfikowane w poprzednich krokach. Zalecając zabezpieczenia i alternatywne rozwiązania ograniczające lub eliminujące zidentyfikowane ryzyka należy wziąć pod uwagę następujące czynniki:

- skuteczność zalecanych możliwości (np. kompatybilność systemu),
- przepisy i regulacje,
- politykę organizacyjną,
- wpływ na operacje,
- bezpieczeństwo oraz niezawodność.

Dalsze rekomendacje w zakresie opracowywania zaleceń dotyczących zabezpieczeń w organizacji zawarte są w publikacji NSC 800-53.

10.1.6. KROK 6 - DOKUMENTACJA WYNIKÓW

Sprawozdanie z szacowania ryzyka to mechanizm służący do formalnego raportowania wyników wszystkich działań dotyczących szacowania ryzyka. Zamierzoną funkcją tego sprawozdania jest opisanie i udokumentowanie stanu ryzyka systemu podczas gdy działa on w swoim właściwym środowisku (zgodnie z opisem w charakterystyce systemu) oraz udzielenie kierownictwu organizacji wystarczających informacji umożliwiających podjęcie rozsądnych, opartych na ryzyku decyzji, np. w sprawie środków, jakie należy przydzielić do fazy mitygacji ryzyka. Wreszcie, organizacja powinna zapewnić, aby wyniki szacowania ryzyka zawarte w planie i etapach działania systemu (POA&M) i planie bezpieczeństwa systemu.

Jako minimum, sprawozdanie z szacowania ryzyka powinno opisywać:

- zakres szacowania w oparciu o charakterystykę systemu,
- zastosowaną metodologię szacowania ryzyka,
- indywidualne obserwacje poczynione podczas szacowania ryzyka,
- oszacowanie ogólnego stanu ryzyka w systemie.

10.2. MITYGACJA RYZYKA

Drugą fazą procesu zarządzania ryzykiem jest mitygacja ryzyka. Istotną kwestią jest wyeliminowanie wszelkiego ryzyka z systemu jest niepraktyczne, a być może nawet niemożliwe, proces postepowania z ryzykiem zmierza do ustalenia priorytetów, oceny i wdrożenia odpowiednich zabezpieczeń ograniczających ryzyko zalecanych na podstawie zaleceń przedstawionych w dokumencie NSC 800-53.

Osoby zarządzające systemem i organizacją mają kilka możliwości mitygacji ryzyka obecnego w systemie. Są to: przyjęcie ryzyka, unikanie ryzyka, ograniczanie ryzyka, planowanie ryzyka, badania i uznanie ryzyka, oraz przeniesienie ryzyka.

Na rysunku 10-3 zilustrowano prostą strategię, która może zostać użyta do ustalenia, czy konieczne jest podjęcie działań mitygujących ryzyko. Wychodząc z każdego ryzyka

zidentyfikowanego i przeanalizowanego w trakcie pierwszego procesu—czyli podczas szacowania ryzyka-kierownictwo musi zdecydować, czy ryzyko jest akceptowalne, a następnie czy należy wdrożyć dodatkowe zabezpieczenia w celu złagodzenia niedopuszczalnego ryzyka. Pierwsze pole decyzji na rysunku dotyczy zagrożeń polegających na zamierzonych atakach. Zagrożenia naturalne i błędy ludzkie nie są w tym schemacie decyzyjnym uwzględniane, ponieważ nie są z nimi związane koszty, które należałoby rozważyć, a więc strategia przechodzi do następnego pola decyzji.

Rysunek 10-3. Strategia mitygacji ryzyka

Po podjęciu decyzji o tym, które ryzyka należy uwzględnić w procesie mitygacji ryzyka, dobór zabezpieczeń odbywa się według siedmioetapowego podejścia:

1. uporządkowanie działań pod względem priorytetu,
2. ocena zalecanych rozwiązań w zakresie zabezpieczeń,
3. przeprowadzenie analizy wydajności kosztów,
4. wybór zabezpieczeń,
5. przypisanie odpowiedzialności,
6. opracowanie planu wdrożenia środków bezpieczeństwa,
7. wdrożenie wybranego zabezpieczenia/wybranych zabezpieczeń.

Proces wyboru zabezpieczeń w celu mitygacji ryzyka do akceptowalnego poziomu jest oparty na kategoryzacji bezpieczeństwa systemu wykorzystującej metodologię podaną w NSC 199. Kategoryzacja bezpieczeństwa jest realizowana na dwa sposoby:

(1) określa, które zabezpieczenia bazowe zostają wybrane z NSC800-53, oraz
(2) pomaga w oszacowaniu poziomu ryzyka stwarzanego przez parę zagrożenie/podatność zidentyfikowaną podczas szacowania ryzyka (omówienie identyfikacji zestawów zagrożenie/podatność, zob. Rozdział 5 niniejszego podręcznika oraz NSC 800-30). NSC 200, zaleca wykorzystanie NSC 800-53 do wyboru zabezpieczeń bazowych dla systemów publicznych. Wybrane zabezpieczenia systemu są grupowane w jedną z trzech kategorii: zarządcze, operacyjne lub techniczne. Mają one charakter prewencyjny lub detekcyjny.

W przypadku nowych systemów, po zidentyfikowaniu i dopracowaniu zabezpieczeń oraz przeprowadzeniu wstępnego szacowania ryzyka, wybrane zabezpieczenia muszą zostać wdrożone. W przypadku systemów istniejących, wdrożone zabezpieczenia są poddawane weryfikacji.

Organizacje mogą wykorzystać zabezpieczenia stosowane w wielu systemach poprzez oznaczenie ich jako zabezpieczenia wspólne, których wdrożenie, ocena i monitorowanie odbywa się na poziomie organizacji lub w obszarach szczególnej wiedzy specjalistycznej (np. kadry, bezpieczeństwo fizyczne, zarządzanie budynkami). Właściciel systemu musi rozumieć, kto odpowiada za wdrożenie tych zabezpieczeń i zidentyfikować ryzyko, jakie będzie ze sobą niosło to rozszerzenie zaufania. Informacje na temat zabezpieczeń wspólnych, zob. NSC 800-53.

Ponieważ całkowite wyeliminowanie ryzyka jest niemożliwe, należy zauważyć, że pewien stopień ryzyka szczątkowego pozostanie nawet po wyborze i wdrożeniu zabezpieczeń. Ryzyko szczątkowe powinno zostać przeanalizowane, aby zapewnić, że jego poziom jest akceptowalny. Do wprowadzeniu odpowiednich zabezpieczeń dotyczących zidentyfikowanych ryzyk, osoba autoryzująca podpisuje oświadczenie o akceptacji wszelkiego ryzyka szczątkowego i autoryzuje użytkowanie nowego systemu informacyjnego lub wnioskuje o dalsze wykorzystanie istniejącego systemu informacyjnego. Jeżeli ryzyko szczątkowe nie zostanie ograniczone do akceptowalnego poziomu, cykl zarządzania ryzykiem należy powtórzyć, aby zidentyfikować sposób obniżenia go do poziomu, który można zaakceptować.

10.3. OCENA I EWALUACJA

Trzecią i ostatnią fazą procesu zarządzania ryzykiem jest ewaluacja i ocena. W dzisiejszych dynamicznych i podlegających ciągłym przemianom środowiskach informacyjnych sztuka zarządzania ryzykiem musi mieć charakter bieżący i nieustannie ewoluujący. Systemy są modernizowane i rozbudowywane, ich komponenty są doskonalone, a architektury ciągle ewoluują.

Ewaluacja i ocena zabezpieczeń, przeprowadzana w fazie certyfikacji bezpieczeństwa (*ang. Security Certification Phase*) podczas certyfikacji i akredytacji bezpieczeństwa systemu, dostarcza danych wejściowych potrzebnych do zakończenia szacowania ryzyka[78]. Jej wyniki dostarczają osobie autoryzującej informacji niezbędnych do podjęcia wiarygodnej i opartej na ryzyku decyzji o autoryzacji działania systemu informacyjnego. Najlepiej, gdy działania dotyczące szacowania ryzyka są wykonywane równolegle z certyfikacją i akredytacją systemu. Ponowne wykorzystanie danych z szacowania nie tylko zaoszczędzi cenne zasoby, ale też dostarczy osobie autoryzującej najbardziej aktualnych informacji o ryzyku.

Wiele działań dotyczących zarządzania ryzykiem dotyczy określonego punktu w czasie, stanowiąc statyczne przedstawienie dynamicznego środowiska. Wszystkie zmiany zachodzące w systemach podczas zwykłych, codziennych operacji mogą w pewien sposób negatywnie wpływać na bezpieczeństwo systemu, a celem procesu ewaluacji i oceny zarządzania ryzykiem jest zapewnienie, aby system nadal funkcjonował bezpiecznie i w sposób zabezpieczony. Cel ten zostaje częściowo osiągnięty poprzez wdrożenie silnego programu zarządzania konfiguracją[79]. Dodatkowo, aby na bieżąco monitorować bezpieczeństwo systemu informacyjnego, organizacje muszą śledzić ustalenia oceny zabezpieczeń tak, aby mieć pewność, że są one odpowiednio uwzględniane i przestają stanowić lub wprowadzać nowe ryzyka dla systemu.

Proces zarządzania ryzykiem obejmuje cały cykl życia systemu, począwszy od wczesnych etapów powstawania projektu aż do wycofania systemu i jego danych

---

78 Dodatkowe wytyczne w zakresie procesu certyfikacji i akredytacji, zob. NSC 800-37, a także Rozdział 11 „Certyfikacja i akredytacja" niniejszego podręcznika.

79 Dodatkowe wytyczne w zakresie zarządzania konfiguracją, zob. Rozdział 14 „Zarządzanie konfiguracją" niniejszego podręcznika.

z użycia. Począwszy od powstania projektu, organizacje powinny brać pod uwagę możliwe zagrożenia, podatności i ryzyka dotyczące systemu, tak aby mogły lepiej przygotować system do bezpiecznego i skutecznego działania w zamierzonym środowisku, w granicach wybranego progu ryzyka, w sposób uznany za akceptowalny przez członka wyższego kierownictwa organizacji podczas procesu certyfikacji i akredytacji.

REFERENCJE:

Federal Information Processing Standard 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.

Federal Information Processing Standard 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems (draft)*, April 2006

National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

National Institute of Standards and Technology Special Publication 800-53, *Revision 1*, *Recommended Security Controls for Federal Information System*, February 2006.

National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.

National Institute of Standards and Technology Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle*, Rev. 1, June 2004.

ROZDZIAŁ 11

11. CERTYFIKACJA, AKREDYTACJA I OCENY BEZPIECZEŃSTWA

Certyfikacja i akredytacja bezpieczeństwa to ważne działania, które wspierają proces zarządzania ryzykiem i stanowią integralną część realizowanego przez organizację programu bezpieczeństwa informacji. Proces certyfikacji i akredytacji bezpieczeństwa ma zapewnić, aby system informacyjny podlegał odpowiedniemu przeglądowi zarządczemu, bieżącemu monitorowaniu pod kątem zabezpieczeń, a także, okresowo, ponownej certyfikacji i akredytacji.

Certyfikacja i akredytacja bezpieczeństwa pełnią funkcje podobne do kontroli jakości. Stanowi ona decyzję zarządczą podejmowaną przez członka wyższego kierownictwa organizacji w sprawie autoryzowania działania systemu informacyjnego oraz wyraźnego zaakceptowania ryzyka w imieniu organizacji. W tym sensie, sprawia ona, że osoby akceptujące ryzyko stają się w pełni odpowiedzialne za swoje decyzje, a przez to zachęca do zachowania staranności w procesie podejmowania decyzji.

Stosowne przepisy prawa nakładają na zobowiązane organizacje obowiązek szacowania ryzyka związanego z cyberbezpieczeństwem i przygotowania planów bezpieczeństwa dla wszystkich systemów. Szacowanie ryzyka i plany bezpieczeństwa stanowią niezbędne komponenty procesu certyfikacji i akredytacji bezpieczeństwa. Niezależnie od tego czy ma charakter formalny czy nieformalny, oszacowanie ryzyka dostarcza dużej części danych potrzebnych do sformułowania planu bezpieczeństwa, który uwzględnia ryzyka zidentyfikowane dla danego systemu. Zarówno oszacowanie ryzyka, jak i opracowanie oraz utrzymanie planu bezpieczeństwa dokładnie odzwierciedlającego wymagania i środki bezpieczeństwa wdrożone w danym systemie należy włączyć do cyklu życia systemu (*ang. System Development Life Cycle*, *SDLC*)[80].

Oprócz oszacowania ryzyka i planów bezpieczeństwa systemu, ważną rolę w akredytacji bezpieczeństwa odgrywają oceny bezpieczeństwa. Kierownictwo

[80] Dodatkowe informacje na temat cyklu życia systemu, zob. NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*, a także Rozdział 3 „Cykl życia systemu" niniejszego podręcznika.

organizacji musi koniecznie posiadać możliwie najpełniejsze i najdokładniejsze informacje o stanie bezpieczeństwa swoich systemów informacyjnych, aby móc podejmować terminowe i rozsądne decyzje oparte na ryzyku. Informacje i dowody uzupełniające potrzebne do akredytacji bezpieczeństwa są opracowywane podczas szczegółowej oceny systemu pod kątem bezpieczeństwa, która zazwyczaj nazywana jest certyfikacją bezpieczeństwa.

Certyfikacja bezpieczeństwa to kompleksowa ocena zabezpieczeń zarządczych, operacyjnych i technicznych w systemie informacyjnym, wykonywana dla wsparcia akredytacji bezpieczeństwa w celu ustalenia stopnia, w jakim zabezpieczenia zostały wdrożone prawidłowo, działają zgodnie z zamierzeniem i dają pożądany wynik w zakresie spełnienia wymagań bezpieczeństwa dotyczących systemu. Wyniki certyfikacji bezpieczeństwa są wykorzystywane do ponownego oszacowania ryzyka i zaktualizowania planu bezpieczeństwa systemu, tym samym dając osobie autoryzującej podstawę faktograficzną dla wydania decyzji w sprawie akredytacji bezpieczeństwa.

Dokonując akredytacji systemu informacyjnego, stosowna osoba w organizacji akceptuje ryzyka związane z działaniem systemu i powiązane implikacje dla operacji, aktywów i personelu organizacji. Ukończenie akredytacji bezpieczeństwa stanowi zapewnienie, że system informacyjny będzie podlegał odpowiedniemu przeglądowi zarządczemu i bieżącemu monitorowaniu zabezpieczeń oraz że akredytacja będzie okresowo powtarzana zgodnie z przepisami lub polityką organizacji oraz w przypadku każdej znaczącej zmiany w systemie lub jego środowisku operacyjnym.

Szczegółowe zalecenia dotyczące sposobu certyfikowania i akredytowania systemów informacyjnych zawarte są w publikacji NSC 800-37 i mają zastosowanie do wszystkich systemów informacyjnych, które nie zostały określone jako systemy bezpieczeństwa narodowego. Podmioty publiczne, a także organizacje sektora prywatnego, są zachęcane do korzystania z tych wytycznych według swoich potrzeb. Wytyczne mają na celu:

- umożliwienie bardziej spójnych, porównywalnych i powtarzalnych ocen zabezpieczeń w systemach informacyjnych;

- promowanie lepszego zrozumienia ryzyka związanego z misją organizacji wynikającego z działania systemów informacyjnych;
- stworzenie bardziej kompletnych, rzetelnych i godnych zaufania informacji dla osób autoryzujących, które ułatwią podejmowanie bardziej świadomych decyzji dotyczących akredytacji bezpieczeństwa.

11.1. ROLE I OBOWIĄZKI ZWIĄZANE Z CERTYFIKACJĄ, AKREDYTACJĄ I OCENAMI BEZPIECZEŃSTWA

Chociaż organizacje posiadają różnorodne konwencje nazewnicze/nomenklatury dotyczące ról w zakresie bezpieczeństwa informacji lub certyfikacji i akredytacji bezpieczeństwa, najbardziej podstawowe funkcje w procesie certyfikacji i akredytacji bezpieczeństwa są zasadniczo takie same we wszystkich organizacjach[81]. Proces certyfikacji i akredytacji bezpieczeństwa opisany w niniejszej publikacji jest elastyczny, pozwalając każdej organizacji na zrealizowanie zamysłu konkretnych zadań w obrębie ich organizacji.

11.1.1. CHIEF INFORMATION OFFICER - CIO

CIO (*ang. Chief Information Officer*) blisko współpracuje z osobami autoryzującymi i ich pełnomocnikami dla zapewnienia skutecznego wdrożenia organizacyjnego programu bezpieczeństwa, w tym wszystkich aspektów jego komponentu dotyczącego certyfikacji i akredytacji bezpieczeństwa. CIO ma następujące obowiązki związane z certyfikacją i akredytacją bezpieczeństwa:

- rozpowszechnianie ekonomicznych praktyk, takich jak zachęcanie do maksymalnego ponownego wykorzystywania i dzielenia się informacjami związanymi z bezpieczeństwem, dotyczącymi:
    - ✓ ocen zagrożeń i podatności,
    - ✓ szacunków ryzyka,

[81] Dodatkowe wytyczne dotyczące ról i obowiązków z zakresu bezpieczeństwa, zob. Rozdział 2 „Zarządzanie", Rozdział 5 „Planowanie finansowe", Rozdział 8 „Planowanie bezpieczeństwa" i Rozdział 14 „Zarządzanie konfiguracją" niniejszego podręcznika.

- ✓ wyników ocen wspólnych zabezpieczeń,
- ✓ wszelkich innych informacji ogólnych, które mogą być przydatne właścicielom systemów informacyjnych i ich personelowi zajmującemu się bezpieczeństwem.

- wspólnie z osobą autoryzującą, ustalenie odpowiedniego przydziału zasobów do programów i systemów bezpieczeństwa,
- w pewnych przypadkach, działanie w charakterze osoby autoryzującej w odniesieniu do organizacyjnych systemów ogólnego wsparcia lub osoby współautoryzującej w doniesieniu do wybranych systemów organizacji.

11.1.2. OSOBA AUTORYZUJĄCA

Osoba autoryzująca (lub wyznaczony organ zatwierdzający/akredytujący) to osoba z wyższego kierownictwa uprawniona do formalnego objęcia odpowiedzialności za to, że poziom ryzyka związany z działaniem systemu informacyjnego będzie dla organizacji akceptowalny. Możliwe jest, że konkretny system będzie wymagać więcej niż jednej osoby autoryzującej. W takim przypadku, w planie bezpieczeństwa systemu należy udokumentować porozumienia zawarte między osobami autoryzującymi. W większości przypadków, korzystne może być uzgodnienie wyboru wiodącej osoby autoryzującej, która będzie reprezentować interesy wszystkich pozostałych. Osoba autoryzujące posiada nieodłączne uprawnienia organizacji i jako taka musi być pracownikiem organizacji. Osoba autoryzująca ma następujące obowiązki związane z certyfikacją i akredytacją bezpieczeństwa:

- nadzorowanie budżetu i operacji biznesowych systemu;
- zatwierdzanie wymagań w zakresie bezpieczeństwa systemu, planów bezpieczeństwa systemu oraz protokołów uzgodnień i/lub porozumień o współpracy;
- podejmowanie i wydawanie ostatecznych lub tymczasowych decyzji w sprawie przyznania, warunkowego przyznania lub odmowy przyznania uprawnień do użytkowania systemu;

- wyznaczanie, według uznania, pełnomocnika, który będzie występować w imieniu osoby autoryzującej i prowadzić konieczne działania wymagane podczas certyfikacji i akredytacji bezpieczeństwa systemu.

Pełnomocnik osoby autoryzującej

Pełnomocnik osoby autoryzującej może zostać upoważniony do występowania w jej imieniu we wszystkich działania certyfikacyjnych i akredytacyjnych, za które osoba autoryzująca ponosi odpowiedzialność, z wyjątkiem: 1) wydania decyzji o akredytacji bezpieczeństwa dla systemu, oraz 2) podpisania dokumentu decyzji o akredytacji bezpieczeństwa dla systemu.

11.1.3. SENIOR AGENCY INFORMATION SECURITY OFFICER - SAISO

SAISO (lub członek personelu pomocniczego) może pełnić funkcję pełnomocnika osoby autoryzującej. SAISO jest głównym łącznikiem między CIO i osobami autoryzującymi, właścicielami systemu informacyjnego i ISSO (*ang. Information System Security Officer*).

11.1.4. WŁAŚCICIEL SYSTEMU INFORMACYJNEGO

Właściciel systemu informacyjnego odpowiada za zamówienia, rozwój, integrację, modyfikację lub obsługę i utrzymanie systemu informacyjnego. Właściciel systemu informacyjnego ma następujące obowiązki związane z certyfikacją i akredytacją bezpieczeństwa:

- opracowanie i utrzymanie planu bezpieczeństwa systemu;
- zapewnienie uruchomienia i użytkowania systemu według uzgodnionych wymagań bezpieczeństwa;
- autoryzowanie dostępu użytkowników do systemu informacyjnego (oraz decydowanie o rodzajach przywilejów lub praw dostępu);
- zapewnienie niezbędnego przeszkolenia użytkowników i personelu wsparcia systemu (np. w zakresie zasad zachowania);
- informowanie kluczowych osób w organizacji o potrzebie przeprowadzenia certyfikacji i akredytacji bezpieczeństwa systemu informacyjnego;

- zapewnienie dostępności odpowiednich zasobów na potrzeby certyfikacji i akredytacji bezpieczeństwa;
- udostępnienia organowi certyfikującemu koniecznej dokumentacji związanej z systemem;
- podjęcie odpowiednich kroków w celu zniwelowania lub wyeliminowania podatności zidentyfikowanych w procesie certyfikacji i akredytacji bezpieczeństwa;
- zgromadzenie pakietu akredytacji bezpieczeństwa i przesłanie go osobie autoryzującej lub jej pełnomocnikowi do zaopiniowania.

11.1.5. WŁAŚCICIEL INFORMACJI

Właściciel informacji posiada uprawnienia ustawowe, zarządcze lub operacyjne w zakresie określonych informacji oraz jest odpowiedzialny za ustanowienie polityki i procedur regulujących ich wytwarzanie, gromadzenie, przetwarzanie, rozpowszechnianie i usuwanie. Właściciel informacji ma następujące obowiązki związane z certyfikacją i akredytacją bezpieczeństwa:

- ustanowienie zasad odpowiedniego użytkowania i ochrony przedmiotowych informacji (np. zasad zachowania);
- informowanie odpowiedniego właściciela systemu o poziomie wiarygodności informacji wymaganym dla systemu.

11.1.6. INFORMATION SYSTEM SECURITY OFFICER - ISSO

ISSO odpowiada przed osobą autoryzującą, właścicielem systemu informacyjnego lub SAISO za zapewnienie utrzymania odpowiedniego stanu bezpieczeństwa operacyjnego programu lub systemu informacyjnego. ISSO ma następujące obowiązki związane z certyfikacją i akredytacją bezpieczeństwa:

- występowanie w charakterze głównego doradcy wobec osoby autoryzującej, właściciela systemu informacyjnego lub SAISO we wszystkich sprawach dotyczących bezpieczeństwa systemu informacyjnego;

- wykonywanie lub nadzorowanie wykonania wszystkich codziennych operacji systemu związanych z bezpieczeństwem;
- opracowanie lub pomoc w opracowaniu polityk bezpieczeństwa systemu;
- zapewnienie przestrzegania zasad bezpieczeństwa systemu;
- koordynowanie zmian/zarządzanie zmianami w systemie wspólnie z właścicielem systemu i właścicielem informacji (w razie konieczności);
- ocenianie wpływu zmian systemowych na bezpieczeństwo;
- opracowanie i aktualizowanie planu bezpieczeństwa systemu.

11.1.7. ORGAN CERTYFIKUJĄCY

Organ certyfikujący (*ang. Certification Agent*) to osoba, grupa osób lub organizacja odpowiedzialna za przeprowadzenie certyfikacji bezpieczeństwa lub kompleksowej oceny skuteczności zabezpieczeń w systemie informacyjnym. Bezstronność i niezależność organu certyfikującego to ważne czynniki w ocenie wiarygodności wyników oceny bezpieczeństwa i zapewnieniu, aby osoba autoryzująca otrzymała możliwie najbardziej obiektywne informacje umożliwiające podjęcie świadomej, opartej na ryzyku decyzji w sprawie akredytacji. Organ certyfikujący ma następujące obowiązki związane z certyfikacją i akredytacją bezpieczeństwa:

- przeprowadzenie oceny planu bezpieczeństwa systemu w celu zapewnienia, aby zawierał on stosowne zabezpieczenia przed zainicjowaniem procesu certyfikacji;
- wykonanie kompleksowej analizy zabezpieczeń zarządczych, operacyjnych i technicznych obecnych w systemie informacyjnym;
- zalecenie działań naprawczych w celu zniwelowania lub wyeliminowania podatności obecnych w systemie informacyjnym.

11.1.8. PRZEDSTAWICIELE UŻYTKOWNIKÓW

Użytkownicy odpowiadają za identyfikowanie wymagań dotyczących misji/operacji oraz za zachowanie zgodności z wymaganiami bezpieczeństwa i zabezpieczeniami opisanymi w planie bezpieczeństwa systemu. Przedstawiciele użytkowników (*ang. User*

Representatives) to osoby reprezentujące interesy operacyjne społeczności użytkowników i pełnią rolę jej łączników w trakcie całego cyklu życia systemu informacyjnego. Przedstawiciele użytkowników w razie potrzeby pomagają w procesie certyfikacji i akredytacji bezpieczeństwa, aby zapewnić spełnienie wymagań misji przy jednoczesnym spełnieniu wymagań bezpieczeństwa i wykorzystaniu zabezpieczeń zdefiniowanych w planie bezpieczeństwa systemu.

11.2. DELEGOWANIE RÓL

Pewne role związane z certyfikacją i akredytacją bezpieczeństwa mogą być delegowane według uznania wyższego kierownictwa organizacji. W takim przypadku, delegowanie musi zostać udokumentowane. Kierownictwo organizacji może powoływać odpowiednio wykwalifikowane osoby, w tym wykonawców, do wykonywania zadań związanych z rolami w certyfikacji i akredytacji bezpieczeństwa, z wyjątkiem CIO i osoby autoryzującej (AO. Osoby pełniące delegowane role mogą działać z uprawnieniami wynikającymi z zakresu wyznaczonym dla konkretnych działań związanych z certyfikacją i akredytacją bezpieczeństwa. Personel organizacji zachowuje jednak ostateczną odpowiedzialność za wyniki działań osób pełniących delegowane role.

11.3. PROCES CERTYFIKACJI I AKREDYTACJI BEZPIECZEŃSTWA

Proces certyfikacji i akredytacji bezpieczeństwa składa się z czterech oddzielnych faz, z których każda dzieli się na dokładnie zdefiniowane zadania i podzadania. Cztery fazy to:

- faza inicjacji,
- faza certyfikacji bezpieczeństwa,
- faza akredytacji bezpieczeństwa,
- faza ciągłego monitorowania.

Faza inicjacji składa się z trzech zadań. Są to: (1) przygotowanie, (2) zawiadomienie i identyfikacja zasobów, oraz (3) przegląd, analiza i akceptacja planu bezpieczeństwa systemu. Faza ta stanowi potwierdzenie, że osoba autoryzująca i SAISO zgadzają się

z treścią planu bezpieczeństwa systemu zanim organ certyfikujący rozpocznie ocenę zabezpieczeń systemu informacyjnego.

Faza certyfikacji bezpieczeństwa składa się z dwóch zadań. Są to: (1) ocena zabezpieczeń, oraz (2) udokumentowanie certyfikacji bezpieczeństwa. System informacyjny musi spełnić minimalne wymagania bezpieczeństwa wg. NSC 200, poprzez wdrożenie odpowiednich zabezpieczeń i wymagań dotyczących wiarygodności zawartych w NSC 800- 53. Oceny systemu polegają na zbadaniu, dokonaniu przeglądu i przetestowaniu wdrożenia odpowiednich bazowych środków bezpieczeństwa zawartych w NSC 800-53. Procedury oceny i składania sprawozdań z wyników oceny zawarto w NSC 800-53A.

Faza certyfikacji bezpieczeństwa ustala stopień, w jakim zabezpieczenia zostały prawidłowo wdrożone, działają zgodnie z zamierzeniami i dają pożądany stan bezpieczeństwa systemu. W tej fazie identyfikowane są też konkretne działania podjęte lub planowane w celu skorygowania braków w zabezpieczeniach i zniwelowania lub wyeliminowania znanych podatności systemu. Na zakończenie tej fazy, osoba autoryzująca powinna dysponować wystarczającymi danymi do oceny poziomu ryzyka, jakie system stwarza dla organizacji oraz do wydania decyzji w sprawie akredytacji bezpieczeństwa.

Faza akredytacji bezpieczeństwa składa się z dwóch zadań. Są to: (1) decyzja w sprawie akredytacji bezpieczeństwa oraz (2) udokumentowanie akredytacji bezpieczeństwa. Celem tej fazy jest pomoc organowi akredytującemu w ustaleniu, czy poziom ryzyka stwarzanego przez znane podatności pozostałe w systemie (po wdrożeniu uzgodnionego zestawu zabezpieczeń) jest dla organizacji akceptowalny. Po udanym zakończeniu tej fazy właściciel systemu informacyjnego stanie przed jednym z trzech poniższych scenariuszy:

- udzielenie formalnego upoważnienia do działania systemu informacyjnego;
- udzielenie tymczasowego upoważnienia do działania systemu informacyjnego pod określonymi warunkami;
- odmowa udzielenia upoważnienia do działania systemu informacyjnego.

Pakiet akredytacji bezpieczeństwa

Właściciel systemu informacyjnego jest zazwyczaj odpowiedzialny za zebranie dokumentacji dotyczącej certyfikacji i akredytacji. Właściciel systemu powinien jednakże ściśle współpracować z właścicielem informacji, ISSO oraz organem certyfikującym, aby zapewnić, że pakiet akredytacyjny spełnia wszystkie wymagania organizacji.

Fazę ciągłego monitorowania omówiono w podrozdziale 11.6.

11.4. DOKUMENTACJA CERTYFIKACJI BEZPIECZEŃSTWA

Kulminacją całego procesu certyfikacji i akredytacji bezpieczeństwa jest wydanie przez pracownika organizacji decyzji w sprawie zarządzania ryzykiem. Pakiet akredytacji bezpieczeństwa dokumentuje wyniki certyfikacji bezpieczeństwa i dostarcza osobie autoryzującej informacji niezbędnych do podjęcia wiarygodnej, opartej na ryzyku decyzji o tym, czy upoważnić systemu informacyjny do działania. Pakiet akredytacji bezpieczeństwa zawiera następujące dokumenty:

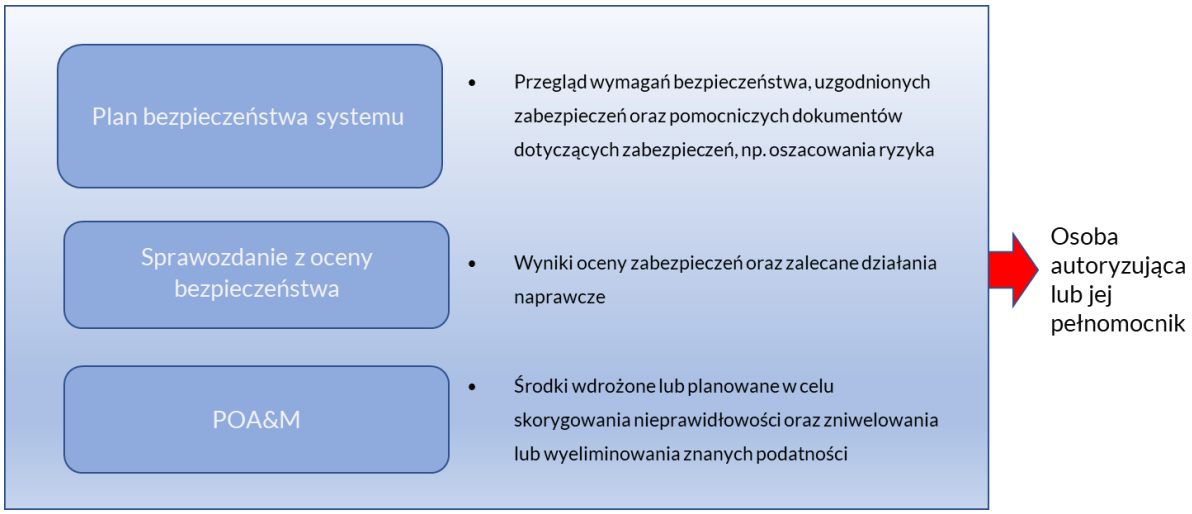
- zatwierdzony plan bezpieczeństwa systemu,
- sprawozdanie z oceny bezpieczeństwa,
- plan i etapy działania (POA&M).

Plan bezpieczeństwa systemu stanowi przegląd wymagań bezpieczeństwa dla systemu informacyjnego i zawiera wyjaśnienie środków podjętych lub planowanych przez właściciela systemu informacyjnego w celu spełnienia tych wymagań[82]. Chociaż nie jest on ściśle wymagany, a jego sporządzenie pozostawiane jest do uznania organizacji, plan ten może zawierać pomocnicze załączniki lub, w ramach odniesień, inne dokumenty dotyczące bezpieczeństwa systemu. Wśród dokumentów tych mogą się znaleźć: oszacowanie ryzyka, ocena wpływu na prywatność, plan awaryjny, plan zarządzania konfiguracją, listy kontrolne konfiguracji zabezpieczeń oraz ewentualne umowy o połączeniu systemów.

[82] Dodatkowe wytyczne w zakresie planowania bezpieczeństwa systemu, zob. NSC 800-18, a także Rozdział 8 „Planowanie bezpieczeństwa" niniejszego podręcznika.

Sprawozdanie z oceny bezpieczeństwa (*ang. Security Assessment Report - SAR*) podsumowuje wyniki działań podjętych przez organ certyfikujący. Sprawozdanie z oceny bezpieczeństwa może też zawierać listę zalecanych działań naprawczych i wypełniony formularz sprawozdawczy.

Dokument **POA&M** opisuje środki wdrożone lub planowane w celu naprawienia wszelkich braków stwierdzonych podczas oceny zabezpieczeń oraz zniwelowania lub wyeliminowania znanych podatności systemu. Na rys. 11-1 przedstawiono przegląd kluczowych części składowych pakietu akredytacji bezpieczeństwa.



Rysunek 11-1. Kluczowe komponenty akredytacji bezpieczeństwa

11.5. DECYZJE W SPRAWIE AKREDYTACJI

Pakiet akredytacji bezpieczeństwa dokumentuje wyniki certyfikacji bezpieczeństwa. Dla zapewnienia pełnego uwzględnienia potrzeb biznesowych i operacyjnych organizacji, osoba autoryzująca powinna przed wydaniem decyzji w sprawie akredytacji bezpieczeństwa skontaktować się z właścicielem systemu. Podczas tego spotkania organy certyfikacji i akredytacji powinny wyraźnie uzasadnić swoją decyzję opartą na ryzyku oraz, w stosownych przypadkach, podać pełne wyjaśnienie warunków autoryzacji.

Decyzja o akredytacji bezpieczeństwa informuje o decyzji podjętej przez organ akredytujący i przekazuje właścicielowi systemu informacyjnego:

- decyzję w sprawie akredytacji bezpieczeństwa - czyli oficjalną decyzję osoby autoryzującej o akredytacji systemu, akredytacji systemu pod pewnymi warunkami lub odmowie akredytacji systemu;
- uzasadnienie decyzji wydanej przez osobę autoryzującą;
- warunki autoryzacji - limity lub ograniczenia dotyczące użytkowania systemu, które są dla właściciela systemu wiążące.

Treść dokumentacji dotyczącej certyfikacji i akredytacji bezpieczeństwa, w szczególności informacje o podatnościach systemu informacyjnego, należy sklasyfikować i odpowiednio chronić zgodnie z polityką organizacji, a także zarchiwizować zgodnie z obowiązującymi w organizacji zasadami przechowywania danych.

11.6. CIĄGŁE MONITOROWANIE

Faza ciągłego monitorowania jest niezbędnym komponentem każdego programu bezpieczeństwa. Podczas niej na bieżąco sprawdzany jest status zabezpieczeń systemu informacyjnego. Skuteczny program ciągłego monitorowania może służyć wsparciu realizacji wymogu corocznych audytów w zakresie oceny zabezpieczeń systemów informacyjnych. Jako minimum, skuteczny program monitorowania wymaga realizacji:

- procesów zarządzania konfiguracją i kontroli konfiguracji systemu informacyjnego;
- analiz wpływu zmian w systemie informacyjnym na bezpieczeństwo;
- oceny wybranych zabezpieczeń systemu informacyjnego i złożenia odpowiednim osobom w organizacji sprawozdania ze stanu bezpieczeństwa systemu informacyjnego.

Aby ustalić, które zabezpieczenia należy wybrać do przeglądu, organizacje powinny najpierw skupić się na pozycjach POA&M, które zostały zakończone. Te nowo wdrożone zabezpieczenia należy poddać walidacji. Organizacje powinny przeprowadzić testy pod kątem związanych z bezpieczeństwem zmian w systemie, które już wystąpiły, ale które nie stanowią znaczących zmian wymagających nowego

procesu certyfikacji i akredytacji. Organizacje powinny zidentyfikować wszystkie zabezpieczenia, które są monitorowane w sposób ciągły jako coroczne działania z zakresu testowania i ewaluacji. Do przykładów należą m.in. bieżące szkolenia w zakresie bezpieczeństwa, działania związane z ochroną przed zdarzeniami typu odmowa świadczenia usługi (DoS) i przed złośliwym kodem, monitorowanie w zakresie wykrywania włamań, przeglądy plików dziennika itp. Następnie organizacje powinny przeanalizować pozostałe zabezpieczeniom, które nie zostały przetestowane w bieżącym roku i w oparciu o ryzyko, znaczenie danego zabezpieczenia i datę ostatniego testu zdecydować, czy wykonać test coroczny.

Wyniki ciągłego monitorowania powinny być regularnie zgłaszane do osoby autoryzującej i SAISO, a do planu bezpieczeństwa systemu należy wprowadzać niezbędne aktualizacje.

11.7. OCENY PROGRAMU BEZPIECZEŃSTWA INFORMACJI

Organizacje powinny dokonywać opracowania, udokumentowania i wdrożenia w całej swojej strukturze programu bezpieczeństwa informacji mającego zapewnić bezpieczeństwo informacji oraz systemów informacyjnych, które obsługują ich działania i zasoby, w tym te udostępniane lub zarządzane przez inne organizacje, wykonawców i inne podmioty.

Dla zapewnienia adekwatności i skuteczności środków bezpieczeństwa informacji, należy wymagać od CIO oraz personelu odpowiedzialnego za program bezpieczeństwa w organizacji przeprowadzania okresowych przeglądów obowiązującego w organizacji programu bezpieczeństwa informacji i składania sprawozdań, jeśli wymagają tego stosowne przepisy.

Dodatkowo wymagane jest, aby każda organizacja co roku przeprowadziła niezależną ocenę swojego programu bezpieczeństwa informacji. Ocenę tę może przeprowadzać osoba wyznaczona w ramach organizacji lub audytor zewnętrzny. W obu przypadkach, jeśli przepisy wymagają składania rocznych sprawozdań, sprawozdanie powinno zawierać ocenę niezależną.

Aby pomóc organizacjom w spełnieniu wymagań w zakresie corocznej sprawozdawczości, w Kwestionariuszu oceny programu bezpieczeństwa informacji (stanowiącym załącznik 11.A) zawarto szereg pytań dotyczących obszarów, które zwykle należy ująć z sprawozdaniu organizacji. Kwestionariusz zawiera pytania dotyczące całej organizacji, dotyczące programu, które nie znajdują się w publikacji NSC 800-53. Kwestionariusz można dostosowywać dodając specyficzne dla danej organizacji pytania związane z programem. Może on zostać wypełniony przez CIO, SAISO lub niezależnego oceniającego.

Kwestionariusz składa się ze strony tytułowej i szeregu pytań dotyczących obowiązującego w organizacji programu bezpieczeństwa informacji. Na stronie tytułowej należy podać informacje opisowe, takie jak nazwa organizacji, biura lub jednostki operacyjnej, a także imię i nazwisko, tytuł oraz organizację osoby wypełniającej kwestionariusz. Należy również podać datę i okres objęty sprawozdaniem oraz opisać cel oceny. Ostatnią informacją podawaną na stronie tytułowej jest liczba systemów organizacji w poszczególnych kategoriach wpływu wg. NSC 199 (niski, umiarkowany, wysoki).

Znajdujące się dalej pytania dotyczą zarządzania organizacyjnym programem bezpieczeństwa informacji. Każde z nich dotyczy elementów programu bezpieczeństwa informacji, które mają krytyczne znaczenie dla powodzenia tego programu. Ta część kwestionariusza jest elastyczna i można ją rozszerzać. Organizacja może dodać tyle pytań, ile uzna za stosowne, aby pełniej ocenić status i/lub skuteczność swojego programu bezpieczeństwa informacji albo odnieść się do kwestii podnoszonych przez inne zainteresowane strony.

Odpowiedzi na każde pytanie należy udzielić dla każdego poziomu dojrzałości bezpieczeństwa informacyjnego. W przypadku poziomu dojrzałości „Polityka”, aby można było udzielić odpowiedzi „Tak”, zagadnienie powinno być udokumentowane w polityce organizacji. W przypadku poziomu dojrzałości „Procedury”, aby można było udzielić odpowiedzi „Tak”, zagadnienie powinno być udokumentowane w szczegółowych procedurach. W przypadku poziomu dojrzałości „Wdrożone”, aby można było udzielić odpowiedzi „Tak”, wdrożenie musi być zweryfikowane badaniem

procedur i dokumentacji programowej, a także wywiadami z kluczowym personelem, aby ustalić, że procedury są wdrażane. W przypadku poziomu dojrzałości „Przetestowano", aby można było udzielić odpowiedzi „Tak", należy zbadać dokumenty i przeprowadzić wywiady, aby zweryfikować, że zasady i procedury, których dotyczy pytanie są wdrażane i działają zgodnie z zamierzeniami oraz dają pożądany poziom bezpieczeństwa. W przypadku poziomu dojrzałości „Zintegrowano", aby udzielić odpowiedzi „Tak", zasady, procedury, wdrażanie i testowanie muszą podlegać ciągłemu monitorowaniu, a doskonalenie odbywa się w ramach normalnej działalności organizacji.

REFERENCJE:

Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

Federal Information Processing Standard 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

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

National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems (draft)*, April 2006.

National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

National Institute of Standards and Technology Special Publication 800-53, *Revision 1*, *Recommended Security Controls for Federal Information System*, February 2006.

National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.

National Institute of Standards and Technology Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle*, Rev. 1, June 2004.

Załącznik 11.A Kwestionariusz oceny programu bezpieczeństwa informacji

Nazwa organizacji:_____

Imię i nazwisko osoby odpowiedzialnej: _____

Imiona i nazwiska oceniających: _____

Data sporządzenia sprawozdania: _____

Okres objęty sprawozdaniem: _____

Cel sprawozdania: _____

Podsumowanie systemu organizacji:

Liczba systemów w każdej kategorii poziomu wpływu wg. NSC 199

Niski: _____ **Umiarkowany:** _____ **Wysoki:** _____

Pytania dotyczące programu bezpieczeństwa informacji

Odpowiedzi na każde pytanie należy udzielić dla każdego poziomu dojrzałości bezpieczeństwa informacyjnego. Każda kolumna przedstawia poziom dojrzałości bezpieczeństwa informacyjnego. W przypadku poziomu dojrzałości „Polityka", aby można było udzielić odpowiedzi „Tak", zagadnienie powinno być udokumentowane w polityce organizacji. W przypadku poziomu dojrzałości „Procedury", aby można było udzielić odpowiedzi „Tak", zagadnienie powinno być udokumentowane w szczegółowych procedurach. W przypadku poziomu dojrzałości „Wdrożono", aby można było udzielić odpowiedzi „Tak", wdrożenie musi być zweryfikowane badaniem procedur i dokumentacji programowej, a także wywiadami z kluczowym personelem, aby ustalić, że procedury są wdrażane. W przypadku poziomu dojrzałości „Przetestowano", aby można było udzielić odpowiedzi „Tak", należy zbadać dokumenty i przeprowadzić wywiady, aby zweryfikować, że zasady i procedury, których dotyczy pytanie są wdrażane i działają zgodnie z zamierzeniami oraz dają pożądany poziom bezpieczeństwa. W przypadku poziomu dojrzałości „Zintegrowano", aby udzielić odpowiedzi „Tak", zasady, procedury, wdrażanie i testowanie muszą podlegać ciągłemu monitorowaniu, a doskonalenie odbywa się w ramach normalnej działalności organizacji.

Pytania dotyczące programu	Zasady	Procedury	Wdrożono	Przetestowano	Zintegrowano	Uwagi
1. Proces przeglądu zabezpieczeń Czy kierownictwo zapewnia, aby działania naprawcze dotyczące bezpieczeństwa informacji były śledzone przy użyciu procesu POA&M?						

Pytania dotyczące programu	Zasady	Procedury	Wdrożono	Przetestowano	Zintegrowano	Uwagi
2. Planowanie finansowe i kontrola inwestycji Czy organizacja wymaga użycia uzasadnienia biznesowego/Załącznika 300/Załącznika 53 do rejestracji zasobów wymaganych do utrzymania akceptowalnego poziomu ryzyka dla wszystkich swoich programów i systemów?						
3. Komisja oceny inwestycji Czy powołano i upoważniono Komisję oceny inwestycji (lub podobne gremium) dla zapewnienia, aby wszystkie wnioski inwestycyjne zawierały wymagane zasoby bezpieczeństwa, a wszystkie wyjątki od tego wymogu były dokumentowane?						
4. Integrowanie bezpieczeństwa informacji i ochrony infrastruktury krytycznej z planowaniem finansowym i kontrolą inwestycji Czy realizowana jest integracja bezpieczeństwa informacji i ochrony infrastruktury krytycznej						

Pytania dotyczące programu	Zasady	Procedury	Wdrożono	Przetestowano	Zintegrowano	Uwagi
z procesem planowania finansowego i kontroli inwestycji?						
5. Budżet i zasoby Czy zasoby bezpieczeństwa informacji (etaty wewnętrzne i finansowanie) przydzielone do ochrony informacji i systemów informacyjnych są zgodne z oszacowanym ryzykiem?						
6. Wykaz systemów i projektów Czy projekty i systemy IT zostały zidentyfikowane w wykazie i czy informacje o nich są istotne dla procesu zarządzania inwestycjami? Czy prowadzony jest wykaz systemów?						
7. Metryki bezpieczeństwa informacyjnego Czy metryki bezpieczeństwa informacyjnego są zbierane w całej organizacji i zgłaszane?						

Pytania dotyczące programu	Zasady	Procedury	Wdrożono	Przetestowano	Zintegrowano	Uwagi
8. Architektura korporacyjna oraz profil bezpieczeństwa i prywatności architektury korporacyjnej Czy wymogi i możliwości w zakresie bezpieczeństwa i ochrony prywatności informacji na poziomie systemu i organizacji są dokumentowane w ramach architektury korporacyjnej organizacji? Czy informacje te są wykorzystywane do zrozumienia aktualnego ryzyka dla misji organizacji? Czy informacje te są wykorzystywane do pomocy kierownictwu programu i organizacji w wyborze najlepszych rozwiązań z zakresu bezpieczeństwa i ochrony prywatności dla realizacji misji?						
9. Plan ochrony infrastruktury krytycznej Jeżeli jest to wymagane, czy w Twojej organizacji jest udokumentowany plan ochrony infrastruktury krytycznej i zasobów kluczowych.						

Pytania dotyczące programu	Zasady	Procedury	Wdrożono	Przetestowano	Zintegrowano	Uwagi
10. Zarządzanie cyklem życia Czy istnieje proces zarządzania cyklem życia systemu, który wymaga, aby każdy system podlegał certyfikacji i akredytacji? Czy działanie każdego systemu zostało oficjalnie zatwierdzone? Czy o procesie zarządzania cyklem życia są informowane odpowiednie osoby?						

Pytanie dla przypadku, w którym istnieje obowiązek powołania przez organizację SAISO, który kieruje jednostką w organizacji odpowiedzialną za misję i zasoby przeznaczone na opracowanie i utrzymanie organizacyjnego programu bezpieczeństwa informacji. Odpowiedź „Tak” potwierdza zgodność. Odpowiedzi „Nie” powinno towarzyszyć wyjaśnienie i termin, w jakim ten obowiązek zostanie spełniony.

Pytanie	Zrealizowano?	Uwagi
SAISO Czy powołano SAISO z misją i zasobami przeznaczonymi na opracowanie i utrzymanie organizacyjnego programu bezpieczeństwa informacji?		

Załącznik 11.B Zabezpieczenia minimalne

Zabezpieczenia znajdujące się w katalogu zabezpieczeń publikacji NSC 800-53 mają ściśle zdefiniowaną organizację i strukturę. Dla łatwego wykorzystania w doborze i specyfikacji zabezpieczeń podzielono je na klasy i kategorie. Występują trzy ogólne klasy zabezpieczeń (tzn. zarządcze, operacyjne i techniczne[83]). W każdej kategorii znajdują się zabezpieczenia związane z funkcją bezpieczeństwa tej kategorii. Każdej kategorii zabezpieczeń przypisano niepowtarzalny, dwuliterowy identyfikator.

Tabela 11-1 zawiera zestawienie klas i kategorii w katalogu zabezpieczeń wraz z przypisanymi identyfikatorami kategorii.

Tabela 11-1. Klasy, kategorie i identyfikatory zabezpieczeń

KLASA	KATEGORIA	IDENTYFIKATOR
Zarządcze	Szacowanie ryzyka	RA
Zarządcze	Planowanie	PL
Zarządcze	Nabywanie systemu i usług	SA
Zarządcze	Certyfikacja, akredytacja i oceny bezpieczeństwa	CA
Zarządcze	Programy zarządzania	PM
Zarządcze	Przejrzystość przetwarzanie danych osobowych	PT
Zarządcze	Zarządzanie ryzykiem w łańcuchu dostaw	SR
Operacyjne	Bezpieczeństwo osobowe	PS
Operacyjne	Ochrona fizyczna i środowiskowa	PE
Operacyjne	Planowanie awaryjne	CP
Operacyjne	Zarządzanie konfiguracją	CM

[83] Kategorie zabezpieczeń z publikacji NSC 800-53 są powiązane z jedną z trzech klas zabezpieczeń (zarządcze, operacyjne, techniczne). Kategorie są umieszczane w odpowiednich klasach na podstawie dominujących cech zabezpieczeń w danej kategorii. Jednakże wiele zabezpieczeń można w logiczny sposób przypisać do więcej niż jednej klasy. Na przykład, pozycja CP-1, czyli polityka i procedury z kategorii „Planowanie awaryjne", jest wymieniona jako zabezpieczenie operacyjne, ale posiada również cechy odpowiadające zarządzaniu bezpieczeństwem.

KLASA	KATEGORIA	IDENTYFIKATOR
Operacyjne	Utrzymanie	MA
Operacyjne	Integralność systemu i informacji	SI
Operacyjne	Ochrona nośników danych	MP
Operacyjne	Reagowanie na incydenty	IR
Operacyjne	Uświadamianie i szkolenia	AT
Techniczne	Identyfikacja i uwierzytelnianie	IA
Techniczne	Kontrola dostępu	AC
Techniczne	Audyt i rozliczalność	AU
Techniczne	Ochrona systemów i sieci telekomunikacyjnych	SC

Poniżej zdefiniowano klasy zabezpieczeń (tzn. zarządcze, operacyjne i techniczne) dla zachowania jasności podczas przygotowywania planów bezpieczeństwa systemu.

Zabezpieczenia zarządcze skupiają się na zarządzaniu systemem informacyjnym oraz ryzykiem dla systemu. Są to techniki i kwestie, które zazwyczaj są podejmowane przez kierownictwo. *Zabezpieczenia operacyjne* dotyczą metod zabezpieczenia koncentrujących się na mechanizmach wdrażanych i wykonywanych głównie przez ludzi (w odróżnieniu od systemów). Są one wdrażane w celu poprawy bezpieczeństwa konkretnego systemu (lub grupy systemów). Często wymagają wiedzy specjalistycznej lub technicznej i również często polegają na działaniach zarządczych oraz zabezpieczeniach technicznych.

Zabezpieczenia techniczne skupiają się na środkach bezpieczeństwa wykonywanych przez system komputerowy. Mogą zapewnić zautomatyzowaną ochronę przed nieautoryzowanym dostępem lub niewłaściwym wykorzystaniem, ułatwiają wykrycie naruszeń bezpieczeństwa oraz stanowią wsparcie dla wymagań bezpieczeństwa dotyczących aplikacji i danych.

ROZDZIAŁ 12

12. NABYWANIE USŁUG I PRODUKTÓW BEZPIECZEŃSTWA

Usługi i produkty bezpieczeństwa informacji to niezbędne elementy programu bezpieczeństwa informacji każdej organizacji. Obecnie na rynku znajduje się wiele produktów i usług, które mają wspierać organizacyjne programy bezpieczeństwa informacji w zakresie systemów informacyjnych. Wybór i użycie produktów i usług bezpieczeństwa w ramach ogólnego programu organizacji ma służyć zarządzaniu projektem, rozwojem i utrzymaniem jej infrastruktury bezpieczeństwa informacji oraz ochronie informacji o krytycznym znaczeniu dla jej misji. Nabywając te produkty i usługi organizacje powinny stosować zasady zarządzania ryzykiem, które są pomocne w identyfikowaniu i postępowaniu z ryzykiem związanym z takimi zakupami.

Jeżeli chodzi o nabywanie produktów bezpieczeństwa informacji, organizacje są zachęcane do przeprowadzenia, w ramach procesu wyboru produktu, analizy kosztów i korzyści, która obejmuje również koszty związane z mitygacją ryzyka. Taka analiza powinna uwzględniać szacunkowy koszt cyklu życia (*ang. Life Cycle Cost - LCC*) dla stanu obecnego oraz dla każdej określonej alternatywy, przy czym należy podkreślić korzyści płynące z każdej z tych alternatyw. Publikacja specjalna NIST SP 800-36, *Guide to Selecting Information Technology (IT) Security Products*[84], definiuje szerokie kategorie produktów bezpieczeństwa oraz określa typy i charakterystyki produktów oraz kwestie środowiskowe w obrębie tych kategorii. Przewodnik podaje następnie listę stosownych pytań, które organizacje powinny zadać wybierając produkty.

Podobnie do nabywania produktów, nabywane usług niesie ze sobą znaczące ryzyko, które organizacje muszą identyfikować i mitygować. Znaczenia systematycznego zarządzania procesem nabywania usług z zakresu bezpieczeństwa informacji nie można bagatelizować ze względu na potencjalny wpływ związanego z tym procesem ryzyka. Wybierając tego typu usługi organizacje powinny wykorzystywać procesy zarządzania ryzykiem w kontekście cyklu życia tych usług, co stwarza ramy organizacyjne dla osób podejmujących decyzje w sprawie bezpieczeństwa informacji. Publikacja NIST SP 800-

[84] Podano jako przykład w celach uzupełniających dla zainteresowanych.

35, *Guide to Information Technology Security Services*[85], pomaga czytelnikowi w wyborze, wdrożeniu i zarządzaniu usługami bezpieczeństwa informacji, omawiając różne fazy cyklu życia tych usług. Decydenci zajmujący się bezpieczeństwem informacji muszą wziąć pod uwagę koszty, wymagania bezpieczeństwa oraz wpływ podejmowanych przez siebie decyzji na misję, działalność, funkcje strategiczne i personel organizacji oraz na podejmowane ustalenia z dostawcami usług.

W procesie wyboru produktów i usług z zakresu bezpieczeństwa informacji uczestniczy wiele osób z całej organizacji. Każda z nich, zarówno na poziomie indywidualnym jak i grupowym, powinna zrozumieć znaczenie bezpieczeństwa w infrastrukturze informatycznej organizacji oraz wpływ swoich decyzji na to bezpieczeństwo. W zależności od potrzeb, organizacja może uwzględnić wszystkie z wymienionych niżej osób albo też wybrać te z nich, które są istotne dla bezpieczeństwa jej informacji:

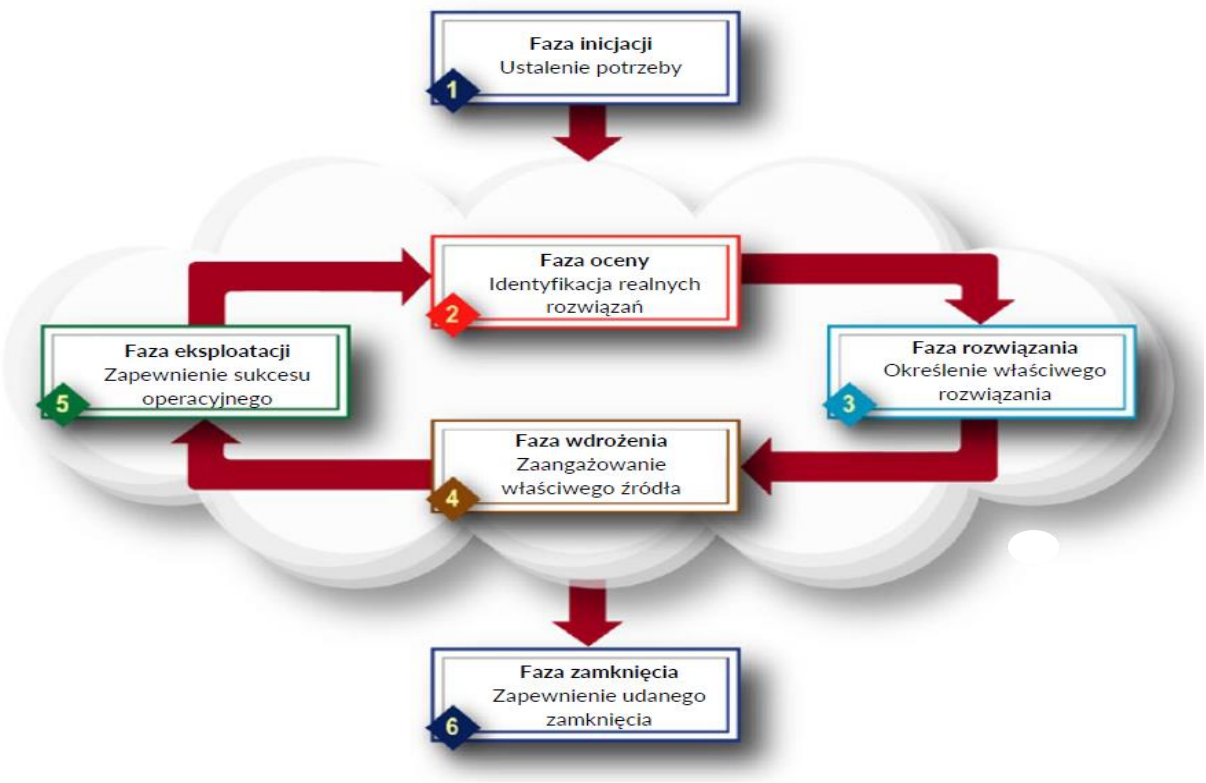
- CIO,
- osoba ds. zakupów,
- przedstawiciel techniczny ds. zakupów,
- komisja oceny inwestycji informacyjnych lub jej odpowiednik,
- menadżer programu bezpieczeństwa,
- ISSO,
- menadżer programu (właściciel danych)/osoba inicjująca zakup,
- inspektor ochrony danych.

12.1. CYKL ŻYCIA USŁUG BEZPIECZEŃSTWA INFORMACJI

Cykl życia usług bezpieczeństwa stwarza ramy, które pomagają osobom podejmującym decyzje dotyczące bezpieczeństwa w organizowaniu i koordynowaniu ich wysiłków—począwszy od inicjacji aż po zakończenie.

[85] Podano jako przykład w celach uzupełniających dla zainteresowanych.

Na rys. 12-1 przedstawiono cykl życia usług bezpieczeństwa w kontekście pozyskiwania usług ogólnych. Tabela 12-1 zawiera krótkie podsumowanie każdej fazy.



Rysunek 12-1. Cykl życia usług bezpieczeństwa informacji

Tabela 12-1. Cykl życia usług bezpieczeństwa informacji

Faza	Działanie
Faza 1 - Inicjacja	• Kiedy zostaje dostrzeżona potrzeba zainicjowania cyklu życia usługi. • Składają się na nią ustalenie potrzeb, kategoryzacja bezpieczeństwa oraz wstępne oszacowanie ryzyka.
Faza 2 - Ocena	• Obejmuje opracowanie dokładnego obrazu aktualnego środowiska zanim decydenci wdrożą usługę i ustanowią dostawcę usług. • Ustala stan bazowy istniejącego środowiska; stworzenie, zgromadzenie i analiza metryk; całkowity koszt własności. • Analiza możliwości i barier. • Identyfikacja opcji i ryzyka.

Faza	Działanie
Faza 3 - Rozwiązanie	• Decydenci wybierają odpowiednie rozwiązanie spośród realnych opcji zidentyfikowanych w fazie oceny. • Opracowanie uzasadnienia biznesowego. • Opracowanie uzgodnień w sprawie usługi. • Opracowanie planu wdrożenia.
Faza 4 - Wdrożenie	• W tej fazie wdrażani są dostawcy usług. • Identyfikacja dostawcy usług i opracowanie umowy na świadczenie usług. • Finalizacja i realizacja planu wdrożenia. • Zarządzanie oczekiwaniami.
Faza 5 - Użytkowanie	• Cykl życia usługi staje się powtarzalny; usługa zaczyna funkcjonować, świadczona usługa jest w pełni zainstalowana i należy prowadzić stałą ocenę poziomu usługi i wyników działania źródła. • Monitorowanie i pomiar wyników działania organizacji. • Ocena i rozwój.
Faza 6 – Zamknięcie/wycofanie z eksploatacji	• Choć jest to mało prawdopodobne z powodu powtarzalnego charakteru cyklu życia, usługa i dostawca usług mogą działać bezterminowo. • Bardziej prawdopodobne jest to, że w środowisku wystąpią takie zmiany, że menadżerowie programu bezpieczeństwa informacji zidentyfikują warunki, które zainicjują świadczenie nowej usługi bezpieczeństwa zastępującej dotychczasową. • Wybór odpowiedniej strategii wyjściowej. • Wdrożenie wybranej strategii wyjściowej.

12.2. WYBÓR USŁUG BEZPIECZEŃSTWA INFORMACJI

Przed wyborem konkretnych usług organizacje powinny dokonać przeglądu stanu swoich programów bezpieczeństwa oraz planowanych lub wdrożonych zabezpieczeń mających chronić systemy informacyjne i dane. Organizacje powinny użyć procesu zarządzania ryzykiem do zidentyfikowania skutecznego połączenia zabezpieczeń zarządczych, operacyjnych i technicznych, które złagodzą ryzyko do akceptowalnego

poziomu. Liczba i rodzaj odpowiednich zabezpieczeń oraz związane z nimi usługi bezpieczeństwa informacji mogą się różnić na przestrzeni całego cyklu życia usług danego systemu. Na to jakie rodzaje zabezpieczeń są odpowiednie dla konkretnego systemu wpływ może mieć względna dojrzałość architektury bezpieczeństwa wdrożonej w danej organizacji. Kombinacja zabezpieczeń jest powiązana z misją organizacji i rolą systemu w jej obrębie w kontekście wsparcia realizacji tej misji. Bardziej szczegółowe spojrzenie na różne rodzaje zabezpieczeń przedstawiono w publikacji NSC 800-53. W tabeli 12-2 podano kategorie usług bezpieczeństwa informacji.

Tabela 12-2. Kategorie usług bezpieczeństwa informacji

Kategorie	Opis
Usługi zarządcze	Techniki i sprawy, którymi w programie bezpieczeństwa komputerowego danej organizacji zazwyczaj zajmuje się kierownictwo. Skupiają się one na zarządzaniu programem bezpieczeństwa komputerowego i ryzyku występującym w obrębie organizacji.
Usługi operacyjne	Usługi skoncentrowane na zabezpieczeniach wdrożonych i wykonywanych przez ludzi (w przeciwieństwie do systemów). Często wymagają wiedzy specjalistycznej lub technicznej i polegają na działaniach kierownictwa i zabezpieczeniach.
Usługi techniczne	Usługi techniczne skupiają się na zabezpieczeniach wykonywanych przez system komputerowy. Ich skuteczność zależy od odpowiedniego działania systemu.

Wybór najbardziej odpowiednich usług oraz kombinacji i poziomu usług to złożona decyzja, podobnie jak decyzja o wyborze dostawcy usług. Istnieje szeroki wachlarz możliwych uzgodnień w zakresie świadczenia usługi. Organizacja może zdecydować, że wymagana usługa będzie świadczona przez jej wewnętrznych pracowników i zespoły albo zlecić jej świadczenie dostawcy usług zewnętrznemu. Usługodawcą tym może być organizacja, w tym grupa zewnętrzna z podległej organizacji, jednostka biznesowa lub dostawca usług komercyjny.

12.2.1. WYBÓR NARZĘDZI ZARZĄDZANIA USŁUGAMI BEZPIECZEŃSTWA INFORMACJI

Ze względu na potencjalne szkody spowodowane niedostatecznym bezpieczeństwem, menadżerowie programu bezpieczeństwa informacji oraz decydenci muszą stosować skuteczne narzędzia zarządcze, aby zwiększyć prawdopodobieństwo sukcesu nabytej usługi bezpieczeństwa. Dwoma ważnymi narzędziami są metryki i umowy o świadczenie usług, które można wykorzystać do uczynienia usługodawców odpowiedzialnymi za wyniki otrzymywane z usług, jakie świadczą organizacji.

- Metryki to narzędzie zarządcze, które ułatwia podejmowanie decyzji i rozliczalność za sprawą zbierania praktycznych i istotnych danych, analizy danych oraz sprawozdawczości w zakresie wyników działania.
- Umowa o świadczenie usług to umowa zawierana między usługodawcą i organizacją chcącą korzystać z usługi, która określa jakie usługi ma świadczyć dostawca usług, w jakim zakresie, przez jaki czas itp.

12.2.2. KWESTIE ZWIĄZANE Z USŁUGAMI BEZPIECZEŃSTWA INFORMACJI

Wdrożenie usługi bezpieczeństwa i związanych z nią uzgodnień może być złożoną sprawą. Każda usługa bezpieczeństwa charakteryzuje się właściwymi sobie kosztami i powiązanym ryzykiem, podobnie jak każde uzgodnienie w sprawie usług. Podjęcie decyzji na podstawie jednej kwestii może mieć dla organizacji duże implikacje w innych obszarach. Na przykład, jeżeli okaże się, że zewnętrzny dostawca usług może świadczyć daną usługę w sposób bardziej opłacalny niż aktualny dostawca usług wewnętrzny, osoby podejmujące decyzje związane z bezpieczeństwem będą musiały rozważyć implikacje dla obecnego personelu organizacji. Decydenci będą musieli zrównoważyć krótkoterminowe koszty/wartość z potencjalnym długoterminowym ryzykiem związanym z ewentualnym spadkiem morale pracowników, wyczerpaniem zasobów i kapitałem intelektualnym. W tabeli 12-3 przedstawiono listę ogólnych czynników i kwestii związanych z nabywaniem usług bezpieczeństwa w rozbiciu na sześć kategorii. Lista nie jest zamknięta - zawiera najpowszechniejsze, ale nie wszystkie, czynniki i kwestie.

Tabela 12-3. Kategorie kwestii związanych z usługami bezpieczeństwa informacji

Kategorie	Kwestie
Strategiczne/Związane z misją	Chociaż bezpieczeństwo w ogóle, a bezpieczeństwo informacji w szczególe jest bardzo ważne, to musi ono stanowić wsparcie dla misji lub funkcji biznesowej. Rozważając implikacje każdej decyzji, decydenci muszą zadać sobie pytanie o to, co jest dla organizacji najlepsze ze strategicznego punktu widzenia i co najlepiej pomoże w realizacji jej misji.
Budżetowe/ związane z finansowaniem	Chociaż kwestia finansowania leży w centrum każdej decyzji biznesowej, koszt to tylko jeden z wielu czynników. Należy skoncentrować się na wartości i kosztach pełnego cyklu życia.
Techniczne/ związane z architekturą	Usługi IT, w tym usługi zarządcze z implikacjami technicznymi. W odniesieniu do całego cyklu życia, menadżerowie programu bezpieczeństwa informacji muszą rozważyć, czy ich decyzje mają techniczny i architektoniczny wpływ na organizację.
Organizacyjne	Takie kwestie jak uszczerbek dla wizerunku i reputacji organizacji, przesunięcie skupienia w obrębie głównych kompetencji czy odporność organizacji są niematerialnymi elementami organizacji. W wielu przypadkach, zatrudnienie podmiotu świadczącego usługi bezpieczeństwa informacji może wymusić zrewidowanie długo akceptowanych, wewnętrznych zabezpieczeń i praktyk biznesowych wynikających z wymagań regulacyjnych i naturalnych podziałów między jednostkami biznesowymi.
Personel	Kwestie związane z wykonawcami i pracownikami organizacji. Kierownictwo musi być świadomie wpływu swoich decyzji na podległych pracowników. W zależności od wdrożonych uzgodnień dotyczących usługi mogą zaistnieć poważne negatywne konsekwencje dla obecnych pracowników. Zrozumienie tych potencjalnych implikacji oraz zajęcie się nimi na wczesnym etapie zapewni, że pracownicy pozostaną ważnym zasobem organizacji.
Polityka/Proces	Skuteczne bezpieczeństwo zaczyna się od silnej polityki. Implikacje dla polityki i procesu należy brać pod uwagę, aby zapewnić odpowiednie transformacje i wdrożenia.

12.2.3. OGÓLNE ROZWAŻANIA DOTYCZĄCE USŁUG BEZPIECZEŃSTWA INFORMACJI

Aby zidentyfikować dostawcę usług, który najlepiej spełnia potrzeby organizacji, decydenci muszą znaleźć odpowiedzi na wiele pytań. W szczególności, zależnie od charakteru danych, do jakich dostawca usług ma dostęp i jakie przetwarza w imieniu organizacji, dostawca usług może podlegać wymaganiom legislacyjnym i regulacyjnym oraz stosować normy, standardy i wytyczne, np. NSC SP 800-53, NSC 80-37 i inne. Pytania dotyczące tych wymagań powinny stać się częścią standardowego procesu stosowanego przez organizację do poszukiwania i oceny usług i usługodawców z obszaru bezpieczeństwa informacji. W tabeli 12-4 przedstawiono reprezentatywne przykłady takich pytań w podziale na sześć kategorii.

Pytania mają charakter wskazówek, a każda organizacja musi sama zdecydować, które z nich są istotne dla jej konkretnych potrzeb. Poniższa lista nie jest zamknięta – organizacje powinny opracować dodatkowe pytania. Wreszcie, na pytanie najlepiej może odpowiedzieć organizacja, a nie dostawca usług.

Tabela 12-4. Ogólne rozważania dotyczące usług bezpieczeństwa informacji

Kategoria	Rozważania
Strategiczne/Związane z misją	1. Jaka jest misja <*dostawcy usług*>[86]? 2. Czy <*dostawca usług*> rozumie misję organizacji? 3. Jak misja i oferta <*dostawcy usług*> jest zgodna i zwiększa zdolność organizacji do realizacji naszej misji? 4. Opisz działalność prowadzoną przez <*dostawcę usług*>, podając liczbę pracowników, klientów i strukturę oraz wysokość przychodów. Czy <*dostawca usług*> planuje duże zmiany strategii/misji lub przewiduje problemy z budżetem/opłacalnością w czasie świadczenia usługi? 5. Czy <*usługa*> jest z założenia usługą świadczoną dla podmiotów publicznych?

[86] Słowo lub wyrażenie umieszczone między „< >” wskazuje, że między nawiasy należy wstawić informację, której dotyczy pytanie.

Kategoria	Rozważania
Budżetowe/ związane z finansowaniem	1. Jaki będzie koszt świadczenia usługi przez <*dostawcę usług*>? 2. Ile usługa kosztowałaby na wyższym poziomie usługowym? Ile na niższym poziomie usługowym? 3. Jak <*dostawca usług*> będzie chronić przed przekroczeniem kosztów? 4. Jakie środki naprawcze <*dostawca usług*> mógłby zaproponować w przypadku przekroczenia kosztów?
Techniczne/związane z architekturą	1. Jak <*dostawca usług*> będzie realizować usługę bezpieczeństwa informacji? 2. Kto zapewni, tj. będzie właścicielem, potrzebny sprzęt/oprogramowanie?? 3. Na jakim poziomie <*dostawca usług*> będzie świadczyć usługę (np. procent dostępności, sprawozdania z metryk, utrzymanie, odświeżenie sprzętu/oprogramowania)? 4. W jaki sposób <*dostawca usług*> zapewni ten poziom usługi? 5. Jakie środki naprawcze <*dostawca usług*> uznaje za odpowiednie w przypadku niespełnienia celów usługowych (np. darmowe usługi)? 6. Jakie są wymagania <*dostawcy usług*> w zakresie wcześniejszego rozwiązania/przedłużenia umowy? 7. W jaki sposób są rozwiązywane kwestie zwiększenia/zmniejszenia zakresu usług? 8. Czy <*dostawca usług*> świadczył już wcześniej tego typu usługę takiej organizacji na tym poziomie? Czy <*dostawca usług*> może przedstawić stosowne referencje? 9. Jakie jest środowisko bezpieczeństwa informacji <*dostawcy usług*>? 10. W jaki sposób <*dostawca usług*> obsługiwałby sytuacje awaryjne?

Kategoria	Rozważania
Organizacyjne	1. Jakie jest środowisko pracy <*dostawcy usług*> i czy jest ono kompatybilne z organizacją? 2. W jakim stopniu <*dostawca usług*> zaadaptuje się do środowiska organizacji? 3. Jaka jest reputacja <*dostawcy usług*> na rynku i w zakresie realizacji celów dotyczących kosztów i usług? Jak <*dostawca usług*> prezentuje się na tle konkurentów?
Personel	1. Czy personel <*dostawcy usług*> będzie przebywać na terenie organizacji, poza nim, czy oba przypadki? 2. Czy personel <*dostawcy usług*> będzie musiał/mógł uzyskać odpowiednie poświadczenia bezpieczeństwa osobowego/obiektowego? 3. Jaki personel <*dostawca usług*> przydzieli do realizacji tego zadania? Jakie umiejętności posiada ten personel? 4. W jaki sposób <*dostawca usług*> zapewni, aby personel był na bieżąco z technologią/obszarem usług?
Polityka/Proces	1. Czy <*dostawca usług*> przewiduje zmiany w zasadach i/lub procesach organizacji? 2. Na ile polityki bezpieczeństwa <*dostawcy usług*> (np. w zakresie planowania awaryjnego) różnią się od zasad organizacji? Jeżeli polityki organizacji spełniają wyższe standardy, czy <*dostawca usług*> będzie miał problem ze spełnieniem tego wyższego standardu? Jeżeli tak, to czy <*dostawca usług*> będzie przestrzegać surowszych zasad organizacji? 3. Jak <*dostawca usług*> rozwiązuje problem wspólnego korzystania z jego danych z danymi innej organizacji? Czy wdrożono procedury zapewniające ochronę danych organizacji?

12.3. WYBÓR PRODUKTÓW BEZPIECZEŃSTWA INFORMACJI

Podobnie jak w przypadku usług bezpieczeństwa, przed wyborem konkretnych produktów organizacje powinny dokonać przeglądu stanu swoich programów bezpieczeństwa oraz planowanych lub wdrożonych zabezpieczeń mających chronić informacje i systemy informacyjne. W tabeli 12-5 przedstawiono ogólne kwestie do rozważenia przed wyborem produktów bezpieczeństwa informacji.

Tabela 12-5. Kwestie do rozważenia podczas wybierania produktów bezpieczeństwa informacji

Rodzaj kwestii	Kwestie
Organizacyjne	• Identyfikacja społeczności użytkowników. • Określenie związku między produktem bezpieczeństwa i misją organizacji. • Zidentyfikowanie wrażliwości danych. • Zidentyfikowanie wymagań organizacji w zakresie bezpieczeństwa. • Wykonanie przeglądu planu bezpieczeństwa. • Wykonanie przeglądu polityk i procedur. • Zidentyfikowanie kwestii operacyjnych, takich jak codzienne operacje, utrzymanie i szkolenia.
Produkt	• Ustalenie całkowitego kosztu cyklu życia (łącznie z nabyciem i transportem). • Ocena łatwości użycia. • Ocena skalowalności. • Zidentyfikowanie wymagań dotyczących interoperacyjności. • Zidentyfikowanie wymagań dotyczących testów. • Wykonanie przeglądu znanych podatności. • Przetestowanie i wdrożenie istotnych poprawek. • Wykonanie przeglądu specyfikacji na tle istniejących i planowanych programów, zasad, procedur i standardów organizacji. • Zidentyfikowanie związanych z bezpieczeństwem zależności z innymi produktami. • Zbadanie interakcji nowego produktu z istniejącą infrastrukturą.

Rodzaj kwestii	Kwestie
Sprzedawca	• Ustalenie czy wybór konkretnego produktu ograniczy przyszłe możliwości wyboru w obszarze bezpieczeństwa. • Ocena doświadczenia i rentowności sprzedającego. • Zbadanie historii sprzedającego w zakresie reagowania na wady zabezpieczeń jego produktów.

Aby ułatwić identyfikację i przegląd powyższych kwestii, podczas rozważania wyboru produktów bezpieczeństwa informacji menadżer programu bezpieczeństwa może skorzystać z zestawu pytań. Tabela 12-6 zawiera listę pytań niezależnych od produktu, które powinny zostać postawione w fazie wyboru produktu. Pytania pogrupowano w trzech kategoriach dotyczących odpowiednio organizacji, produktu i dostawcy. Należy jednak zauważyć, że poniższa lista nie jest zamknięta, ani też nie dotyczy wszystkich możliwych okoliczności. Pytania mają charakter wskazówek, a organizacje powinny je dopracowywać i uzupełniać w zależności od wymagań stawianych przez konkretną sytuację, zapewniając przy tym, aby podejmowane przez nie decyzje były zgodne z ich architekturą i ustalonym uzasadnieniem biznesowym.

Tabela 12-6. Pytania dotyczące wyboru produktu bezpieczeństwa informacji

Rodzaj kwestii	Pytania	Uwagi
Organizacyjne	• Czy zidentyfikowano przewidywaną grupę użytkowników?	
Organizacyjne	• Jaka liczba i rodzaj użytkowników będzie korzystać z produktu bezpieczeństwa według przewidywań organizacji?	
Organizacyjne	• Czy związek między tym produktem bezpieczeństwa i realizacją misji organizacji jest zrozumiały i udokumentowany?	

Rodzaj kwestii	Pytania	Uwagi
Organizacyjne	• Czy ustalono wrażliwość danych, które organizacja zamierza chronić?	W przypadku modułów kryptograficznych, dla których organizacje ustaliły potrzebę ochrony informacji środkami kryptograficznymi, możliwy jest wybór wyłącznie produktów zgodnych z programem walidacji modułów kryptograficznych (*ang. cryptographic module validation program - CMVP*).
Organizacyjne	• Czy wymagania organizacji w zakresie bezpieczeństwa są wsparte planem, politykami i procedurami bezpieczeństwa?	
Organizacyjne	• Czy określono wymagania bezpieczeństwa i porównano je ze specyfikacją produktu?	
Organizacyjne	• Czy w odniesieniu do wybieranego produktu użyto w umowie odpowiednich zwrotów językowych?	
Organizacyjne	• Czy rozważono kwestie operacyjne, takie jak codzienne operacje, utrzymanie, planowanie awaryjne, uświadamianie i szkolenia czy dokumentacja?	
Organizacyjne	• Czy opracowano zasady zamówienia i użycia ocenianych produktów?	Organizacje powinny rozważyć nabycie i wdrożenie produktów bezpieczeństwa informacji, które zostały ocenione i przetestowane przez niezależne akredytowane laboratoria pod kątem odpowiednich specyfikacji i wymagań bezpieczeństwa. Przykładem takich specyfikacji są pliki ochrony oparte na ISO/IEC 15408, Wspólne kryteria

Rodzaj kwestii	Pytania	Uwagi
		oceny zabezpieczeń IT . Organizacje powinny jednakże uwzględniać własne ogólne wymagania i wybierać produkty zgodnie z nimi.
Organizacyjne	• Czy wymagana jest komunikacja poza granicę domeny (implikuje to potrzebę zastosowania kontrolera granicy, np. podsystemu zapory sieciowej, systemu wykrywania włamań i/lub ruterów)?	
Organizacyjne	• Czy zidentyfikowano komponenty systemowe (sprzęt komputerowy lub oprogramowanie) wymagane w przypadku zidentyfikowanego produktu?	
Organizacyjne	• Czy produkt bezpieczeństwa jest zgodny z wymaganiami w zakresie bezpieczeństwa fizycznego i innymi wymaganiami dotyczącymi zasad?	
Organizacyjne	• Czy rozważono wpływ na korporacyjne środowisko operacyjne, w którym ten produkt będzie działać?	
Organizacyjne	• Czy rozważono wpływ nowych technologii na produkt?	
Organizacyjne	• Czy produkt jest niezbędny do mitygacji ryzyka?	Wybierając produkty IT, organizacje muszą rozważyć środowisko zagrożenia i funkcje bezpieczeństwa potrzebne do opłacalnego ograniczenia ryzyka do akceptowalnego poziomu.

Rodzaj kwestii	Pytania	Uwagi
Organizacyjne	• Czy zidentyfikowany produkt wymaga komponentów systemowych (sprzętu komputerowego lub oprogramowania)?	
Organizacyjne	• Czy w przeglądach bezpieczeństwa uwzględniono wymagania w zakresie wsparcia, komponentów typu plug-in czy oprogramowania pośredniczącego (*ang. middleware*)?	
Produkt	• Czy ustalono wsparcie w całym cyklu życia, łatwość użycia, skalowalność i interoperacyjność?	Całkowity cykl życia obejmuje okres „od kołyski aż po grób", a zatem dotyczą go również wymagania w zakresie usunięcia produktu bezpieczeństwa.
Produkt	• Czy opracowano wymagania dotyczące testów akceptacyjnych i integracyjnych oraz zarządzania konfiguracją?	Jeżeli produkt został poddany ocenie zgodnie z programem oceny i walidacji wspólnych kryteriów National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme (NIAP-CCEVS), można skorzystać ze sprawozdań z testów już wykonanych w ramach niezależnego procesu oceny i uniknąć dublowania testów walidacyjnych.
Produkt	• Czy dokonano przeglądu produktu pod kątem występowania znanych podatności?	Znane podatności wielu produktów można odszukać w bazie danych NIST National Vulnerability Database (NVD) http://nvd.nist.gov (poprzednia nazwa: I-CAT).
Produkt	• Czy przetestowano i wdrożono wszystkie istotne poprawki?	

Rodzaj kwestii	Pytania	Uwagi
Produkt	• Czy dokonano przeglądu dostępnych plików ochrony zgodnych ze wspólnymi kryteriami (http://www.commoncriteria.org/protection profiles/pp.html) w celu zidentyfikowania profili ochrony wyrażających wymagania bezpieczeństwa dotyczące potrzeb organizacji w przewidywanym środowisku zagrożenia?	Jeżeli istniejące profile ochrony są nieadekwatne, należy rozważyć przydatność podobnych profili jako punktu wyjściowego do badania produktu, który może spełniać wymagania dotyczące nowego środowiska.
Produkt	• Czy dokonano przeglądu scentralizowanego wykazu certyfikowanych produktów Common Criteria - CC (*ang. CC Centralized Certified Product List*)?	Przeglądu scentralizowanego wykazu certyfikowanych produktów CC należy dokonywać w celu zapewnienia, że w stosownych przypadkach wykorzystywane będą produkty poddane ocenie. Produkty poddane niezależnym testom i ocenie (lub wzajemnie uznawane) zgodnie z NIAP-CCEVS dają pewien poziom pewności, że funkcje bezpieczeństwa produktu działają zgodnie ze specyfikacją. Zasadniczo testy i oceny wykonane przez podmioty trzecie mogą stanowić znacznie mocniejszą podstawę dla zaufania klienta niż w przypadku produktów nieocenionych. Należy jednak zauważyć, że nabycie ocenionego produkty tylko dlatego, że został oceniony, ale bez należytego uwzględnienia rzetelności dostawcy ani stosownych wymagań dotyczących funkcjonalności i wiarygodności może nie być ani przydatne, ani opłacalne. Organizacje powinny wziąć pod uwagę własne ogólne wymagania i wybrać produkt zgodnie z nimi.

Rodzaj kwestii	Pytania	Uwagi
Produkt	• Czy dokonano przeglądu wykazów produktów zgodnych ze standardem FIPS 140-2?[87]	Przeglądu wykazów produktów zgodnych ze standardem FIPS 140-2 należy dokonywać w celu zapewnienia, że w stosownych przypadkach wykorzystywane będą produkty poddane ocenie.
Produkt	• Czy rozważono politykę lub postępowanie dostawcy w zakresie ponownej walidacji produktów w przypadku pojawienia się nowych wydań?	
Produkt	• Czy dokonano przeglądu specyfikacji produktu pod kątem istniejących i planowanych programów, polityk, procedur i standardów organizacji?	Przykłady to: polityka organizacji w zakresie Internetu, polityka i program w zakresie infrastruktury klucza publicznego, program kart inteligentnych oraz polityka łączenia i zatwierdzania sieci.
Produkt	• Czy w produkcie występują zależności od innych produktów związane z bezpieczeństwem?	Na przykład, system operacyjny lub moduł kryptograficzny.
Produkt	• Czy połączenie nowego produktu z istniejącą infrastrukturą wprowadzi nowe podatności lub współzależności?	
Produkt	• Z jaką częstością występują awarie produktu i jaka jest adekwatność działań naprawczych?	
Dostawca	• Czy wybór konkretnego produktu ograniczy przyszły wybór innych modyfikacji lub udoskonaleń komputerowych lub operacyjnych?	Uwaga: utrudnieniem w oszacowaniu wpływu na przyszłą infrastrukturę bezpieczeństwa organizacji może być tempo zmian technologicznych.

[87] Podano jako przykład dla zainteresowanych.

Rodzaj kwestii	Pytania	Uwagi
Sprzedawca	• Czy dostawca ma doświadczenie w wytwarzaniu wysokiej jakości produktów bezpieczeństwa informacji?	
Sprzedawca	• Jakie są „osiągnięcia" dostawcy dotyczące reagowania na błędy bezpieczeństwa jego produktów?	
Sprzedawca	• W jaki sposób sprzedawca realizuje utrzymanie oprogramowania i sprzętu komputerowego, wsparcie użytkowników końcowych i umowy serwisowe?	
Sprzedawca	• Jaka jest długoterminowa rentowność sprzedawcy?	
Sprzedawca	• Czy sprzedawca opracował instrukcję konfiguracji bezpieczeństwa?	
Sprzedawca	• Czy sprzedawca posiada powiązaną instrukcję bezpieczeństwa dotyczącą produktu?	
Sprzedawca	• Czy sprzedawca stosuje lub odnosi się do list kontrolnych, konfiguracji/ustawień bezpieczeństwa lub wzorców oraz innych tego typu materiałów wypracowanych w drodze konsensusu?	

Przykładowe rodzaje produktów to: kontrola dostępu, wykrywanie włamań i inne produkty związane z bezpieczeństwem informacji. Przed podjęciem decyzji o zakupie dowolnego rodzaju produktu bezpieczeństwa, decydenci powinni rozważyć m.in. jego zdolności, kompatybilność z innymi produktami oraz kwestie środowiskowe.

12.4. LISTY KONTROLE BEZPIECZEŃSTWA DOTYCZĄCE PRODUKTÓW IT

Niemal codziennie ujawniane są podatności produktów IT, a w Internecie dostępnych jest wiele gotowych sposób ich wykorzystania. Ponieważ produkty IT są często przeznaczone dla szerokiej grupy różnorodnych użytkowników, zazwyczaj nie mają domyślnie włączonych restrykcyjnych zabezpieczeń. Dlatego wiele z nich jest podatnych na ataki od razu po uruchomieniu. W celu podniesienia poziomu wiedzy menadżerowie programów bezpieczeństwa mogą zapoznać się z publikacją NIST SP 800-70, *Security Configuration Checklists Program for IT Products*, która pomaga w sprawnym opracowaniu i rozpowszechnieniu list kontrolnych bezpieczeństwa, co umożliwia organizacjom i użytkownikom indywidualnym lepsze zabezpieczenie ich produktów. Lista kontrolna bezpieczeństwa (nazywania niekiedy instrukcją blokady lub utwardzenia albo benchmarkiem) to w najprostszej swojej formie szereg instrukcji dotyczących konfiguracji produktu odpowiadającej określonym warunkom pracy.

12.5. KONFLIKT INTERESÓW W ORGANIZACJI

Organizacyjny konflikt interesów (*ang. Organizational Conflict of Interest - OCI*) może wystąpić, kiedy strona umowy ma przeszły, obecny lub przyszły interes dotyczący pracy, która została lub ma zostać wykonana, który to interes może zmniejszyć zdolność do świadczenia technicznie prawidłowej i obiektywnej obsługi albo może skutkować powstaniem nieuczciwej przewagi konkurencyjnej. Organizacje powinny uczynić co w ich mocy, aby unikać organizacyjnego konfliktu interesów zanim jeszcze powstanie. Jeżeli jednak organizacja stwierdzi wystąpienie OCI, którego nie można uniknąć, ale mimo to chce procedować dalej, to jej kierownictwo musi formalnie uchylić ten OCI.

Identyfikowanie istnienia OCI, mitygacja ich wpływu do akceptowalnego poziomu lub uchylanie to ważne działania, które należy uwzględniać podczas zarządzania cyklem życia usługi bezpieczeństwa informacji. Jednakże każde z tych działań jest złożoną sprawą, w której obecne są kwestie prawne i regulacyjne, i jako takie wymaga konsultacji z radcą lub działem prawnym organizacji.

REFERENCJE:

National Institute of Standards and Technology Special Publication 800-35, *Guide to Information Technology Security Services*, October 2003.

National Institute of Standards and Technology Special Publication 800-36, *Guide to Selecting Information Technology Security Products*, October 2003.

National Institute of Standards and Technology Special Publication 800-53, *Revision 1*, *Recommended Security Controls for Federal Information Systems*, February 2006.

National Institute of Standards and Technology Special Publication 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003.

National Institute of Standards and Technology Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle*, Rev. 1, June 2004.

National Institute of Standards and Technology Special Publication 800-70, *Security Configuration Checklists Program for IT Products - Guidance for Checklists Users and Developers*, May 2005.

National Institute of Standards and Technology ITL Bulletin: *Selecting Information Technology Security Products*, April 2004

National Institute of Standards and Technology ITL Bulletin: *Information Technology Security Services; How to Select, Implement, and Manage*, June 2004.

ROZDZIAŁ 13

13. REAGOWANIE NA INCYDENTY

Ataki na systemy i sieci informacyjne stały się w ostatnich latach liczniejsze, bardziej wyrafinowane i poważniejsze. Chociaż zapobieganie takim atakom byłoby dla organizacji idealnym tokiem działania, to nie wszystkim incydentom bezpieczeństwa informacyjnego można zapobiec. Każda informacja, która w realizacji misji jest uzależniona od systemów i sieci informacyjnych powinna zidentyfikować i oszacować ryzyko dla swoich systemów i informacji oraz obniżyć je do akceptowalnego poziomu[88]. Ważnym komponentem tego procesu zarządzania ryzykiem jest analiza trendów w przeszłych incydentach bezpieczeństwa informacyjnego i identyfikacja skutecznych sposobów radzenia sobie z nimi. Dobrze zdefiniowana zdolność reagowania na incydenty pomaga organizacji szybko wykrywać incydenty, minimalizować straty i zniszczenia, identyfikować słabości oraz niezwłocznie przywracać operacje informatyczne.

Opracowanie i wdrożenie procedur wykrywania, zgłaszania i reagowania na incydenty bezpieczeństwa wymagane jest przez ustawę o krajowym systemie cyberbezpieczeństwa[89]. Dodatkowo, zaleca, aby organizacje identyfikowały w swoich sprawozdaniach wszelkie incydenty (fizyczne i elektroniczne) polegające na utracie lub nieautoryzowanym dostępie do danych osobowych oraz zgłaszały je zgodnie z obowiązującymi przepisami prawa. Organizacje muszą stworzyć, zapewnić i obsługiwać formalną zdolność reagowania na incydenty. Aktualne przepisy prawa nakładają obowiązek zgłaszania incydentów przez podmioty krajowego systemu cyberbezpieczeństwa do jednego z trzech zespołów CSIRT poziomu krajowego - Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (*ang. Computer Security Incident Response Teams – CSIRT*)[90].

---

88 Dodatkowe wytyczne w zakresie klasyfikacji systemów i szacowania ryzyka, zob. NSC 199, NSC 800-30, a także Rozdział 10 „Zarządzanie ryzykiem" i Rozdział 11 „Certyfikacja, akredytacja i oceny bezpieczeństwa" niniejszego podręcznika.

89 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2022 r. poz. 1863 z późn. zm.).

90 Patrz: NSC 800-61.

Publikacja NSC *SP 800-61*, szczegółowo przedstawia składający się z czterech faz proces reagowania na incydenty. Główne fazy procesu reagowania na incydenty: przygotowanie, wykrywanie i analiza, powstrzymanie/zwalczenie/odtworzenie oraz aktywność po incydencie zostały szczegółowo opisane w pozostałej części niniejszego rozdziału. Rysunek 13-1 przedstawia cykl życia reagowania na incydenty.

Rysunek 13-1. Cykl życia reagowania na incydenty

13.1. PRZYGOTOWANIE

Przygotowanie do obsługi incydentów polega nie tylko na ustanowieniu zdolności reagowania na incydenty, aby organizacja była gotowa do reagowania na incydenty, ale także zapobieganie incydentom poprzez zapewnienie, że systemy, sieci i aplikacje są wystarczająco bezpieczne. Zapobieganie incydentom jest obecnie uważane za fundamentalny komponent programów reagowania na incydenty, które nazywane są również programami zarządzania incydentami, mimo że zazwyczaj nie należy to do obowiązków zespołu reagowania na incydenty. Specjalistyczna wiedza posiadana przez ten zespół powinna zostać w jak największym stopniu wykorzystana do ustanowienia zaleceń w zakresie zabezpieczania systemów i zapobiegania incydentom. W tym rozdziale przedstawiono przegląd działań potrzebnych do zapobiegania incydentom i postępowania z nimi, w tym przygotowanie do zbierania danych o incydentach.

13.1.1. PRZYGOTOWANIE DO REAGOWANIA NA INCYDENTY

W zorganizowaniu skutecznej zdolności reagowania na incydenty uczestniczy wiele osób z danej organizacji. Kluczowe dla ustanowienia udanego programu reagowania na incydenty jest podejmowanie prawidłowych decyzji w zakresie planowania i wdrażania. Jednym z pierwszych zadań dotyczących planowania powinno być opracowanie

właściwej dla danej organizacji definicji „incydentu", wyraźnie określającej zakres tego terminu. Dodatkowe zadania, które powinny zostać wykonane podczas fazy przygotowania są następujące:

- **Stworzenie polityki reagowania na incydenty.** Zasady te powinny definiować, jakie zdarzenia są uznawane za incydenty, ustanawiać strukturę organizacyjną reagowania na incydenty, określać role i obowiązki oraz podawać obowiązujące w organizacji wymagania dotyczące zgłaszania incydentów.
- **Opracowanie procedur reagowania na incydenty i zgłaszania incydentów.** Standardowe procedury operacyjne (*ang. Standard Operating Procedures - SOP*), oparte na polityce reagowania na incydenty, nakreślają konkretne procesy techniczne, techniki, listy kontrolne i formularze używane przez zespół reagowania na incydenty. SOP powinny być kompleksowe i szczegółowe, aby zapewnić odzwierciedlenie priorytetów organizacji w operacjach reagowania na incydenty. Ponadto przestrzeganie ustandaryzowanych procedur reagowania jest też skutecznym sposobem minimalizowania błędów, szczególnie tych, które mogą być spowodowane tempem obsługi incydentu i związanym z tym stresem. Przed wdrożeniem standardowych procedur operacyjnych w zakresie reagowania na incydenty, organizacja powinna je przetestować w celu zweryfikowania ich dokładności i przydatności. Po walidacji, SOP należy rozesłać do wszystkich komórek w obrębie całej organizacji. Ponieważ incydenty mogą wystąpić na niezliczone i niemożliwe do przewidzenia sposoby, opracowanie kompleksowych procedur zawierających szczegółowe instrukcje postępowania w przypadku każdego incydentu jest niewykonalne. Najlepszym, co organizacja może zrobić, jest przygotowanie się do obsługi dowolnego typu incydentu, a w szczególności tych najczęstszych.
- **Ustanowienie wytycznych w zakresie komunikowania się z podmiotami zewnętrznymi.** Podczas procesu reagowania na incydent, organizacja być może będzie musiała komunikować się z podmiotami zewnętrznymi, w tym innymi zespołami reagowania na incydenty, organami ścigania, mediami, dostawcami i poszkodowanymi spoza organizacji. Ponieważ taka komunikacja często musi

przebiegać szybko i sprawnie, organizacje powinny posiadać z góry określone wytyczne dotyczące komunikacji, tak aby tylko odpowiednie informacje były udostępniane właściwym podmiotom. Niewłaściwe ujawnienie wrażliwych informacji może prowadzić do większych zakłóceń i strat finansowych niż sam incydent. Stworzenie i utrzymywanie listy wewnętrznych i zewnętrznych punktów kontaktowych (*ang. Point of Contact - POC*) wraz z kontaktami zapasowymi powinno pomóc w ułatwieniu i przyspieszeniu komunikacji.

- **Określenie usług świadczonych przez zespół reagowania na incydenty.** Chociaż głównym zadaniem zespołu reagowania na incydenty jest reakcja na incydenty, większość zespołów świadczy dodatkowe usługi. Przykładowe rodzaje usług, jakie zespół reagowania na incydenty może oferować organizacji to: dystrybucja porad, ocena podatności, wykrywanie naruszeń oraz edukacja i uświadamianie.
- **Wybór struktury zespołu i modelu obsady personelem.** Organizacja powinna wybrać model struktury i obsady zespołu personelem, który najlepiej odpowiada jej potrzebom. Rozważając wybór najlepszego modelu struktury zespołu i jego obsady personelem, organizacja powinna wziąć pod uwagę szereg czynników, takich jak rozmiar organizacji, zróżnicowanie geograficzne głównych zasobów obliczeniowych, potrzeba dostępności przez całą dobę siedem dni w tygodniu, koszt czy posiadana przez personel specjalistyczna wiedza.
- **Obsadzenie personelem i przeszkolenie zespołu reagowania na incydenty.** Członkowie zespołu reagowania na incydenty powinni posiadać doskonałe umiejętności techniczne i umiejętności rozwiązywania problemów, ponieważ mają one krytyczne znaczenie dla sukcesu zespołu. Ważne są również doskonałe predyspozycje pracy w zespole oraz umiejętności w zakresie organizacji, komunikacji i wysławiania się. Większość zespołów reagowania na incydenty zazwyczaj ma kierownika i zastępcę kierownika zespołu, który przejmuje zarządzanie pod nieobecność kierownika zespołu. Dodatkowo, niektóre zespoły mają również kierownika technicznego, który przejmuje nadzór i ostateczną odpowiedzialność za jakość pracy technicznej zespołu. Ponadto, większe zespoły

często wyznaczają kierownika incydentu jako główny POC do obsługi konkretnego incydentu.

Złożoność incydentów wielkoskalowych sprawia, że utrzymanie świadomości sytuacyjnej w zakresie postępowania z takimi incydentami zazwyczaj stanowi wyzwanie dla organizacji. Rolę w reagowaniu na incydenty może odgrywać wiele osób, a organizacje mogą stawać przed koniecznością szybkiego i skutecznego komunikowania się z różnymi grupami zewnętrznymi. Zbieranie, organizowanie i analizowanie wszystkich informacji tak, aby można było podejmować i realizować właściwe decyzje nie należy do łatwych zadań. Kluczem do utrzymania świadomości sytuacyjnej jest skrupulatne przygotowanie do postępowania z incydentami wielkoskalowymi. Dwa szczególne działania będące wsparciem w tym zakresie to:

- **Ustanowienie i utrzymanie dokładnych mechanizmów zawiadamiania.** Organizacje powinny ustanowić, udokumentować, utrzymywać i realizować mechanizmy kontaktu i zawiadamiania różnych osób i grup w godzinach i po godzinach pracy w obrębie organizacji (np. CIO, szef bezpieczeństwa informacji, wsparcie IT, planowanie ciągłości działalności) oraz poza nią (np. organizacje zajmujące się reagowaniem na incydenty, odpowiednicy w innych organizacjach).
- **Opracowanie pisemnych wytycznych dotyczących nadawania priorytetów incydentom.** Zespoły reagowania na incydenty powinny postępować z każdym incydentem zgodnie z priorytetem nadanym mu na podstawie krytycznego charakteru zasobów, których dotyczy zdarzenie, a także w oparciu o aktualny i potencjalny skutek incydentu. Na przykład, zniszczenie danych w stacji roboczej użytkownika może skutkować niewielką utratą produktywności, podczas gdy wynikiem kompromitacji konta administratora (*ang. Root Compromise*) publicznego serwera WWW może być duża utrata przychodów, produktywności, dostępu do usług oraz reputacji, a także ujawnienie wrażliwych danych (np. numerów kart kredytowych, haseł dostępowych, itp.).
- Personel reagujący na incydenty zazwyczaj pracuje w stresujących warunkach, które sprzyjają błędom ludzkim. Ważne jest, aby wyraźnie zdefiniować

i wyartykułować proces nadawania priorytetu obsługi incydentów. Proces ustalania priorytetu obsługi incydentów powinien obejmować opisanie sposobu, w jaki zespół reagowania na incydenty powinien postępować w różnych okolicznościach oraz zawarcie umowy gwarancji świadczenia usługi (*ang. Service-Level Agreement - SLA*) dokumentującej odpowiednie działania i maksymalne czasy reakcji. Takie nadawanie priorytetu ułatwi podejmowanie szybszych i spójniejszych decyzji.

13.1.2. PRZYGOTOWANIE DO ZBIERANIA DANYCH O INCYDENTACH

Organizacje powinny być przygotowane do zebrania zestawu obiektywnych i subiektywnych danych o każdym incydencie. Z biegiem czasu dane o incydentach zebrane przez organizację mogą być wykorzystane na kilka sposobów. Na przykład, dane na temat łącznej liczby godzin poświęconych przez zespół na działania związane z reagowaniem na incydenty oraz kosztów tych działań w określonym przedziale czasu mogą posłużyć do uzasadnienia dodatkowego finansowania zespołu reagowania na incydenty. Badanie charakterystyki incydentów może ujawnić systemowe słabości i zagrożenia, zmiany trendów albo inne dane, które można wykorzystać do wsparcia procesu szacowania ryzyka. Innym zastosowaniem danych jest mierzenie sukcesu zespołu reagowania na incydenty. Jeżeli dane o incydentach są prawidłowo gromadzone i przechowywane, powinny zapewnić kilka miar sukcesu (lub przynajmniej działań) zespołu reagowania na incydenty. Ponadto organizacje, które są zobowiązane do zgłaszania informacji o incydentach, będą musiały zebrać niezbędne dane, aby wypełnić swoje obowiązki (np. w zakresie sprawozdań zawierających statystyki incydentów)[91].

W procesie przygotowania do zbierania danych o incydentach organizacje powinny skupić się na gromadzeniu danych, które są przydatne, a nie tylko dlatego, że są dostępne. Liczby bezwzględne nie mają charakteru informacyjnego - ważne jest zrozumienie, w jaki sposób reprezentują one zagrożenia i podatności dotyczące procesów biznesowych organizacji. Organizacje powinny zdecydować, jakie dane

[91] Dodatkowe wskazówki w zakresie zbierania i raportowania danych o incydentach, zob. Rozdział 7 „Miary wyników" niniejszego podręcznika.

o incydentach należy gromadzić w oparciu o wymagania sprawozdawcze i oczekiwany zwrot z inwestycji z tych danych (np. identyfikacja nowego zagrożenia i postępowanie z powiązanymi z nim podatnościami, zanim będzie można te podatności wykorzystać).

13.1.3. ZAPOBIEGANIE INCYDENTOM

Zapobieganie problemom jest zazwyczaj tańsze i skuteczniejsze niż reagowanie na nie po ich wystąpieniu. Dlatego zapobieganie incydentom jest ważnym uzupełnieniem zdolności reagowania na incydenty. Jeżeli zabezpieczenia są niewystarczające, może dojść do dużej liczby incydentów i przeciążenia zasobów i zdolności do reagowania, co może prowadzić do opóźnionego lub niepełnego odtworzenia, a być może rozleglejszych szkód i dłuższych okresów niedostępność usług. Obsługa incydentów może być skuteczniejsza, jeśli organizacje uzupełniają swoje zdolności reagowania na incydenty odpowiednimi zasobami, aby aktywnie utrzymywać bezpieczeństwo sieci, systemów i aplikacji. Ten proces ma na celu ograniczenie częstości występowania incydentów, przez co pozwala zespołowi reagowania na incydenty skupić się na incydentach.

Przykłady praktyk pomagających zapobiegać incydentom to:

- Posiadanie programu zarządzania poprawkami pomagającego administratorom systemu w identyfikowaniu, nabywaniu, testowaniu i stosowaniu poprawek eliminujących znane podatności systemów i aplikacji.
- Odpowiednie skonfigurowanie (*ang. hardening*) wszystkich hostów w celu wyeliminowania podatności i słabości konfiguracji.
- Takie skonfigurowanie obwodu sieci, aby odrzucać wszelkie działania, które nie są w sposób wyraźny dozwolone.
- Wprowadzenie w całej organizacji oprogramowania wykrywającego i zatrzymującego złośliwy kod.
- Uświadomienie użytkowników w zakresie zasad i procedur dotyczących odpowiedniego użytkowania sieci, systemów i aplikacji.

13.2. WYKRYWANIE I ANALIZA

Wykrywanie i analiza to dla wielu organizacji najtrudniejszy aspekt procesu reagowania na incydenty. Innymi słowy, chodzi tu o precyzyjne wykrywanie i ocenę ewentualnych incydentów - ustalanie czy zdarzenie miało miejsce, a jeśli tak, to jakiego rodzaju, w jakim zakresie i jakiej skali. Incydenty można wykrywać na wiele różnych sposobów, z różnym poziomem szczegółowości i wiarygodności. Funkcje automatycznego wykrywania obejmują systemy wykrywania włamań (*ang. Intrusion Detection System - IDS*) oparte na sieciach i hostach, oprogramowanie antywirusowe i analizatory dzienników. Incydenty można również wykrywać ręcznie, na przykład dzięki zgłoszeniom użytkowników. Niektóre incydenty mają widoczne oznaki, które można łatwo wykryć, natomiast inne są niemal niemożliwe do wykrycia bez zastosowania automatyzacji.

W typowej organizacji, oprogramowanie zabezpieczające komputery każdego dnia rejestruje tysiące lub miliony możliwych oznak incydentów. Do przeprowadzenia wstępnej analizy danych i wybrania zdarzeń, które są przedmiotem weryfikacji przez człowieka potrzebna jest automatyzacja. Oprogramowanie do korelacji zdarzeń oraz scentralizowane rejestrowanie mogą mieć wielką wartość w automatyzacji procesu analizy. Jednak skuteczność procesu zależy od jakości danych, które do niego trafiają. Organizacje powinny ustanowić standardy i procedury rejestrowania, aby zapewnić gromadzenie odpowiednich informacji przez dzienniki i oprogramowanie zabezpieczające oraz regularne przeglądanie danych. Prawidłowe i skuteczne przeglądy danych związanych ze zdarzeniami wymagają rozległej, specjalistycznej wiedzy technicznej i doświadczenia.

W przypadku zidentyfikowania ewentualnego incydentu, zespół reagowania na incydenty powinien działać szybko i sprawnie, aby go przeanalizować i zweryfikować, dokumentując każdą podjętą czynność. Zespół powinien szybko przeprowadzić wstępną analizę, aby ustalić zakres incydentu, metody ataku i atakowane podatności. Analiza powinna dostarczyć zespołowi wystarczających informacji do ustalenia priorytetów dalszych działań, w tym powstrzymania incydentu. Personel zajmujący się incydentem powinien zakładać najgorsze, aż do chwili, gdy dodatkowe analizy nie

wskażą, że jest inaczej. Oprócz wytycznych w zakresie ustalania priorytetów, organizacje powinny również ustanowić proces eskalacji dla przypadków, w których zespół nie reaguje na incydent w wyznaczonym czasie.

Zespół reagowania na incydenty powinien przechowywać dokumentację dotyczącą statusu incydentów, wraz z innymi stosownymi informacjami. Korzystanie z aplikacji lub bazy danych jest konieczne do zapewnienia obsługi i rozwiązywania incydentów w odpowiednim czasie. Zespół reagowania na incydenty powinien chronić te oraz inne dane związane z incydentami, ponieważ często zawierają one wrażliwe informacje na temat najnowszych naruszeń bezpieczeństwa, wykorzystanych podatności oraz użytkowników, którzy mogli wykonać niewłaściwe działania.

13.3. POWSTRZYMYWANIE, ZWALCZANIE I ODTWARZANIE

Incydent należy powstrzymać zanim się rozprzestrzeni, aby uniknąć przeciążenia zasobów i zwiększenia rozmiarów spowodowanych przez niego szkód. Ponieważ większość incydentów wymaga powstrzymania, ważne jest, aby wziąć to pod uwagę na wczesnym etapie postępowania z każdym incydentem. Istotną częścią powstrzymywania jest podejmowanie decyzji, np. dotyczących zamknięcia systemu, odłączenia go od sieci czy wyłączenia niektórych funkcji. Takie decyzje znacznie łatwiej podjąć, jeżeli istnieją z góry określone strategie i procedury powstrzymania incydentu. Organizacje powinny zdefiniować akceptowalne ryzyko w postępowaniu z incydentami i odpowiednio opracować strategie.

Strategie powstrzymywania różnią się w zależności od rodzaju incydentu. Na przykład, strategia powstrzymania infekcji wirusem przenoszonym przez pocztę e-mail różni się znacznie od strategii dotyczącej sieciowego ataku DDoS. Organizacje powinny stworzyć oddzielne strategie powstrzymywania dla każdego typu incydentu. Kryteria wyboru odpowiedniej strategii powinny zostać jasno udokumentowane, aby ułatwić szybkie i skuteczne podejmowanie decyzji. Przykłady takich kryteriów: potencjalne uszkodzenie i kradzież zasobów, potrzeba zabezpieczenia dowodów, skuteczność strategii, czas i zasoby potrzebne do wdrożenia strategii, czas trwania rozwiązania.

Po powstrzymaniu incydentu, konieczne może być jego zwalczenie, czyli wyeliminowanie elementów incydentu, np. usunięcie złośliwego kodu i wyłączenie

naruszonych kont użytkowników. W przypadku niektórych incydentów, zwalczenie albo nie jest konieczne, albo przeprowadzane jest w fazie odtwarzania. Podczas odtwarzania administratorzy przywracają systemy do normalnego działania oraz (w stosownych przypadkach)" utwardzają" systemy, aby zapobiec podobnym incydentom. Odtwarzanie może obejmować takie działania, jak:

- przywracanie systemów z czystych kopii zapasowych,
- odbudowywanie systemów od podstaw,
- zastępowanie zainfekowanych plików czystymi wersjami,
- instalowanie poprawek,
- zmiana haseł,
- uszczelnienie zabezpieczenia obwodu sieci (np. reguły zapór sieciowych).

W ramach procesu odtwarzania często pożądane jest zastosowanie wyższych poziomów rejestracji zdarzeń systemowych lub monitorowania sieci. Raz pomyślnie zaatakowany zasób jest często atakowany ponownie lub w podobny sposób są atakowane inne zasoby w organizacji.

13.4. AKTYWNOŚĆ PO INCYDENCIE

Po opanowaniu incydentu, organizacja powinna zorganizować spotkanie, na którym przedstawione zostaną wnioski, mające na celu dokonanie przeglądu skuteczności procesu postępowania z incydentem i zidentyfikowanie niezbędnych ulepszeń istniejących zabezpieczeń i praktyk bezpieczeństwa. Spotkania tego typu powinny być też organizowane okresowo w przypadku incydentów mniejszej wagi. Informacje zebrane ze wszystkich spotkań na temat zdobytego doświadczenia, a także dane zgromadzone podczas obsługi każdego incydentu, powinny zostać wykorzystane do zidentyfikowania systemowych słabości w zakresie bezpieczeństwa oraz braków w zakresie zasad i procedur. Raporty uzupełniające generowane dla każdego rozwiązanego incydentu, mogą być ważne dla celów dowodowych, użyte jako odniesienie w obsłudze przyszłych incydentów oraz wykorzystane w szkoleniu nowych członków zespołu reagowania na incydenty. Kolejnym cennym źródłem informacji dla

personelu zajmującego się obsługą incydentów może być baza danych zawierająca szczegółowe informacje o każdym zaistniałym incydencie.

REFERENCJE:

Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

National Institute of Standards and Technology Special Publication 800-61, *Computer Security Incident Handling Guide*, January 2003.

ROZDZIAŁ 14

14. ZARZĄDZANIE KONFIGURACJĄ

Celem zarządzania konfiguracją (*ang. Configuration Management - CM*) jest zarządzanie skutkami zmian lub różnic w konfiguracjach systemu lub sieci informacyjnej. Zarządzanie konfiguracją pomaga w usprawnieniu procesów zarządzania zmianami i zapobiega pojawianiu się zmian, które mogłyby mieć szkodliwy wpływ na stan bezpieczeństwa systemu. Jako taki, proces zarządzania konfiguracją obniża ryzyko, że wprowadzone do systemu zmiany (wstawienia/instalacje, usunięcia/deinstalacje i modyfikacje) spowodują kompromitację systemu lub naruszenie poufności, integralności lub dostępności danych poprzez stworzenie powtarzalnego mechanizmu wprowadzania modyfikacji w kontrolowanym środowisku. Zgodnie z procesem zarządzania konfiguracją, zmiany systemu muszą zostać przetestowane przed ich wdrożeniem, aby zaobserwować ich skutki, a przez to zminimalizować ryzyko negatywnych rezultatów.

Każda organizacja musi uwzględnić koszty i wydatki, wymagane planowanie i układanie harmonogramów oraz niezbędne szkolenia związane ze drobiazgowym i skutecznym procesem zarządzania konfiguracją. Jednakże, ponieważ każde ogólne podejście do zarządzania konfiguracją jest uniwersalne, organizacje mogą skonstruować i wdrożyć powtarzalny proces zarządzania konfiguracją, aby zaoszczędzić na zasobach przy okazji przyszłych projektów. Dodatkowo, zarządzanie konfiguracją pomaga wyeliminować ryzyko zamieszania, problemów i zbędnych wydatków. Dodatkowe zasoby wymagane do naprawienia problemu, któremu można było zapobiec, gdyby stosowano dobre praktyki zarządzania konfiguracją, prawdopodobnie znacznie przewyższają wielkości zasobów wymaganych do opracowania i wdrożenia skutecznego procesu CM na poziomie organizacji.

Według NIST SP 800-64, „procedury zarządzania konfiguracją i jej kontroli są kluczowe dla ustanowienia początkowego bazowego poziomu komponentów sprzętu komputerowego, oprogramowania i oprogramowania sprzętowego dla danego systemu informacyjnego, a następnie do kontrolowania i utrzymania dokładnego wykazu wszystkich zmian w systemie. Zmiany dotyczące sprzętu komputerowego, oprogramowania lub

oprogramowania sprzętowego mogą mieć znaczący wpływ na bezpieczeństwo systemu (...) zmiany powinny być dokumentowane, a ich ewentualny wpływ na bezpieczeństwo regularnie oceniany". W dokumencie NSC 800-53, zdefiniowano zabezpieczenia z zakresu zarządzania konfiguracją, które organizacje mają obowiązek wdrożyć w oparciu o kategoryzację bezpieczeństwa systemu informacyjnego. Wymagane zabezpieczenia zarządzania konfiguracją określono w Tabeli 14-1[92].

Tabela 14-1. Kategorie zabezpieczeń CM wg NIST SP 800-53

Identyfikator	Tytuł	Zabezpieczenie
CM-1	Polityka i procedury zarządzania konfiguracją	Organizacja opracowuje, rozpowszechnia i dokonuje okresowych przeglądów/aktualizacji: (1) formalnej, udokumentowanej polityki CM, która adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami; (2) formalnych, udokumentowanych procedur ułatwiających realizację polityki w zakresie zarządzania konfiguracją oraz powiązanych ocen w zakresie zarządzania konfiguracją.
CM-2	Konfiguracja bazowa	Organizacja opracowuje, dokumentuje i utrzymuje bieżącą konfigurację bazową systemu informatycznego oraz zasobu komponentów systemu.

[92] Uzupełniające rekomendacje i zabezpieczenia rozszerzone związane z wdrażaniem tych środków bezpieczeństwa, zob. NSC SP 800-53.

Identyfikator	Tytuł	Zabezpieczenie
CM-3	Zabezpieczanie zmian konfiguracji	Organizacja dokumentuje i kontroluje zmiany w systemie informacyjnym. Odpowiednia osoba z organizacji zatwierdza zmiany w systemie informacyjnym zgodnie z obowiązującymi w organizacji zasadami i procedurami.
CM-4	Analiza wpływu	Organizacja monitoruje zmiany w systemie informacyjnym i przeprowadza analizy wpływu na bezpieczeństwo w celu ustalenia skutków tych zmian.
CM-5	Ograniczenie możliwości dokonywania zmian	Organizacja definiuje, dokumentuje, zatwierdza i egzekwuje fizyczne i logiczne ograniczenia dostępu związane ze zmianami w systemie informacyjnym.
CM-6	Ustawienia konfiguracji	Organizacja konfiguruje ustawienia bezpieczeństwa produktów informacyjnych, które odzwierciedlają najbardziej restrykcyjny tryb zgodny z wymogami operacyjnymi systemu informatycznego.
CM-7	Zasada minimalnej funkcjonalności	Organizacja konfiguruje system informacyjny tak, aby zapewniał tylko niezbędne zdolności i wyraźnie zabrania i/lub ogranicza użycie następujących funkcji, portów, protokołów i/lub usług. Systemy informacyjne mogą zapewniać szeroki zakres funkcji i usług. Niektóre z domyślnie dostarczanych funkcji i usług mogą nie być konieczne do wspierania istotnych operacji (np. kluczowych misji, funkcji). Funkcje i usługi dostarczane przez systemy informacyjne

Identyfikator	Tytuł	Zabezpieczenie
		powinny zostać poddane starannemu przeglądowi w celu ustalenia, które z nich są kwalifikują się do usunięcia (np. protokół transmisji pakietowej, klienci komunikatorów internetowych, protokół przesyłania plików, protokół przesyłania dokumentów hipertekstowych, wymiana plików).

14.1. ZARZĄDZANIE KONFIGURACJĄ W CYKLU ŻYCIA SYSTEMU

Chociaż nie jest tradycyjnie uznawane za funkcję bezpieczeństwa, zarządzanie konfiguracją musi zostać włączone do cyklu życia systemu[93] ze względu na silne implikacje dla bezpieczeństwa. Zarządzanie konfiguracją to tylko jeden z komponentów stanu bezpieczeństwa systemu informacyjnego. Wchodzi ono w zakres zabezpieczeń operacyjnych systemu informacyjnego i jest wzajemnie powiązane z licznymi innymi dziedzinami bezpieczeństwa, takimi jak zarządzanie projektami, zarządzanie ryzykiem, certyfikacja i akredytacja bezpieczeństwa[94] oraz uświadamianie i szkolenia w zakresie bezpieczeństwa[95].

Zarządzanie konfiguracją powinno być realizowane przez cały cykl życia danego projektu lub zadania. Jak wspomniano wyżej, udane zrealizowanie projektu rozwoju systemu lub zarządzania systemem bez prawidłowego i skutecznego procesu zarządzania konfiguracją jest niemal niemożliwe. W cyklu życia systemu, planowanie procesu zarządzania konfiguracją przypada w Fazach 2 i 3, a główna jego realizacja

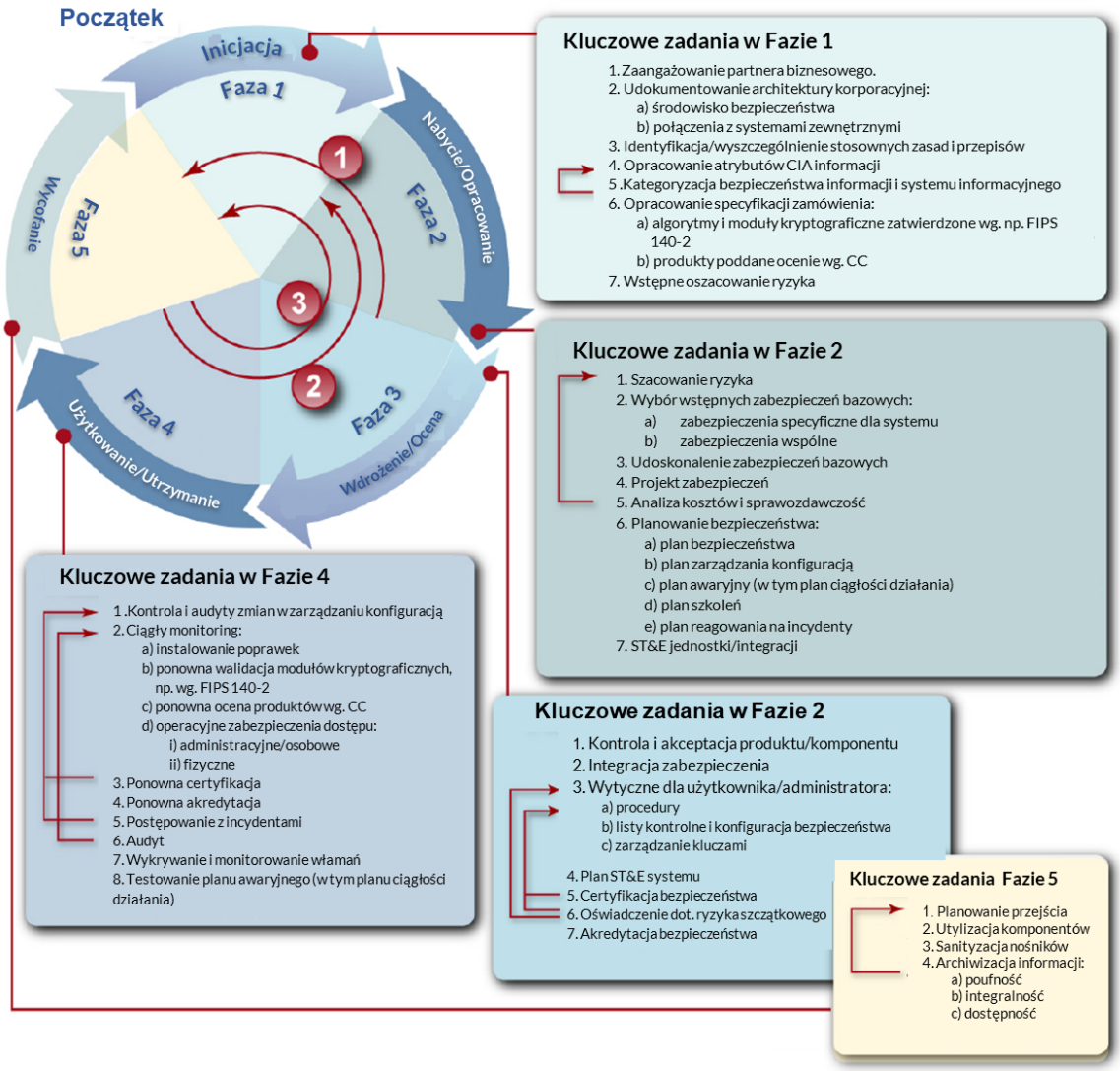
---

93 Dodatkowe informacje na temat cyklu życia systemu, zob. NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*, a także Rozdział 3 „Cykl życia systemu" niniejszego podręcznika.

94 Dodatkowe wytyczne w zakresie certyfikacji i akredytacji, zob. NSC 800-37, a także Rozdział 11 „Certyfikacja, akredytacja i oceny bezpieczeństwa" niniejszego podręcznika.

95 Dodatkowe wytyczne dotyczące świadomości i szkoleń w zakresie bezpieczeństwa, zob. NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*; NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, a także Rozdział 4 „Uświadamianie i szkolenia" niniejszego podręcznika.

przypada w Fazie 4 - Eksploatacja/Utrzymanie. Cykl życia systemu i powiązane kluczowe zadania przedstawiono na rys. 14-1.



Rysunek 14-1. Cykl życia systemu

W Fazie 2 Nabycie/Opracowanie, proces zarządzania ryzykiem zaczyna się od wstępnego oszacowania ryzyka. Dokument NSC 800-30 definiuje zarządzanie ryzykiem jako „proces pozwalający osobom zarządzającym technologią informatyczną zrównoważenie operacyjnych i ekonomicznych kosztów środków bezpieczeństwa oraz osiągnięcie korzyści w zakresie zdolności do realizacji misji swojej organizacji poprzesz ochronę

systemów informacyjnych i danych, które te misje wspierają”[96].Zarządzanie ryzykiem obejmuje proces identyfikacji, analizy i reagowania na ryzyko. Polega on na identyfikacji podatności istniejących w systemie lub jego odpowiednich komponentach. Ponieważ ryzyko to częstokroć niepewność wystąpienia danego zdarzenia, należy wdrożyć wykonalny plan na wypadek wykorzystania potencjalnego ryzyka. Identyfikacja ryzyka polega na ustaleniu ewentualnego działania danego ryzyka na system. Podczas tej fazy, w oparciu o oszacowanie poziomu ryzyka w sieci, dobierane są zabezpieczenia bazowe. Po ustanowieniu zabezpieczeń może się rozpocząć proces zarządzania konfiguracją. Udokumentowany proces zarządzania konfiguracją powinien zawierać procedury i techniki dokonywania w systemie zmian bez wywierania na niego szkodliwego wpływu, zmieniania dowolnych systemów połączonych lub zmieniania sieci przy uwzględnieniu ustanowionego poziomu bezpieczeństwa sieci.

W Fazie 3 (Wdrożenie/Ocena) zostają przetestowane zabezpieczenia wybrane w Fazie 2. Ma tu również miejsce proces certyfikacji i akredytacji. Dokument NSC 800-37, definiuje akredytację bezpieczeństwa jako „oficjalną decyzję zarządczą wydaną przez osobę upoważnioną w celu zezwolenia na funkcjonowanie systemu informacyjnego i wyraźnego zaakceptowania ryzyko dla operacji organizacji, aktywów organizacji lub osób fizycznych, w oparciu o wdrożenie uzgodnionego zestawu środków bezpieczeństwa.” W ramach procesu certyfikacji i akredytacji można wyróżnić cztery fazy (inicjacja, certyfikacja bezpieczeństwa, akredytacja bezpieczeństwa i ciągły monitoring). Czwarta faza, czyli ciągłe monitorowanie, dotyczy głównie zarządzania konfiguracją. „W odniesieniu do zarządzania i kontroli nad konfiguracją, ważne jest udokumentowanie proponowanych lub faktycznych zmian w systemie informacyjnym, a następnie ustalenie ich wpływu na bezpieczeństwo systemu. (…) Udokumentowanie zmian w systemie informacyjnym i oszacowanie ewentualnego wpływu jaki mogą one mieć na bezpieczeństwo systemu to niezbędny aspekt ciągłego monitorowania i utrzymania akredytacji bezpieczeństwa”[97].

---

[96] Dodatkowe wytyczne w zakresie zarządzania ryzykiem, zob. Rozdział 10 „Zarządzanie ryzykiem” niniejszego podręcznika.

[97] Patrz: NSC 800-37.

W Fazie 4 (Eksploatacja/Utrzymanie) ma miejsce kontrola i audyt zmian w ramach zarządzania konfiguracją. Jeżeli w procesie zarządzania konfiguracją zrealizowano znaczącą zmianę, to system należy poddać ponownej certyfikacji i akredytacji. Stałe monitorowanie systemu ma na celu identyfikację ewentualnego ryzyka dla systemu tak, aby można się było nim zająć w ramach procesów zarządzania ryzykiem, certyfikacji i akredytacji oraz zarządzania konfiguracją.

14.2. ROLE I OBOWIĄZKI DOTYCZĄCE ZARZĄDZANIA KONFIGURACJĄ

Z realizacją skutecznego procesu zarządzania konfiguracją związanych jest wiele ról. Należy zauważyć, że jedna osoba fizyczna nie jest ograniczona tylko do jednej roli (np. możliwe jest bycie właścicielem systemu i jednocześnie osobą zarządzającą procesem CM[98]). Organizacja musi zapewnić, aby jej kierownictwo było świadome proponowanych zmian i zweryfikowało fakt wdrożenia drobiazgowego procesu przeglądu i zatwierdzenia. Dodatkowo, należy uwzględnić rozdzielenie obowiązków, aby zapewnić wdrożenie zmian wyłącznie po ich przetestowaniu i zatwierdzeniu. Poniżej podano przykłady ról i obowiązków w przykładowym procesie zarządzania konfiguracją[99]:

- **CIO** (*ang. Chief Information Officer*)**.** Kluczowa osoba w jednostce organizacyjnej odpowiedzialna za technologie informacyjne odpowiada za określenie zasad zarządzania konfiguracją i wdrożenie CM na najwyższym poziomie organizacji.
- **Właściciel systemu.** Właściciel systemu występuje jako organ zwierzchni we wszystkich sprawach dotyczących zarządzania konfiguracją w systemie. Właściciel systemu odpowiada za opracowanie wymagań funkcjonalnych i zweryfikowanie ich odpowiedniego wdrażania.
- **ISSO** (*ang. Information Systems Security Officer*)**.** Osoba w organizacji, której przypisano odpowiedzialność za zapewnienie utrzymania odpowiedniego poziomu bezpieczeństwa operacyjnego dla systemu informacyjnego odpowiada

98 Zarządzanie konfiguracją (ang. configuration management – CM).

99 Dodatkowe wytyczne w zakresie ról i obowiązków, zob. Rozdział 2 „Zarządzanie”, Rozdział 5 „Planowanie finansowe”, Rozdział 8 „Planowanie bezpieczeństwa” i Rozdział 11 „Certyfikacja, akredytacja i oceny bezpieczeństwa” niniejszego podręcznika.

głównie za odnoszenie się do kwestii bezpieczeństwa związanych z programem CM i za dostarczanie specjalistycznej wiedzy i wsparcia decyzyjnego komisji oceny kontroli konfiguracji (*ang. Configuration Control Review Board - CCRB*).

- **CCRB.** Do obowiązków CCRB w zakresie CM należy:
  - ✓ Omawianie i rozpatrywanie wniosków o zmiany, których wdrożenie wymaga dodatkowych funduszy i środków.
  - ✓ Zapewnienie, aby wnioski o zmiany nie miały negatywnego wpływu na żadne systemy lub usługi związane z przedmiotowym systemem lub powiązanymi z nim systemami, podsystemami i obiektami oraz
  - ✓ Ocenę informacji z metryki CM dotyczących finansowania i innych kwestii związanych z CM.

Osoba zarządzająca CM. Osoba zarządzająca CM odpowiada za codzienne działania, w tym:

- ✓ Dokumentowanie i wdrażanie planu CM.
- ✓ Ustanowienie systemowych zabezpieczeń bazowych i oceniania zabezpieczeń.
- ✓ Zapewnienie, aby proponowane zmiany nie wpływały negatywnie na system lub dane organizacji.
- ✓ Zarządzanie wnioskami o zmiany i koordynowanie wdrażania zmian.
- ✓ Przeprowadzanie analizy wpływu zmian.
- ✓ Zatwierdzanie, odrzucanie lub odraczanie zmian.
- ✓ Zawiadamianie użytkowników o zmianach w systemie.
- ✓ Zapewnienie istnienia procesu przechowywania, odnajdywania i dystrybucji materiałów CM oraz
- ✓ Zapewnienie udokumentowania i utrzymania ścieżki audytu.

- **Użytkownicy systemu.** Użytkownicy systemu odpowiadają za zgłaszanie wszelkich słabości lub nowych wymagań identyfikowanych w bieżących wersjach oprogramowania.
- **Deweloperzy.** Deweloperzy odpowiadają za koordynację i współpracę z osobą zarządzającą CM w zakresie identyfikowania, rozstrzygania i wdrażania zabezpieczeń i innych kwestii CM.

14.3. PROCES ZARZĄDZANIA KONFIGURACJĄ

W procesie zarządzania konfiguracją wyróżnia się kroki wymagane dla zapewnienia właściwego wnioskowania, oceniania i autoryzowania wszystkich zmian. Proces zarządzania konfiguracją dostarcza również szczegółowej procedury, która krok po kroku opisuje identyfikowanie, przetwarzanie, śledzenie i dokumentowanie zmian. Przykładowy proces zarządzania konfiguracją przedstawiono na rys. 14-2.

Rysunek 14-2. Proces zarządzania konfiguracją

Krok 1: Identyfikacja zmiany

Pierwszy krok procesu CM zaczyna się od osoby lub procesu związanego z systemem informacyjnym, który identyfikuje potrzebę zmiany. Zmiana może zostać zainicjowana przez wiele osób fizycznych lub właścicieli systemów, albo też osoby te mogą zostać określone w ustaleniach z audytu lub innych przeglądów. Zmiana może polegać na aktualizacji pól lub rekordów bazy danych aż po modernizację systemu operacyjnego z najnowszymi poprawkami. Po zidentyfikowaniu potrzeby zmiany, wniosek o nią należy złożyć do odpowiedniego organu decyzyjnego.

Krok 2: Ocena wniosku o zmianę

Po zainicjowaniu wniosku o zmianę należy dokonać oceny skutków, jakie może ona mieć dla systemu lub innych systemów powiązanych. Analiza wpływu zmiany musi zostać przeprowadzona zgodnie z poniższymi wskazówkami:

- Czy zmiana jest opłacalna i poprawia działanie lub bezpieczeństwo systemu?
- Czy zmiana jest technicznie prawidłowa, konieczna i wykonalna w ramach ograniczeń systemu?
- Czy zmiana będzie miała wpływ na bezpieczeństwo systemu?
- Czy uwzględniono koszty związane z wdrożeniem zmiany? oraz
- Czy zmiana ma wpływ na komponenty bezpieczeństwa?

Krok 3: Decyzja o realizacji

Po tym jak zmiana została oceniona i przetestowana, należy podjąć jedną z następujących decyzji:

- **Zatwierdzenie.** Realizacja zmiany zostaje autoryzowana i może nastąpić w dowolnym momencie po złożeniu odpowiedniego podpisu autoryzującego.
- **Odrzucenie.** Natychmiastowe odrzucenie wniosku niezależnie od okoliczności i dostarczonych informacji.
- **Odroczenie.** Natychmiastowa decyzja o odroczeniu aż do kolejnego zawiadomienia. W tej sytuacji, przed wydaniem ostatecznej decyzji potrzebne może być wykonanie dodatkowych testów lub analiz.

Krok 4: Realizacja zatwierdzonego wniosku o zmianę

Po podjęciu decyzji o wdrożeniu, zmianę należy przenieść ze środowiska testowego do produkcyjnego. Jeżeli jest to wymagane, aktualizacja środowiska produkcyjnego powinna zostać wykonana przez inne osoby niż te, które opracowały zmiany, co da większą pewność, że niezatwierdzone zmiany nie zostaną wdrożone do produkcji.

Krok 5: Ciągłe monitorowanie

Proces zarządzania konfiguracją wymaga ciągłego monitorowania, aby zapewnić, że działa zgodnie z zamierzeniami oraz że wprowadzone zmiany nie mają negatywnego wpływu na jego funkcjonowanie ani stan bezpieczeństwa. Organizacje mogą realizować cele ciągłego monitorowania poprzez przeprowadzanie testów weryfikujących konfigurację, aby zapewnić, że wybrana konfiguracja danego systemu nie została zmieniona poza ustanowionym procesem CM. Oprócz testów weryfikujących

konfigurację, organizacje mogą przeprowadzać również audyty systemu. Zarówno testy weryfikujące konfigurację, jak i audyty systemu polegają na zbadaniu cech systemu i dokumentacji pomocniczej w celu zweryfikowania, czy konfiguracja spełnia potrzeby użytkowników oraz czy obecna konfiguracja jest zatwierdzoną bazową konfiguracją systemu.

W ramach ogólnego procesu CM, organizacje powinny w tym kroku realizować również działania z zakresu zarządzania poprawkami. Zarządzanie poprawkami wspomaga proces obniżania potencjalnego ryzyka dla sieci poprzez „łatanie" lub naprawianie znanych podatności w dowolnym środowisku sieci lub systemu. Dostawcy są coraz bardziej aktywni w opracowywaniu i udostępnianiu publiczności poprawek (lub antidotów) dla znanych podatności, a organizacje muszą zachować czujność, aby zapewnić, że wychwycą wszystkie stosowne poprawki w momencie ich wydania, przetestują ich realizację pod kątem negatywnych skutków i wdrożą je, jeżeli zostanie to uznane za właściwe po zakończeniu testów. Wprowadzanie poprawek jest związane z Fazą 4 cyklu życia, a także Fazami 2 i 3. W Fazie 2, zarządzanie poprawkami jest związane z zarządzaniem ryzykiem i ma zapobiegać wykorzystaniu i skompromitowaniu wszelkich podatności. Faza 3 obejmuje testowanie w celu zapewnienia, aby żadna zmiana (w tym polegająca na poprawce) nie miała negatywnego wpływu na system.

REFERENCJE:

National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

National Institute of Standards and Technology Special Publication 800-53, *Revision 1*, *Recommended Security Controls for Federal Information Systems*, February 2006.

National Institute of Standards and Technology Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle*, October 2003.

ZAŁĄCZNIK A AKRONIMY

Akronim	Terminologia angielska	Terminologia polska
BIA	*Business Impact Analysis*	Analiza wpływu na działalność
BLSR	*Baseline Security Requirements*	Bazowe wymagania bezpieczeństwa
BRM	*Business Reference Model*	Model referencyjny działalności
C&A	*Certification and Accreditation*	Certyfikacja i akredytacja
CC	*Common Criteria*	Wspólne kryteria
CCB	*Configuration Control Board*	Komisja kontroli konfiguracji
CCEVS	*Common Criteria Evaluation and Validation Scheme*	Program oceny i walidacji wspólnych kryteriów
CCRB	*Configuration Control Review Board*	Komisja przeglądu kontroli konfiguracji
CFO	*Chief Financial Officer*	Kluczowa osoba w jednostce organizacyjnej odpowiedzialna za finanse
CIO	*Chief Information Officer*	Kluczowa osoba w jednostce organizacyjnej odpowiedzialna za technologie informacyjne
CIP	*Critical Infrastructure Protection*	Ochrona infrastruktury krytycznej
CISO	*Computer Information Security Officer*	Kluczowa osoba w jednostce organizacyjnej odpowiedzialna za bezpieczeństwo informacji
CM	*Configuration Management*	Zarządzanie konfiguracją
CMVP	*Cryptographic Module Validation Program*	Program walidacji modułów kryptograficznych
COOP	*Continuity of Operations*	Kontynuacja operacji
CPIC	*Capital Planning and Investment Control*	Planowanie finansowe i kontrola inwestycji

CSO	*Chief Security Officer*	Wyższe stanowisko kierownicze ds. Bezpieczeństwa informacji
DAA	*Designated Approving Authority*	Wyznaczony organ zatwierdzający
DRM	*Data and Information Reference Model*	Model referencyjny danych i informacji
FAQ	*Frequently Asked Questions*)	Najczęściej zadawane pytania
FEA	*Federal Enterprise Architecture*	Federalna architektura korporacyjna
FIPS	*Federal Information Processing Standard*	Federalny standard przetwarzania informacji
GSS	*General Support System*	System ogólnego wsparcia
IA	*Information Assurance*	Wiarygodność informacji
IDS	*Intrusion Detection System*	System wykrywania włamań
IEC	*International Electrotechnical Commission*	Międzynarodowa komisja elektrotechniczna
IG	*Inspector General*	Inspektor generalny
IRB	*Investment Review Board*	Komisja oceny inwestycji
ISA	*Interconnection Security Agreement*	Umowa o bezpiecznym połączeniu systemów
ISDN	*Integrated Services Digital Network*	Sieć cyfrowa z integracją usług
ISO	*International Organization for Standardization*	Międzynarodowa organizacja normalizacyjna
ISSO	*Information System Security Officer*	Osoba w organizacji, której przypisano odpowiedzialność za zapewnienie utrzymania odpowiedniego poziomu bezpieczeństwa operacyjnego dla systemu informacyjnego
IT	*Information Technology*	Technologia informatyczna/informacyjna

ITL	*Information Technology Laboratory*	Laboratorium informacyjne
KSA	*Knowledge, Skills, and Abilities*	Wiedza, umiejętności i zdolności
LAN	*Local Area Network*	Lokalna sieć komputerowa
LCC	*Life Cycle Cost*	Koszt cyklu życia
MA	*Major Application*	Aplikacja główna
MAO	*Maximum Allowable Outage*	Maksymalny dopuszczalny czas przestoju
MOA	*Memorandum of Agreement*	Porozumienie o współpracy
MOU	*Memorandum of Understanding*	Protokół uzgodnień
NIAP	*National Information Assurance Partnership*	Krajowe partnerstwo na rzecz zapewnienia bezpieczeństwa informacji
NIST	*National Institute of Standards and Technology*	Narodowy Instytut Standaryzacji i Technologii
NVD	*National Vulnerability Database*	Krajowa baza podatności danych na zagrożenia; uprzednio znana pod nazwą I-CAT
OCI	*Organizational Conflict of Interest*	Organizacyjny konflikt interesów
OMB	*Office of Management and Budget*	Biuro ds. Zarządzania i Budżetu
PKI	*Public Key Infrastructure*	Infrastruktura klucza publicznego (*ang. Public key infrastructure*)
POA&M	*Plan of Action and Milestones*	Plan i etapy działania; Kamienie milowe
POC	*Point of Contact*	Punkt kontaktowy
PRM	*Performance Reference Model*	Model referencyjny wydajności
RTO	*Recovery Time Objective*	Czas odzyskiwania

SAISO	*Senior Agency Information Security Officer*	Kluczowa osoba w jednostce organizacyjnej odpowiedzialna za bezpieczeństwo informacji
SANS	*SysAdmin, Audit, Network, Security*	Administrator systemu, audyt, sieć, bezpieczeństwo
SDLC	*System Development Life Cycle*	Cykl życia systemu
SLA	*Service-Level Agreement*	Umowa gwarancji świadczenia usługi
SOP	*Standard Operating Procedure*	Standardowa procedura operacyjna
SP	*Special Publication*	Publikacja specjalna
SPP	*Security and Privacy Profile*	Profil bezpieczeństwa i prywatności
SRM	*Service Component Reference Model*	Model referencyjny komponentu usługowego
ST&E	*Security, Test, and Evaluation*	Bezpieczeństwo, badanie i ocena
TRM	*Technical Reference Model*	Techniczny model referencyjny
UPS	*Uninterruptible Power Supply*	Zasilanie bezprzerwowe
CERT	*Computer Emergency Readiness Team*	Zespół reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet
CSIRT	*Computer Security Incident Response Teams*	Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego
VPN	*Virtual Private Network*	Wirtualna sieć prywatna
WAN	*Wide Area Network*	Rozległa sieć informatyczna

ZAŁĄCZNIK B NAJCZĘŚCIEJ ZADAWANE PYTANIA

B.1 UŚWIADAMIANIE I SZKOLENIA - PODSUMOWANIE NAJCZĘŚCIEJ ZADAWANYCH PYTAŃ

P.[100] *Dlaczego szczegółowy program uświadamiania i szkolenia jest istotny dla programu bezpieczeństwa?*

P. Czym jest świadomość w zakresie bezpieczeństwa?

P. Czym jest szkolenie w zakresie bezpieczeństwa?

P. W jaki sposób można ustanowić program uświadamiania i szkolenia?

P. Jak organizacja może podnieść świadomość w zakresie bezpieczeństwa?

P. Kiedy należy zmienić program uświadamiania i szkolenia?

P. Czym jest szkolenie oparte na podziale ról?

P. W jaki sposób można oszacować wsparcie dla programu uświadamiania i szkolenia?

P. W jaki sposób można zmierzyć skuteczność programu uświadamiania i szkolenia?

P. Czym różnią się od siebie „certyfikaty" nadawane przez dostawców, podmioty trzecie lub uczelnie?

P. Co wspólnego z bezpieczeństwem mają „profesjonalizacja" i rozwój zawodowy?

P. Dlaczego szczegółowy program uświadamiania i szkolenia jest istotny dla programu bezpieczeństwa?

O.[101] Największym komponentów tworzącym rozwiązania w zakresie bezpieczeństwa informacji jest personel. Stanowi on zasób, który:

- rozwija zasady i procedury;
- projektuje i rozwija aplikacje i systemy;

---

[100] P. – pytanie.

[101] O. – odpowiedź.

- wdraża i monitoruje środki bezpieczeństwa;
- zapewnia zgodność z przepisami;
- zarządza misją i celami biznesowymi;
- wykorzystuje informacje.

Jeżeli chodzi o całościowe rozwiązanie w zakresie bezpieczeństwa, znaczenie personelu dla realizacji celów bezpieczeństwa informacji oraz waga szkolenia jako środka przeciwdziałania są nie do przecenienia. Ustanowienie i utrzymanie solidnej i odpowiedniej świadomości bezpieczeństwa informacji oraz programu szkoleń w tym zakresie, w ramach ogólnego programu bezpieczeństwa informacji, to główny kanał dostarczania personelowi informacji i narzędzi potrzebnych do ochrony żywotnych zasobów informacyjnych organizacji. Organizacje, które nieprzerwanie szkolą swój personel w zakresie zasad bezpieczeństwa organizacyjnego i obowiązków dotyczących bezpieczeństwa opartych na podziale ról będą bardziej skuteczne w ochronie informacji.

P. Czym jest świadomość w zakresie bezpieczeństwa?

O. „Świadomość" to dla wszystkich pracowników punkt wyjścia w poszukiwaniu wiedzy na temat bezpieczeństwa informacji. Świadomość ma na celu skupienie uwagi jednostki na zagadnieniu lub zbiorze zagadnień. Świadomość to nie szkolenie.

Programy świadomości w zakresie bezpieczeństwa są rozwiązaniem łączącym działania promujące bezpieczeństwo, ustanawiające rozliczalność i dostarczające personelowi nowych wiadomości o bezpieczeństwie. Programy świadomości docierają do użytkowników w sposób ciągły i w różnych formach z przekazem dotyczącym bezpieczeństwa i dostarczają im informacji o bezpieczeństwie.

P. Czym jest szkolenie w zakresie bezpieczeństwa?

O. Szkolenie w zakresie bezpieczeństwa ma za zadanie wykształcić w personelu odpowiednią i potrzebną wiedzę oraz umiejętności. Szkolenie wspiera rozwój kompetencji i pomaga personelowi zrozumieć i nauczyć się w jaki sposób należy pełnić role związane z bezpieczeństwem. Szkolenie w zakresie bezpieczeństwa

obejmuje kursy z bezpieczeństwa ogólnego odpowiednie i właściwe dla całego personelu, a także oferuje przeszkolenie oparte na podziale ról, które jest dostosowane do konkretnych potrzeb każdej z ról w zakresie bezpieczeństwa.

P. W jaki sposób można ustanowić program uświadamiania i szkolenia?

O. Przygotowanie wykonalnego programu uświadamiania i szkolenia wymaga czasu, a jeżeli odbywa się to od podstaw, to najlepiej przyjąć podejście etapowe. Program uświadamiania i szkolenia można zbudować realizując pięcioetapowy proces:

1. analiza;
2. projekt;
3. opracowanie;
4. wdrożenie;
5. ewaluacja.

Pomocne informacje można znaleźć się w dokumentach: NIST SP 800-50, Building an Information Technology Security Awareness and Training Program, and NIST SP 800-16, Information Technology Security Training Requirements: A Role-and Performance-Based Model.

P. W jaki sposób organizacja może podnieść świadomość w zakresie bezpieczeństwa?

O. Organizacja może podnieść świadomość w zakresie bezpieczeństwa poprzez ustanowienie ciągłego programu, który wykorzystuje różne metody, w tym:

- Narzędzia promujące tematy bezpieczeństwa, w tym takie wydarzenia jak dzień świadomości bezpieczeństwa, materiały promocyjne oraz reguły postępowania.
- Komunikowanie materiałów związanych z bezpieczeństwem użytkownikom, kierownikom, dyrektorom, właścicielom systemu oraz innym osobom poprzez takie działania jak ocena (modele jak jest/jak ma być), plan strategiczny czy realizacja programu.

- Działania popularyzacyjne, wykorzystujące wewnętrzne i zewnętrzne „najlepsze praktyki" w zakresie bezpieczeństwa, takie jak portale internetowe, elektroniczne biuletyny poświęcone bezpieczeństwu czy FAQ.
- Miary pozwalające zmierzyć skuteczność programu uświadamiania.

P. Kiedy należy zmienić program uświadamiania i szkolenia?

O. Programy uświadamiania i szkolenia powinny podlegać ciągłym zmianom, aby odpowiadać potrzebom właściwym dla środowiska, kultury, działalności i misji danej organizacji. Programy powinny stale ewoluować w miarę pojawiania się nowych technologii i związanych z nimi kwestii bezpieczeństwa. Potrzeby szkoleniowe będą się zmieniać wraz z zapotrzebowaniem na nowe umiejętności i zdolności odpowiadające nowym zasadom oraz wynikającym z nich zmianom architektonicznym i technologicznym. Wpływ na pomysły dotyczące najlepszych sposobów projektowania rozwiązań i treści szkoleniowych będzie miała zmiana misji i/lub celów organizacji. Pojawiające się kwestie, np. obrona ojczyzny, również wpływają na charakter i zakres działań z zakresu rozwoju zawodowego niezbędnych dla bieżącego informowania/edukowania użytkowników o najnowszych zagrożeniach, podatnościach i środkach przeciwdziałania. W końcu, zmiany wynikające z ewolucji polityk bezpieczeństwa powinny znajdować odzwierciedlenie w materiałach uświadamiających i szkoleniowych z zakresu bezpieczeństwa.

P. Czym jest szkolenie oparte na podziale ról?

O. Osoby fizyczne mogą wymagać szkolenia opartego na funkcjach jakie faktycznie wykonują w swojej pracy. Z upływem czasu lub w wyniku przejścia do innej organizacji, osoba nabywa różne role dotyczące wykorzystywania technologii informacyjnej. Czasem jest ona użytkownikiem aplikacji, kiedy indziej może uczestniczyć w tworzeniu nowego systemu, a w jeszcze w innych przypadkach może być członkiem organu ds. wyboru źródeł zajmującego się doborem i oceną systemów IT oferowanych przez dostawców. Wiedza i umiejętności z zakresu bezpieczeństwa posiadane przez daną osobę, a zatem również jej potrzeby szkoleniowe, ulegają zmianom wraz ze zmianami roli, którą ona pełni.

W związku z tym, potrzeby w zakresie wiedzy i umiejętności sklasyfikowano pod względem funkcji pracy w sześciu specjalnościach opartych na pełnionych rolach, które stanowią kategorie generycznych ról w organizacji: zarządzanie, nabywanie, projektowanie i rozwijanie, wdrażanie i użytkowanie, oraz dokonywanie przeglądów i ewaluacji. Fatyczne stanowiska w danej organizacji są przydzielane do roli w celu ustalenia faktycznych wymagań dotyczących szkolenia na tym stanowisku. Przykładowo personel pracujący na stanowiskach, na których obowiązki i zadania odpowiadają personelowi ds. zamówień, przedstawiciela technicznego ds. zamówień czy członka organu ds. wyboru źródeł, otrzymałby rolę „nabywanie". Osoba autoryzująca, osoba odpowiedzialna za bezpieczeństwo informacji i inspektor, audytor odpowiadają roli „dokonywanie przeglądów i ewaluacji", ponieważ zajmują się głównie działaniami związanymi ze zgodnością.

P. W jaki sposób można oszacować wsparcie dla programu uświadamiania i szkolenia?

O. Wsparcie dla programu uświadamiania i szkolenia można wykazać przy pomocy wielu wskaźników. Oto kilka przykładów:

- Okazanie zaangażowania i wsparcia przez kluczowego interesariusza.
- Zabudżetowanie i udostępnienie wystarczających środków na realizację uzgodnionej strategii uświadamiania i szkolenia.
- Sfinansowanie i wdrożenie infrastruktury wspierającej szeroką dystrybucję i publikację materiałów uświadamiających i szkoleniowych w zakresie bezpieczeństwa (np. Internet, poczta elektroniczna, systemy zarządzania nauką).
- Osoby na wyższych stanowiskach kierowniczych przekazują personelowi komunikaty dotyczące bezpieczeństwa (np. spotkania z personelem, audycje szefa organizacji skierowane do wszystkich użytkowników), są orędownikami programu i okazują wsparcie dla szkolenia poprzez przeznaczanie środków na jego finansowanie.
- Poziom uczestnictwa w dobrowolnych forach/briefingach/szkoleniach poświęconych bezpieczeństwu jest niezmiennie wysoki.

- Dyrektorzy i kierownicy nie wykorzystują swojej pozycji w organizacji do unikania środków bezpieczeństwa, które są konsekwentnie przestrzegane przez szeregowych pracowników.

P. W jaki sposób można zmierzyć skuteczność programu uświadamiania i szkolenia?

O. Skuteczność programu uświadamiania i szkolenia można pokazać przy pomocy wielu wskaźników. Oto kilka przykładów:

- Organizacja przestaje być nękana szalejącymi atakami wirusów internetowych.
- Użytkownicy potrafią zidentyfikować i ograniczyć „spam" w poczcie elektronicznej.
- Ocena wiarygodności ulega poprawie.
- Wyniki oceny świadomości wskazują na zachowanie wiedzy z zakresu bezpieczeństwa przekazanej w ubiegłym roku.
- Personel jest bardziej responsywny/sprawny w wykonywaniu swoich obowiązków z zakresu bezpieczeństwa.
- Personel na wszystkich poziomach wykazuje minimalny poziom umiejętności posługiwania się komputerem.
- Personel jest mniej podatny na inżynierię społeczną.
- Użytkownicy stosują silniejsze hasła.

P. Czym różnią się od siebie „certyfikaty" nadawane przez dostawców, podmioty trzecie lub uczelnie?

O. Istnieją wyraźne różnice między „certyfikatami" szkoleń, które są oferowane przez różne organizacje. Można spotkać się przede wszystkim z certyfikatami ukończenia szkolenia, certyfikatami nadawanymi przez podmioty branżowe i/lub dostawców, a także świadectwami nauki nadawanymi przez instytucje akademickie:

- **Certyfikat ukończenia szkolenia** jest nadawany osobie dla potwierdzenia, że uczestniczyła ona w kursie—nie stwierdza on, czy dana osoba faktycznie nabyła wiedzę i/lub umiejętności.
- **Certyfikaty nadawane przez podmioty branżowe i dostawców** wymagają solidnego połączenia wyszkolenia, wykształcenia i doświadczenia. Posiadanie wiedzy i umiejętności jest potwierdzane w procesie walidacji. Certyfikaty takie oferują różny stopień pewności co do tego, że dana osoba posiadła podstawową wiedzę, umiejętności i zdolności z zakresu objętego szkoleniem. Przygotowanie do uzyskania certyfikatu potwierdzającego posiadanie wiedzy lub umiejętności zazwyczaj obejmuje udział w szkoleniu z określonego zakresu wiedzy lub programu nauczania technicznego i jest często uzupełniane przez zajęcia praktyczne.
- **Świadectwa nauki** w zakresie wiarygodności informacji są nadawane przez instytucje akademickie osobom, które spełniły wszystkie wymagania dotyczące ukończenia nauki. Do uzyskania tych świadectw zazwyczaj wymagane jest zaliczenie stosownej liczby godzin badań naukowych, ukończenie co najmniej czterech kursów (z możliwością wyboru jednego lub dwóch kursów dodatkowych) oraz mogą wymagać napisania pracy badawczej, projektu lub studium przypadku.

P. Co wspólnego z bezpieczeństwem mają „profesjonalizacja" i rozwój zawodowy?

O. Profesjonalizacja wspiera potrzebę spójności i standaryzacji polityk, procesów i procedur obowiązujących w organizacji. W przypadku osób zawodowo zajmujących się bezpieczeństwem tendencja do profesjonalizacji odzwierciedla zmianę organizacyjną, jaka zachodzi we wszystkich organizacjach, w miarę jak kładą one coraz większy nacisk na bezpieczeństwo i zdają sobie sprawę z tego, że bezpieczeństwo to praca w pełnym wymiarze czasu. Profesjonalizacja jest osiągana przez rozwój zawodowy. Dążenie do rozwoju zawodowego i zdobywania certyfikatów określane jest mianem „profesjonalizacji".

Rozwój zawodowy łączy szkolenie, kształcenie i doświadczenie z pewną formą oceny, która potwierdza wiedzę i umiejętności oraz „certyfikuje” uprzednio określony poziom kompetencji. Właściwe połączenie świadomości, szkolenia, wykształcenia, doświadczenia i certyfikacji służy rozwojowi zawodowemu, a ten z kolei prowadzi do powstania efektywnie działającego personelu.

B.2 PLANOWANIE FINANSOWE - PODSUMOWANIE NAJCZĘŚCIEJ ZADAWANYCH PYTAŃ

P. Czym jest integracja bezpieczeństwa z procesem planowania finansowego i kontroli inwestycji (ang. Capital Planning and Investment Control - CPIC)?

P. Jakie kryteria należy poddać ocenie podczas ustalania priorytetów możliwości planowania inwestycji?

P. Co jest podstawą priorytetów bezpieczeństwa informacji, którą organizacja powinna uwzględnić we wszystkich swoich inwestycjach?

P. Czym jest luka zgodności?

P. Czym jest wpływ działania naprawczego?

P. Co to jest Załącznik 300?

P. Co to jest Załącznik 53?

P. Jaki jest związek między Załącznikiem 300 i Załącznikiem 53?

P. Jaka jest rola kierownika ds. programu bezpieczeństwa w zakresie integracji bezpieczeństwa informacji z procesem CPIC?

P. Czy istnieje proces integracji bezpieczeństwa z planowaniem finansowym i kontrolą inwestycji?

O. Tak. Istnieje siedmiostopniowy proces nadawania priorytetów działaniom w zakresie bezpieczeństwa oraz działaniom naprawczym:

1. Identyfikacja stanu bazowego.
2. Identyfikacja wymagań w zakresie nadawania priorytetów.
3. Ustalenie priorytetów na poziomie korporacji.
4. Ustalenie priorytetów na poziomie systemu.
5. Opracowanie materiałów pomocniczych.
6. Powołanie Komisji oceny inwestycji i wprowadzenie zarządzania portfelem.

7. Przedłożenie Załączników 300 i Załącznika 53 oraz prowadzenia zarządzania programami.

P. Jakie kryteria należy poddać ocenie podczas ustalania priorytetów możliwości planowania inwestycji?

O. Priorytetowy charakter mają wymagania dotyczące najpilniejszych potrzeb inwestycyjnych z zakresu bezpieczeństwa. Szczegółowe kryteria dotyczące ustalania priorytetów będą różnić się w zależności od misji i celów danej organizacji oraz obowiązujących przepisów i uregulowań. Priorytety mogą opierać się na misji organizacji, wytycznych lub innych priorytetach zewnętrznych/wewnętrznych. Przykładowe priorytety w zakresie bezpieczeństwa to: certyfikacja i akredytacja wszystkich systemów czy wdrożenie infrastruktury klucza publicznego w całej organizacji.

P. Co jest podstawą priorytetów bezpieczeństwa informacji, którą organizacja powinna uwzględnić we wszystkich swoich inwestycjach?

O. Priorytety mogą opierać się na misji organizacji, wytycznych władzy wykonawczej lub innych priorytetach zewnętrznych/wewnętrznych. Przykładowe priorytety w zakresie bezpieczeństwa to: certyfikacja i akredytacja wszystkich systemów czy wdrożenie PKI w całym przedsiębiorstwie.

P. Czym jest luka zgodności?

O. Luka zgodności to różnica między pożądanym i faktycznym stopniem zgodności z wymaganiami bezpieczeństwa. Na przykład, jeżeli w danym systemie informacyjnym ukończono 80 procent działań związanych z certyfikacją i akredytacją, to luka zgodności dla tej inwestycji wynosi 20 procent. Faktyczna zgodność wynosząca 80 procent odjęta od pożądanego stopnia zgodności wynoszącego 100 procent daje lukę zgodności wynoszącą 20 procent. Im mniejsza luka zgodności, tym wyższy stopień zgodności danego systemu lub zabezpieczenia organizacyjnego.

P. Czym jest wpływ działania naprawczego?

A. Wpływ działania naprawczego to stosunek luki zgodności do kosztu działania naprawczego. Jest obliczamy jako iloraz wartości procentowej luki zgodności i kosztu wdrożenia odpowiedniego działania naprawczego/odpowiednich działań naprawczych. Wynikiem jest proporcja rezultatu do kosztu. Im jest ona wyższa, tym większa będzie opłacalność przeprowadzonego działania naprawczego.

Otrzymana proporcja jest mnożona przez 100 000 na potrzeby dalszych obliczeń.

$$\left(\frac{\text{Wartość procentowa luki zgodności po zrealizowaniu działania naprawczego}}{\text{Koszt działania naprawczego}} \right) \times 100{,}000$$

P. Co to jest Załącznik 300?[102]

O. Załącznik 300 to mechanizm, który ujmuje wszystkie analizy i działania wymagane do pełnego przeglądu (Komisja Oceny Inwestycji, CIO). Co więcej, Załącznik 300 to dokument, który wykorzystuje się do oceny inwestycji i podjęcia ostatecznej decyzji o finansowaniu. Umożliwia on dokonanie solidnej oceny danej inwestycji i stanowi uzasadnienie wniosków dotyczących cyklu życia i finansowania inwestycji IT.

P. Co to jest Załącznik 53?

O. Załącznik 53 umożliwia dokonanie ogólnego przeglądu całego portfela IT organizacji poprzez wyszczególnienie informacji o każdej inwestycji IT, cyklu życia i kosztach roku budżetowego. Oprócz ujęcia wszystkich inwestycji opisanych w Załącznikach 300, Załącznik 53 zawiera również inwestycje IT, które nie

[102] Informacje zawarte w rozdziale 5 odnoszą się do specyfikacji rynku amerykańskiego i zostały podane w celach poglądowych. Przy zastosowaniu tych wskazówek każdorazowo należy uwzględniać obowiązujące przepisy krajowe i regulacje wewnętrze organizacji.

wymagają Załącznika 300 (np. dotyczące już istniejących systemów z kosztami poniżej ustalonych dla organizacji progów).

P. Jaka jest rola kierownika ds. programu bezpieczeństwa w zakresie integracji bezpieczeństwa informacji z procesem CPIC?

O. Do obowiązków kierownika ds. programu bezpieczeństwa należy zarządzanie bezpieczeństwem informacji w całej organizacji. W przypadku procesu CPIC, kierownik ds. bezpieczeństwa informacji:

- Opracowuje i utrzymuje odpowiednie polityki dotyczące bezpieczeństwa informacji w całym okresie życia inwestycji;
  - ✓ Faza wyboru:
    - analiza wrażliwości danych,
    - ocena wpływu na prywatność,
    - ocena ryzyka,
    - plan bezpieczeństwa systemu,
    - planowanie awaryjne.
  - ✓ Faza kontroli:
    - certyfikacja i akredytacja (C&A),
    - plan i etapy działania (POA&M),
    - ponowna certyfikacja.
  - ✓ Faza ewaluacji:
    - określanie wrażliwości danych i ich usuwanie.
- Ustanawia proces, w ramach którego personel bezpieczeństwa dokonuje przeglądu rozdziałów „Bezpieczeństwo i prywatność" Załączników 300 dla każdej większej inwestycji, tak aby przedstawiały dokładne informacje i zabezpieczenia wprowadzone do systemu; oraz
- Pomaga w ustalaniu priorytetów działań naprawczych w oparciu o kwestie bezpieczeństwa IT w organizacji.

B.3 POŁĄCZENIA MIĘDZYSYSTEMOWE - PODSUMOWANIE NAJCZĘŚCIEJ ZADAWANYCH PYTAŃ

P. Czym jest ISA?

P. Jakie są elementy składowe ISA?

P. Czym jest MOU/MOA?

P. Jakie są elementy składowe MOU/MOA?

P. Jaka jest różnica między MOU/MOA i ISA?

P. Czy łączenie MOU/MOA i ISA jest dopuszczalne?

P. Kiedy musi mieć miejsce akredytacja i certyfikacja?

P. Jak często należy przeprowadzać przeglądy bezpieczeństwa?

P. Jakie kryteria powinny stosować organizacje do ustanowienia bazowych minimalnych zabezpieczeń, które należy wdrożyć w każdym z łączących się systemów?

P. Czy organizacje muszą aktualizować plan bezpieczeństwa systemu?

P. Czy poszczególne komputery łączące się z aplikacją przez Internet, znajdujące się za zaporą ogniową, wymagają ISA?

P. Czy dowolna strona ISA może ją wypowiedzieć?

P. Czy obie strony muszą udzielić odpowiedzi dla każdej pozycji ISA?

P. Czy ISA podlega jakimś wymaganiom federalnym?

P. Czym jest ISA?

O. Umowa o bezpiecznym połączeniu systemów (*ang. Interconnection Security Agreement - ISA*) to umowa zawierana przez organizacje posiadające i użytkujące połączone systemy informacyjne, która dokumentuje wymagania techniczne dla tego połączenia. ISA to dokument dotyczący bezpieczeństwa, który określa wymagania w zakresie połączenia systemów informacyjnych, opisuje zabezpieczenia, jakie zostaną zastosowane do ochrony systemów i danych oraz

zawiera rysunek topograficzny połączenia ISA to wzajemne zobowiązanie właścicieli obydwu systemów do przestrzegania określonych zasad postępowania. Zasady te mają charakter uznaniowy i powinny opierać się na ryzyku.

P. Jakie są elementy składowe ISA?

O. ISA powinna zawierać stronę tytułową oraz dokument składający się z ponumerowanych rozdziałów. Informacje w nich przedstawione powinny odnosić się do potrzeby połączenia oraz do zabezpieczeń wymaganych i wdrożonych w celu ochrony poufność, integralności i dostępności systemów i danych. Zakres informacji powinien być wystarczający do wydania rozważnej decyzji o zatwierdzeniu połączenia. Przykładowe rozdziały to:

- Rozdział 1: Wykaz wymagań w zakresie połączeń międzysystemowych,
- Rozdział 2: Względy bezpieczeństwa systemów,
- Rozdział 3: Rysunek topologiczny,
- Rozdział 4: Osoby upoważnione do podpisania dokumentu.

P. Czym jest MOU/MOA?

O. Protokół uzgodnień (*ang. Memorandum of Understanding, MOU*) / Porozumienie o współpracy (*ang. Memorandum of Agreement, MOA*) to dokument, który określa obowiązki dwóch lub więcej organizacji w zakresie ustanowienia, użytkowania i zabezpieczenia połączenia systemów. Definiuje cel połączenia, identyfikuje stosowne organy, precyzuje obowiązki każdej z organizacji, określa podział kosztów oraz ustala harmonogram zakończenia lub ponownej autoryzacji połączenia. MOU/MOA dokumentuje warunki wymiany zasobów danych i informacji oraz powinien zostać podpisany przez upoważnioną osobę w organizacji.

P. Jakie są elementy składowe MOU/MOA?

O. Każda organizacja może w stosownych przypadkach korzystać z własnego wzoru MOU/MOA, pamiętając jednocześnie, że jako dokument zarządczy nie powinien

on zawierać szczegółów technicznych połączenia. Każdy rozdział MOU/MOA powinien zawierać ogólne informacje, natomiast do szczegółów technicznych należy odnieść się oddzielnie w ISA. Dokument MOU/MOA powinien zawierać stronę tytułową, na której wymienione są obydwie organizacje będące jego stronami. Oprócz strony tytułowej, MOU/MOA może zawierać następujące rozdziały:

- Rozdział 1: Zastąpienie
  - ✓ Jeżeli MOU/MOA zastępuje inny dokument, to w tym miejscy powinny zostać wymienione jego tytuł i data.
- Rozdział 2: Wstęp
  - ✓ We wstępie podany zostaje cel zawarcia porozumienia przez strony oraz co będzie ono regulowało (np. stosunek między „Organizacją A" i „Organizacją B").
- Rozdział 3: Podstawy prawne
  - ✓ Przykładowa treść tego rozdziału to: „Podstawą obowiązywania niniejszego porozumienia jest „……" wydane przez …… w dniu (data)."
- Rozdział 4: Tło
  - ✓ W rozdziale dotyczącym tła porozumienia, strony powinny podać cel zawarcia porozumienia (np. „zamiarem obydwu stron niniejszego porozumienia jest połączenie następujących systemów informacyjnych……").
- Rozdział 5: Komunikacja między stronami
  - ✓ Częsta wymiana oficjalnych pism między stronami jest niezbędna do zapewnienia udanego zarządzania połączeniem i użytkowania go. W tym rozdziale strony zgadzają się utrzymywać otwarte linie komunikacji między wyznaczonymi pracownikami zarówno na poziomie zarządczym, jak i technicznym.

- Rozdział 6: Cel ISA
  - ✓ W tym rozdziale podany zostaje cel ISA.
- Rozdział 7: Wymagania bezpieczeństwa
  - ✓ Obydwie strony zgadzają się współpracować dla zapewnienia wspólnego bezpieczeństwa połączonych systemów oraz danych, które są w nich przechowywane, przetwarzane i przesyłane, zgodnie z postanowieniami ISA. Każda ze stron powinna określić środki bezpieczeństwa zastosowane do podłączania w oparciu o kategoryzację bezpieczeństwa informacji i poziom wpływu każdego z systemów oraz uzgodnić zestaw wzajemnych zabezpieczeń.
- Rozdział 8: Kwestie kosztów
  - ✓ W tym rozdziale opisane zostają warunki dotyczące kosztów związanych z mechanizmem i/lub medium połączenia.
- Rozdział 9: Ramy czasowe trwania porozumienia
  - ✓ W tym rozdziale podane zostają ramy czasowe porozumienia (np. „Niniejsze porozumienie obowiązuje przez jeden (1) rok od daty złożenia ostatniego podpisu w polu poniżej. Po upływie jednego (1) roku, niniejsze porozumienie wygasa").
- Rozdział 10: Osoby upoważnione do podpisania dokumentu

Należy pamiętać, iż jest to skrócony opis każdego z rozdziałów MOU/MOA. Szczegółowe informacje na ten temat podano w Załączniku 6.A.

P. Jaka jest różnica między ISA i MOU/MOA?

O. ISA jest wsparciem dla dokumentu MOU/MOA, który ustanawia wymagania dotyczące wymiany danych między dwiema organizacjami. MOU/MOA dokumentuje wymagania biznesowe i prawne niezbędne dla wsparcia relacji biznesowych między dwiema organizacjami. MOU/MOA nie powinien zawierać szczegółów technicznych ustanawianego połączenia. Tę funkcje pełni ISA. ISA to oddzielny dokument związany z bezpieczeństwem, który opisuje rozwiązania

techniczne i wymagania bezpieczeństwa dotyczące połączenia. Nie zastępuje on MOU/MOA. Kolejne aktualizacje MOU/MOA powinny odnosić się do odpowiedniej ISA obejmującego powiązania, które są przedmiotem MOU/MOA. ISA może zostać podpisana wyłącznie przez obydwie osoby autoryzujące (lub inne osoby z kierownictwa organizacji wyznaczone w tym celu), których nazwiska podano w Rozdziale 4 umowy. ISA powinna zostać oficjalnie podpisana przed ogłoszeniem gotowości operacyjnej połączenia.

P. Czy łączenie MOU/MOA i ISA jest dopuszczalne?

O. Tak. Organizacje mogą łączyć ISA i MOU/MOA, aby uprościć procesy zarządzania i ograniczyć ilość sporządzanej dokumentacji. Łącząc ISA i MOU/MOA, organizacje muszą dopilnować, aby treść oraz cel obydwu dokumentów pozostały nienaruszone.

P. Kiedy musi mieć miejsce akredytacja i certyfikacja?

O. Przed połączeniem systemów informacyjnych, każda z organizacji powinna dopilnować odpowiedniej certyfikacji i akredytacji swojego systemu zgodnie z przepisami i wytycznymi w tym zakresie. Proces certyfikacji i akredytacji dotyczy zarówno systemów nowych, jak i już produkowanych. Obejmuje on szereg działań związanych z bezpieczeństwem, w tym opracowanie i aktualizowanie planu bezpieczeństwa systemu, przeprowadzenie oceny ryzyka, przygotowanie planu awaryjnego oraz przeprowadzenie przeglądu bezpieczeństwa.

Ustanowienie połączenia może stanowić znaczącą zmianę dla łączonych systemów. Każda organizacja powinna wykonać ocenę dla ustalenia, czy recertyfikacja nowej konfiguracji jest wskazana.

P. Jak często należy przeprowadzać przeglądy bezpieczeństwa?

O. Jedna lub obydwie organizacje powinny przeprowadzać przegląd zabezpieczeń połączenia co najmniej raz w roku albo przy każdej znaczącej zmianie, aby upewnić się, że działają poprawnie i oferują odpowiedni poziom ochrony.

P. Jakie kryteria powinny stosować organizacje do ustanowienia zabezpieczeń bazowych, które należy wdrożyć w każdym z łączących się systemów?

O. Zabezpieczenia połączonych systemów powinny zostać poddane ewaluacji i spełnić standardy zabezpieczeń zarządczych, operacyjnych i technicznych najwyższej klasy między obydwoma systemami zgodnie z dokumentem NSC 800-53 i NSC 800-53B.

P. Czy organizacje muszą aktualizować plan bezpieczeństwa systemu?

O. Tak. Obydwie organizacje aktualizują swoje plany bezpieczeństwa systemu i inne stosowne dokumenty co najmniej raz w roku albo przy każdej znaczącej zmianie w ich systemach informacyjnych lub ustanowionym połączeniu. Informacje na temat aktualizacji planów bezpieczeństwa systemu, zob. NSC 800-18.

P. Czy poszczególne komputery łączące się z aplikacją przez Internet, znajdujące się za zaporą ogniową, wymagają ISA?

O. Nie. ISA to umowa zawierana między ***organizacjami***, a nie pojedynczymi systemami. Każdy system uczestniczący w połączeniu jest zarządzany przez osobę formalnie odpowiedzialną za użytkowanie systemu na dopuszczalnym poziomie ryzyka.

P. Czy dowolna strona ISA może ją wypowiedzieć?

O. Tak. W treści ISA należy stwierdzić w jaki sposób, kiedy i przez kogo umowa może zostać wypowiedziana. Decyzja w tej sprawie jest podejmowana podczas przygotowywania projektu umowy.

P. Czy obie strony muszą udzielić odpowiedzi dla każdej pozycji ISA?

O. Tak. Obie strony muszą udzielić odpowiedzi dla każdej pozycji, nawet jeżeli ma ona wpływ tylko na jedną z nich.

B.4 MIERNIKI WYNIKÓW - PODSUMOWANIE NAJCZĘŚCIEJ ZADAWANYCH PYTAŃ

P. Co daje organizacji korzystanie z metryk?

P. Jakie są współzależne komponenty programu metryki bezpieczeństwa?

P. Co mierzy metryka bezpieczeństwa informacji?

P. Jak jest różnica między rozwijaniem a wdrażaniem programu metryki?

P. Jakie działania składają się na proces metryki bezpieczeństwa informacji?

P. Jakie działania składają się na proces wdrażania bezpieczeństwa informacji?

P. Czy wykorzystanie programu metryki może pomóc organizacji w spełnieniu wymagań prawnych?

P. Metryka pomaga odpowiedzieć na trzy podstawowe pytania. Jakie to pytania?

P. Jak wybierane są różne metryki?

P. Czy w procesie wyboru metryki można użyć wagi?

P. Czy istnieją jakieś konkretne właściwości, które należy zdefiniować w każdej metryce?

P. Co daje organizacji korzystanie z metryk?

O. Metryki dają organizacjom wiele korzyści, w tym:

- poprawę rozliczalności bezpieczeństwa;
- umożliwienie kierownictwu wychwycenia konkretnych zabezpieczeń technicznych, operacyjnych lub zarządczych, które nie są wdrażane albo są wdrażane niewłaściwie;
- uzasadnienie wniosków inwestycyjnych przy użyciu zestawienia danych ilościowych i jakościowych;
- kierowanie inwestycji specjalnie do obszarów wymagających poprawy w celu maksymalizacji ich wartości;

- ustalenie skuteczności wdrożonych procesów, procedur i środków bezpieczeństwa informacji poprzez odniesienie wyników działań z zakresu bezpieczeństwa informacji (np. danych o incydentach, przychodów utraconych w wyniku cyberataków) do odpowiednich wymagań oraz inwestycji w bezpieczeństwo informacji.

P. Jakie są współzależne komponenty programu metryki bezpieczeństwa?

O. Współzależne komponenty programu metryki bezpieczeństwa to:

1. Mocne wsparcie ze strony wyższego kierownictwa, które kładzie nacisk na bezpieczeństwo na najwyższych szczeblach organizacji.
2. Praktyczne polityki i procedury bezpieczeństwa wsparte upoważnieniami koniecznymi do egzekwowania zgodności. Według definicji, praktyczne polityki i procedury bezpieczeństwa są osiągalne i zapewniają realne bezpieczeństwo poprzez zastosowanie odpowiednich zabezpieczeń. Metryki nie są łatwo osiągalne, jeżeli nie wdrożono żadnych procedur.
3. Wymierne metryki wyników, które mają za zadanie wychwytywać i dostarczać istotnych informacji na temat wyników. Aby uzyskane dane były istotne, wymierne metryki wyników muszą zostać oparte na celach i atrybutach bezpieczeństwa informacji oraz być łatwe do uzyskania i możliwe do zmierzenia. Muszą być również powtarzalne, pokazywać istotne tendencje wyników w czasie, a także być przydatne w śledzeniu wyników i kierowaniu środków oraz
4. Spójna, okresowa analiza danych metryki pozwalająca stosować wyciągnięte wnioski, poprawiać skuteczność istniejących środków bezpieczeństwa oraz planować przyszłe zabezpieczenia w celu spełnienia pojawiających się wymagań bezpieczeństwa. Jeżeli zebrane dane mają być istotne dla zarządzania i mają ułatwiać usprawnianie ogólnego planu bezpieczeństwa, to priorytetem dla interesariuszy i użytkowników musi być zbieranie dokładnych danych.

P. Co mierzy metryka bezpieczeństwa informacji?

O. Metryka mierzy wydajność i skuteczność oraz wdrożenie i wpływ działań z zakresu bezpieczeństwa.

P. Jak jest różnica między opracowaniem a wdrożeniem programu metryki?

O. Proces opracowania metryki skutkuje ustanowieniem początkowego zbioru metryk i wyborem podzbioru metryk, który jest odpowiedni dla danej organizacji w danym czasie. Proces wdrażania programu metryki wykorzystuje metrykę, która jest z natury iteracyjna i zapewnia pomiar odpowiednich aspektów bezpieczeństwa informacji w określonym czasie.

P. Jakie działania składają się na proces metryki bezpieczeństwa informacji?

A. Na proces opracowania metryki bezpieczeństwa informacji składają się dwa główne działania:

1. zidentyfikowanie i zdefiniowanie bieżącego programu bezpieczeństwa informacji oraz
2. opracowanie i dobór konkretnych metryk do pomiaru wdrażania, wydajności, skuteczności i wpływu środków bezpieczeństwa.

P. Jakie działania składają się na proces wdrażania bezpieczeństwa informacji?

O. Proces wdrażania bezpieczeństwa informacji składa się z sześciu faz:

1. przygotowanie do zbierania danych,
2. zbieranie danych i analiza wyników,
3. zidentyfikowanie działań naprawczych,
4. opracowanie uzasadnienia biznesowego,
5. uzyskanie zasobów,
6. zastosowanie działań naprawczych.

P. Czy wykorzystanie programu metryki może pomóc organizacji w spełnieniu wymagań prawnych?

A. Tak. Metryki bezpieczeństwa informacji pomogą w spełnieniu wymogu złożenia corocznego sprawozdania poprzez zapewnienie infrastruktury do zorganizowanego zbierania, analizy i raportowania danych. Dodatkowo, metrykę bezpieczeństwa informacji można wykorzystywać jako dane wejściowe dla przeprowadzanych audytów. Wdrożenie programu metryki bezpieczeństwa pokaże zaangażowanie się organizacji w aktywne zapewnianie bezpieczeństwa.

P. Metryka pomaga odpowiedzieć na trzy podstawowe pytania. Jakie to pytania?

O. Metryki są jednym z elementów zestawu narzędzi menedżera do podejmowania i uzasadniania decyzji. Metryki są wykorzystywane do odpowiedzi na trzy podstawowe pytania:

1. Czy wdrażam zadania, za które jestem odpowiedzialny?
2. Jak wydajnie i skutecznie realizuję te zadania?
3. Jaki jest wpływ tych zadań na misję mojej organizacji?

P. Jak wybierane są różne metryki?

O. Uniwersum możliwych metryk, w oparciu o istniejące zasady i procedury, będzie całkiem spore. Metryki należy uporządkować pod względem priorytetów, aby mieć pewność, że zbiór ostatecznie wybrany do wdrożenia posiada następujące cechy:

- Ułatwia wdrożenie zabezpieczeń o wysokim priorytecie. Wysoki priorytet może być określony w najnowszych sprawozdaniach, wynikach oceny ryzyka lub w wewnętrznych celach organizacji.
- Wykorzystuje dane, które można realnie uzyskać z istniejących procesów i repozytoriów danych.
- Mierzy procesy, które już istnieją i są stosunkowo stabilne. Mierzenie nieistniejących lub niestabilnych procesów nie da istotnych informacji na

temat wydajności bezpieczeństwa, a zatem nie przyda się w kierowaniu uwagi na konkretne aspekty tej wydajności.

Metryki można pozyskać z istniejących źródeł danych, w tym certyfikacji i akredytacji, ocen bezpieczeństwa, POA&M, statystyki zdarzeń oraz przeglądów niezależnych lub zainicjowanych przez organizację.

P. Czy w procesie wyboru metryki można użyć wagi?

O. Tak. W przypadku przypisania wag do metryk w fazie przygotowania do zbierania danych, wagi powinny zostać użyte do ustalenia priorytetów dla działań naprawczych. Ewentualnie, wagi można przypisać do działań naprawczych w fazie identyfikacji tych działań na podstawie newralgiczności wdrożenia poszczególnych działań naprawczych, ich kosztu oraz siły wpływu na stan bezpieczeństwa organizacji.

P. Czy istnieją jakieś konkretne właściwości, które należy zdefiniować w każdej metryce?

O. Po zidentyfikowaniu stosownych metryk zawierających wyżej opisane cechy, należy je udokumentować przy użyciu takich szczegółów pomocniczych, jak częstotliwość zbierania danych, źródło danych, formuła obliczania, dowody wdrożenia dla mierzonego działania oraz wskazówki do interpretacji danych metryki.

B.5 PLANOWANIE BEZPIECZEŃSTWA - PODSUMOWANIE NAJCZĘŚCIEJ ZADAWANYCH PYTAŃ

P. Czy w przypadku aplikacji pomocniczych wymagane są specjalne plany bezpieczeństwa systemu?

P. Czym są „Zasady zachowania”?

P. Co należy rozważyć przy dobieraniu początkowego zbioru środków bezpieczeństwa?

P. Czy organizacja może dostosować swoje zabezpieczenia bazowe?

P. Jaki krok następuje po opracowaniu planu bezpieczeństwa systemu informacyjnego?

P. Czy w przypadku aplikacji pomocniczych wymagane są specjalne plany bezpieczeństwa systemu?

O. Nie. Dla aplikacji pomocniczych nie są wymagane specjalne plany bezpieczeństwa systemu[103], ponieważ zabezpieczenia dla tych aplikacji są zazwyczaj zapewniane przez system ogólnego wsparcia (*ang. General Support System - GSS*) lub aplikację główną (*ang. Major Application - MA*), w ramach których działają. W przypadkach, gdzie aplikacja pomocnicza nie jest połączona z MA ani GSS, powinna ona zostać pokrótce opisana w planie GSS, który albo ma wspólną lokalizację fizyczną albo jest obsługiwany przez tę samą organizację.

P. Czym są „Zasady zachowania”?

O. Zasady powinny podawać konsekwencje sprzecznego zachowania lub braku zgodności oraz określać formalny sposób, w jaki organizacja dokumentuje zrozumienie przez użytkownika zasad i przewidzianych w związku z nimi konsekwencji. Zasady zachowania powinny zostać udostępnione wszystkim użytkownikom zanim uzyskają oni autoryzację dostępu do systemu.

---

[103] Dokument NSC 800-37 definiuje aplikację pomocniczą jako aplikację, inną niż aplikacja główna, która wymaga zwrócenia uwagi na bezpieczeństwo ze względu na ryzyko i skalę szkód wynikających z utraty, niewłaściwego użycia lub nieautoryzowanego dostępu do informacji w aplikacji lub ich modyfikacji. Aplikacje pomocnicze są zazwyczaj włączane jako część GSS.

P. Co należy rozważyć przy dobieraniu początkowego zbioru środków bezpieczeństwa?

O. Podczas wyznaczania granic systemu oraz doboru początkowego zestawu zabezpieczeń (tzn. zabezpieczeń bazowych) należy rozważyć poziomy wpływu podane w NSC 199. Zabezpieczenia bazowe można następnie dostosować w oparciu o ocenę ryzyka i lokalne uwarunkowania, w tym wymagania bezpieczeństwa właściwe dla organizacji, informacje o konkretnym zagrożeniu, analizy kosztów i korzyści, dostępność zabezpieczeń kompensacyjnych lub szczególnych okoliczności.

P. Czy organizacja może dostosować swoje zabezpieczenia bazowe?

O. Tak. Organizacja ma swobodę w dostosowywaniu zabezpieczeń. Działania dostosowawcze obejmują: (1) procedury ustalania zakresu działania systemu, (2) specyfikację zabezpieczeń kompensacyjnych oraz (3) specyfikację zdefiniowanych przez organizację parametrów zabezpieczeń, tam gdzie to dozwolone. Wszystkie działania dostosowawcze należy udokumentować w planie bezpieczeństwa systemu.

P. Jaki krok następuje po opracowaniu planu bezpieczeństwa systemu informacyjnego?

O. Ważne jest, aby po opracowaniu planu bezpieczeństwa systemu informacyjnego poddawać go okresowej ocenie, dokonywać przeglądu każdej zmiany w statusie, funkcjonalności czy projekcie systemu oraz dopilnować, aby plan niezmiennie odzwierciedlał prawidłowe informacje o systemie. Dokument ten, a także jego dokładność, mają krytyczne znaczenie dla certyfikacji systemu. Wszystkie plany należy poddawać przeglądowi i w stosowanych przypadkach aktualizacji co najmniej raz w roku.

B.6 PLANOWANIE AWARYJNE W ZAKRESIE IT - PODSUMOWANIE NAJCZĘŚCIEJ ZADAWANYCH PYTAŃ

P. Czym jest planowanie awaryjne w zakresie IT?

P. W jakim przedziale czasu konieczne jest przywrócenie systemów i danych w przypadku wystąpienia zakłócenia?

P. Czym jest deklaracja zasad planowania awaryjnego?

P. Czym jest analiza wpływu na działalność (ang. Business Impact Analysis, BIA)?

P. Czym jest maksymalny dopuszczalny czas przestoju (ang. Maximum Allowable Outage - MAO)?

P. Czym jest czas odzyskiwania (ang. Recovery Time Objective - RTO)?

P. Jakie komponenty strategii planowania awaryjnego w zakresie IT należy poddać testom?

P. Gdzie powinna być przechowywana kopia zapasowa danych?

P. Czym jest planowanie awaryjne w zakresie IT?

O. Planowanie awaryjne w zakresie IT to modułowy element większego programu planowania awaryjnego i planu kontynuacji operacji obejmującego IT, procesy biznesowe, zarządzanie ryzykiem, zarządzanie finansowe, komunikację kryzysową, bezpieczeństwo personelu i mienia oraz ciągłość funkcjonowania państwa. Każdy z tych elementów funkcjonuje samodzielnie, ale razem mogą stworzyć skoordynowaną synergię, która skutecznie i wydajnie chroni całą organizację.

P. W jakim przedziale czasu konieczne jest przywrócenie systemów i danych w przypadku wystąpienia zakłócenia?

O. W przypadku wystąpienia zakłócenia, strategię przywracania należy wdrożyć w przewidzianym czasie odzyskiwania (RTO).

P. Czym jest deklaracja zasad planowania awaryjnego?

O. Deklaracja zasad planowania awaryjnego to pierwszy krok w opracowywaniu planu awaryjnego w zakresie IT. Zasady te mogą istnieć na poziomie komórki organizacyjnej, organizacji i/lub programu organizacji. Deklaracja powinna definiować ogólne cele planowania awaryjnego oraz identyfikować kierownictwo, role i obowiązki, wymagania dotyczące zasobów, harmonogramy testów, szkolenia i ćwiczeń, a także zawierać plany obsługi serwisowej i minimalne wymagania dotyczące częstotliwości wykonywania kopii zapasowych.

P. Czym jest analiza wpływu na działalność (*ang. Business Impact Analysis, BIA*)?

A. BIA to kluczowy krok ku zrozumieniu komponentów, współzależności i wpływu potencjalnych przestojów w systemach informacyjnych. Strategię i procedury planu awaryjnego należy projektować szczególnie na podstawie wyników BIA. Analiza wpływu na działalność jest wykonywana poprzez identyfikację krytycznych zasobów systemu. Każdy kluczowy zasób jest następnie badany w celu ustalenia jak długo jego funkcjonalność może pozostawać niedostępna w systemie informacyjnym zanim wystąpi nieakceptowalny wpływ.

P. Czym jest maksymalny dopuszczalny czas przestoju (*ang. Maximum Allowable Outage, MAO*)?

O. W oparciu o potencjalny wpływ, jest to czas przez jaki system informacyjny może pozostawać bez kluczowego zasobu; jest on wykorzystywany jako priorytet odzyskiwania będący podstawą planowania.

P. Czym jest czas odzyskiwania (*ang. Recovery Time Objective, RTO*)?

O. RTO systemu informacyjnego jest ustalany w oparciu o punkt równowagi między MAO i kosztem odzyskania. Strategie odzyskiwania należy tworzyć tak, aby spełnić wymóg RTO. Strategia musi również uwzględniać odzyskiwanie krytycznych komponentów systemu informacyjnego w ramach danego priorytetu, zgodnie z ich RTO.

P. Jakie komponenty strategii planowania awaryjnego w zakresie IT należy poddać testom?

O. Testowanie strategii planowania awaryjnego w zakresie IT powinno obejmować:

1. odzyskanie systemu z zapasowych nośników na alternatywnej platformie,
2. koordynację między zespołami ds. odzyskiwania,
3. łączność wewnętrzną i zewnętrzną,
4. działanie systemu z wykorzystaniem alternatywnego sprzętu,
5. przywrócenie normalnego działania,
6. procedury zawiadamiania.

P. Gdzie powinna być przechowywana kopia zapasowa danych?

O. Zapasowa kopia danych powinna być przechowywana poza siedzibą organizacji, a nośniki powinny być poddawane częstej rotacji. Dodatkowo, przechowywane dane powinny być rutynowo testowane, aby potwierdzić ich integralność.

P. Czy należy szkolić i edukować personel w temacie planowania awaryjnego w zakresie IT?

O. Tak. Personel wybrany do wykonywania planu awaryjnego w zakresie IT musi być przeszkolony w realizacji procedur. Szkolenie personelu powinno obejmować:

- cel programu,
- koordynację i komunikację między zespołami,
- procedury raportowania,
- wymagania bezpieczeństwa,
- procesy właściwe dla danego zespołu,
- obowiązki indywidualne.

Ćwiczenia w zakresie planu powinny być projektowane indywidualnie, a następnie zbiorczo badać różne komponenty całego planu. Ćwiczenia można prowadzić w warunkach sali lekcyjnej i polegać na omówieniu konkretnych

komponentów planu i/lub zagadnień dotyczących wpływu, albo też mieć postać symulacji odzyskiwania danych przy użyciu faktycznego sprzętu zastępczego, danych i miejsc alternatywnych.

B.7 ZARZĄDZANIE RYZYKIEM - PODSUMOWANIE NAJCZĘŚCIEJ ZADAWANYCH PYTAŃ

P. Jaki jest główny cel procesu zarządzania ryzykiem?

P. Ile procesów obejmuje zarządzanie ryzykiem?

P. Jakie możliwości ograniczenia ryzyka obecnego w systemie mają zarządzający systemem i organizacją?

P. Zdefiniuj postepowanie z ryzykiem i wyjaśnij, jakie kroki są podejmowane w celu kontroli jego realizacji.

P. Ustanowiono zabezpieczenia. Czy możliwe jest przejście do ostatniego kroku procesu zarządzania ryzykiem?

P. Jaka jest formalna definicja ryzyka?

P. Czy możliwe jest obliczenie prawdopodobieństwa wykorzystania danej podatności przez zagrożenie?

P. Jakie są kroki w procesie szacowania ryzyka?

P. Jak opisywany jest system?

P. Czy istnieją powszechne zagrożenia dla systemu?

P. Czym jest podatność?

P. Jakie są poziomy ryzyka?

P. Jak często przeprowadzany jest proces szacowania ryzyka?

P. Jaki jest główny cel procesu zarządzania ryzykiem?

A. Głównym celem procesu zarządzania ryzykiem w organizacji powinna być ochrona organizacji i jej zdolności do realizacji misji, a nie tylko jej zasobów informacyjnych.

P. Ile procesów obejmuje zarządzanie ryzykiem?

O. Istnieją trzy procesy zarządzania ryzykiem: szacowanie ryzyka, mitygacja ryzyka

oraz ocenę. Kiedy zostaną zastosowane odpowiednio i z należytą starannością, procesy te powinny spełnić wymagania w zakresie „zapewnienia środków bezpieczeństwa informacji współmiernych do ryzyka i skali szkód wynikających z nieautoryzowanego dostępu, użytkowania, ujawnienia, zakłócenia, modyfikacji lub zniszczenia informacji i systemów informacyjnych”[104] zbieranych/użytkowanych przez organizacje, a także „zapewnienie, aby procesy zarządzania bezpieczeństwem informacji zostały zintegrowane z realizowanymi przez organizację procesami planowania strategicznego i operacyjnego”[105].

P. Jakie możliwości minimalizowania ryzyka obecnego w systemie mają osoby zarządzające systemem i organizacją?

O. Osoby zarządzające systemem i organizacją mają kilka możliwości zmniejszania ryzyka obecnego w systemie. Są to: przyjęcie ryzyka, unikanie ryzyka, ograniczanie ryzyka, planowanie ryzyka, badania i uznanie ryzyka oraz przeniesienie ryzyka.

P. Zdefiniuj postępowanie z ryzykiem i wyjaśnij, jakie kroki są podejmowane w celu kontroli jego realizacji.

O. Mitygacja ryzyka to drugi z procesów ogólnego procesu zarządzania ryzykiem. Ponieważ wyeliminowanie wszelkiego ryzyka z systemu jest niepraktyczne, a być może nawet niemożliwe, proces ograniczania ryzyka zmierza do ustalenia priorytetów, oceny i wdrożenia odpowiednich zabezpieczeń ograniczających ryzyko zalecanych na podstawie rekomendacji przedstawionych w dokumencie NSC 800-53 i NSC 800-53B. Po podjęciu decyzji o tym, które ryzyka należy uwzględnić w procesie mitygacji ryzyka, wdrożenie zabezpieczeń odbywa się według siedmioetapowego podejścia:

1. uporządkowanie działań pod względem priorytetu,
2. ocena zalecanych rozwiązań w zakresie zabezpieczeń,

---

104 Przykładowy cytat z Federal Information Security Management Act (FISMA).

105 Tamże.

3. przeprowadzenie analizy wydajności kosztów,
4. wybór zabezpieczenia,
5. przypisanie odpowiedzialności,
6. opracowanie planu wdrożenia środków bezpieczeństwa,
7. wdrożenie wybranego zabezpieczenia/wybranych zabezpieczeń.

P. Ustanowiono zabezpieczenia. Czy można już przejść do ostatniego kroku procesu zarządzania ryzykiem?

O. Nie. Należy zauważyć, iż nawet po wyborze i wdrożeniu zabezpieczeń pewien stopień ryzyka szczątkowego będzie nadal obecny. Zakładanie, że wszelkie ryzyko zostanie wyeliminowane jest niepraktyczne. Pozostałe ryzyko szczątkowe należy poddać analizie w celu zapewnienia, pozostanie na akceptowalnym poziomie. Po wprowadzeniu odpowiednich zabezpieczeń dotyczących zidentyfikowanych ryzyk, osoba autoryzująca podpisuje oświadczenie o akceptacji wszelkiego ryzyka szczątkowego i autoryzuje użytkowanie nowego systemu informacyjnego lub dalsze wykorzystanie istniejącego systemu informacyjnego. Jeżeli ryzyko szczątkowe nie zostanie ograniczone do akceptowalnego poziomu, cykl zarządzania ryzykiem należy powtórzyć, aby zidentyfikować sposób obniżenia go do poziomu, który można zaakceptować.

P. Jaka jest formalna definicja ryzyka?

O. Ustawa o krajowym systemie cyberbezpieczeństwa definiuje ryzyko jako „kombinację prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji”[106].

Publikacja NSC 800-30 definiuje ryzyko jako „funkcję prawdopodobieństwa wykorzystania potencjalnej podatności przez dane źródło zagrożenia i wpływu tego negatywnego zdarzenia na organizację”.

[106] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2022 r. poz. 1863 z późn. zm.).

P. Czy możliwe jest obliczenie prawdopodobieństwa wykorzystania danej podatności przez zagrożenie?

O. Tak. Prawdopodobieństwo, że dane zagrożenie skutecznie wykorzysta daną podatność jest szacowane poprzez ocenę motywacji, okazji i sposobów wykorzystania tej podatności. Wpływ udanego wykorzystania podatności szacowany jest poprzez analizę skutku, jaki to wykorzystanie może mieć na poufność, integralność i dostępność systemu i przetwarzanych w nim danych.

P. Jakie są kroki w procesie szacowania ryzyka?

A. Proces szacowania ryzyka składa się z sześciu kroków:

- Krok 1: scharakteryzowanie systemu,
- Krok 2: identyfikacja zagrożenia,
- Krok 3: identyfikacja podatności,
- Krok 4: analiza zabezpieczeń, ustalenie prawdopodobieństwa, analiza wpływu, ustalenie ryzyka,
- Krok 5: zalecenia dotyczące zabezpieczeń,
- Krok 6: udokumentowanie wyników.

P. Jak opisywany jest system?

O. System jest opisywany w kategoriach sprzętu, oprogramowania, interfejsów z innymi systemami, danych, ludzi, misji oraz krytyczności i wrażliwości (zgodnie z wcześniejszym opisem według NSC 199 użytym do ustalenia odpowiedniej kategorii bezpieczeństwa). Dodatkowo, opisywane są właściwe dla systemu wymagania funkcjonalne, zasady i architektura bezpieczeństwa, topologia sieci, przepływy informacji, zabezpieczenia zarządcze, operacyjne i techniczne, a także mechanizmy bezpieczeństwa fizycznego i środowiskowego.

P. Czy istnieją powszechne zagrożenia dla systemu?

O. Tak. Istnieją powszechne zagrożenia, które zazwyczaj występują niezależnie od tego, jaki system jest poddawany ocenie. Zagrożenia te można sklasyfikować w trzech obszarach: (1) zagrożenia naturalne (np. powodzie, trzęsienia ziemi,

wichury, osunięcia ziemi, lawiny, burze z wyładowaniami elektrycznymi), (2) zagrożenia ludzkie (zamierzone i niezamierzone) oraz (3) zagrożenia środowiskowe (np. awaria zasilania).

P. Czym jest podatność?

O. Ustawa o krajowym systemie cyberbezpieczeństwa definiuje podatność jako „właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa”[107].

Dokument NSC 800-30 definiuje podatność jako „wadę lub słabość procedur bezpieczeństwa, projektu, wdrożenia lub zabezpieczeń wewnętrznych systemu, którą można wykorzystać (przypadkowo lub w sposób zamierzony) i która skutkuje naruszeniem bezpieczeństwa lub złamaniem zasad bezpieczeństwa”.

P. Jakie są poziomy ryzyka?

O. Skala ryzyka - z ocenami ryzyka: wysokie, umiarkowane i niskie - przedstawia stopień lub poziom ryzyka, na jaki narażony może zostać system informacyjny, obiekt lub procedura w przypadku wykorzystania danej podatności. Skala ryzyka przedstawia również działania, jakie muszą zostać podjęte dla każdego poziomu ryzyka przez kierownictwo wyższego szczebla, właścicieli misji. Opisy ryzyka i związanych z nim działań są następujące:

- Wysokie: Jeżeli obserwacja lub ustalenie zostaje ocenione jako wysokie ryzyko, to istnieje pilna potrzeba wdrożenia środków naprawczych. Istniejący system może dalej działać, ale jak najszybciej należy wdrożyć plan działań naprawczych.
- Umiarkowane: Jeżeli obserwacja zostaje oceniona jako umiarkowane ryzyko, to potrzebne są działania naprawcze i w rozsądnym terminie należy opracować uwzględniający je plan.

[107] Tamże.

- Niskie: Jeżeli obserwacja zostaje opisana jako niskie ryzyko, to osoba autoryzująca system musi ustalić, czy potrzebne są działania naprawcze lub zdecydować o akceptacji ryzyka.

P. Jak często przeprowadzany jest proces szacowania ryzyka?

O. Proces szacowania ryzyka w organizacji jest powtarzany w ustalonych okresach. Jednakże szacowanie ryzyka powinno być wykonywane, a także zintegrowane z cyklem życia systemów informacyjnych nie dlatego, że jest wymagane przepisami prawa lub regulacjami, ale dlatego, że jest to dobra praktyka, która stanowi wsparcie celów biznesowych i misji organizacji.

B.8 CERTYFIKACJA, AKREDYTACJA I OCENY BEZPIECZEŃSTWA - PODSUMOWANIE NAJCZĘŚCIEJ ZADAWANYCH PYTAŃ

P. Czym jest certyfikacja bezpieczeństwa?

P. Czym jest akredytacja bezpieczeństwa?

P. Czy są jakieś niezbędne działania wspierające akredytację bezpieczeństwa?

P. Jakie są fazy procesu certyfikacji i akredytacji?

P. Co znajduje się w pakiecie akredytacji bezpieczeństwa?

P. Czym jest kwestionariusz oceny programu bezpieczeństwa informacji?

P. Czy wszystkie zabezpieczenia, o których mowa w dokumencie NSC 800-53 potrzebują corocznego przetestowania, aby spełnić wymaganie dotyczące corocznych testów?

P. Jakie czynniki powinny zostać uwzględnione podczas korzystania ze zautomatyzowanego narzędzia sprawozdawczości w zakresie oceny systemu?

P. Jakie działania związane z bezpieczeństwem powinny zostać zrealizowane przed przeprowadzeniem oceny systemu?

P. Czy organizacja musi dostosować formularz sprawozdawczy systemu do swoich uwarunkowań?

P. Czym jest certyfikacja bezpieczeństwa?

O. Certyfikacja bezpieczeństwa to kompleksowa ocena zabezpieczeń zarządczych, operacyjnych i technicznych w systemie informacyjnym, wykonywana dla wsparcia akredytacji bezpieczeństwa w celu ustalenia stopnia, w jakim zabezpieczenia zostały wdrożone prawidłowo, działają zgodnie z zamierzeniem i dają pożądany wynik w zakresie spełnienia wymagań bezpieczeństwa dotyczących systemu. Wyniki certyfikacji bezpieczeństwa są wykorzystywane do ponownego oszacowania ryzyka i zaktualizowania planu bezpieczeństwa systemu, tym samym dając osobie autoryzującej podstawę faktograficzną dla wydania decyzji w sprawie akredytacji bezpieczeństwa.

P. Czym jest akredytacja bezpieczeństwa?

O. Akredytacja w zakresie bezpieczeństwa to oficjalna decyzja kierownictwa wydana przez wyższego szczebla przedstawiciela organizacji, zezwalająca na eksploatację systemu informacyjnego i jednoznacznie akceptująca ryzyko dla działań organizacji, jej majątku lub osób w oparciu o wdrożenie uzgodnionego zestawu środków bezpieczeństwa. Akredytując system informacyjny, osoba wyższego szczebla w organizacji przyjmuje odpowiedzialność za bezpieczeństwo systemu i jest w pełni rozliczalna z wszelkich negatywnych skutków dla organizacji w przypadku naruszenia bezpieczeństwa. Tym samym, odpowiedzialność i rozliczalność to podstawowe zasady charakteryzujące akredytację bezpieczeństwa.

P. Czy są jakieś niezbędne działania wspierające akredytację bezpieczeństwa?

O. Tak. Oszacowanie ryzyka i opracowanie planów bezpieczeństwa systemu to dwa ważne działania w ramach realizowanego przez organizację programu bezpieczeństwa informacji, które bezpośrednio wspierają akredytację bezpieczeństwa i są wymagane stosownymi przepisami.

Szacowanie ryzyka ma wpływ na opracowywanie zabezpieczeń systemów informacyjnych i generuje dużą część informacji potrzebnych dla związanych z nimi planów bezpieczeństwa systemu. Oszacowanie ryzyka można przeprowadzić na różne sposoby w zależności od konkretnych potrzeb organizacji. Szacowanie ryzyka to proces, który powinien zostać włączony w cykl życia systemu. Jako minimum, należy sporządzić dokumentację, która opisuje stosowany proces i uzyskiwane wyniki.

Plany bezpieczeństwa systemu dostarczają przeglądu wymagań w zakresie bezpieczeństwa informacji i opisują wdrożone lub planowane zabezpieczenia mające spełnić te wymagania. Plany bezpieczeństwa systemu mogą zawierać, jako odniesienia lub załączniki, inne ważne dokumenty związane z bezpieczeństwem wytworzone w ramach realizowanego przez organizację programu bezpieczeństwa informacji (np. oszacowania ryzyka, plany awaryjne, plany reagowania na incydenty, plany uświadamiania i szkolenia w zakresie

bezpieczeństwa, zasady zachowania systemu informacyjnego, plany zarządzania konfiguracją, listy kontrolne konfiguracji bezpieczeństwa, oceny wpływu na prywatność, umowy o wzajemnym połączeniu systemów).

P. Jakie są fazy procesu certyfikacji i akredytacji?

O. Proces certyfikacji i akredytacji bezpieczeństwa składa się z czterech odrębnych faz:

1. Faza inicjacji. W tej fazie potwierdzone zostanie, że osoba autoryzująca i SAISO zgadzają się z treścią planu bezpieczeństwa systemu zanim organ certyfikujący rozpocznie ocenę zabezpieczeń systemu informacyjnego.
2. Faza certyfikacji bezpieczeństwa. W tej fazie zostanie ustalony stopień prawidłowości wdrożenia zabezpieczeń systemu informacyjnego, działania zgodnie z zamierzeniem oraz uzyskania pożądanego wyniku w zakresie spełnienia wymagań bezpieczeństwa dotyczących systemu.
3. Faza akredytacji bezpieczeństwa. W tej fazie zostanie ustalone, czy ryzyko dla działalności organizacji, zasobów organizacji lub osób fizycznych stwarzane przez znane podatności, które pozostały w systemie informacyjnym (po wdrożeniu uzgodnionego zestawu zabezpieczeń) jest na akceptowalnym poziomie.
4. Faza ciągłego monitorowania. W tej fazie wykonywane są regularny nadzór i monitorowanie zabezpieczeń systemu informacyjnego, a osoba autoryzująca jest informowana o zmianach mogących mieć wpływ na bezpieczeństwo systemu.

P. Co znajduje się w pakiecie akredytacji bezpieczeństwa?

O. Pakiet akredytacji bezpieczeństwa zawiera następujące dokumenty: zatwierdzony plan bezpieczeństwa systemu, sprawozdanie z oceny bezpieczeństwa oraz POA&M. Po sporządzeniu tych dokumentów, właściciel systemu informacyjnego przedkłada ostateczny pakiet akredytacji bezpieczeństwa osobie autoryzującej lub wyznaczonemu przedstawicielowi.

P. Czym jest kwestionariusz oceny programu bezpieczeństwa informacji?

O. Aby pomóc organizacjom w spełnieniu wymagań w zakresie sprawozdawczości, w kwestionariuszu oceny programu bezpieczeństwa informacji (Załącznik 11.A) zawarto szereg pytań dotyczących obszarów, które zwykle należy ująć w sprawozdaniu organizacji.

P. Czy wszystkie zabezpieczenia, o których mowa w dokumencie NSC 800-53, NSC 800-53B wymagają okresowego przetestowania, aby spełnić zalecenia dotyczące testów?

O. Aby spełnić wymagania dotyczące testów i ocen nie trzeba testować wszystkich zabezpieczeń, o których mowa w dokumencie NSC 800-53, NSC 800-53B. Organizacje powinny najpierw skupić się na pozycjach POA&M, które zostały zamknięte. Te nowo wdrożone zabezpieczenia należy poddać walidacji. Organizacje powinny przeprowadzić testy pod kątem związanych z bezpieczeństwem zmian w systemie, które już wystąpiły, ale które nie stanowią znaczących zmian wymagających nowego procesu certyfikacji i akredytacji. Organizacje powinny zidentyfikować wszystkie zabezpieczenia, które są monitorowane w sposób ciągły jako coroczne działania z zakresu testowania i ewaluacji. Do przykładów należą m.in. bieżące szkolenia w zakresie bezpieczeństwa, działania związane z ochroną przed zdarzeniami typu odmowa świadczenia usługi (DoS) i przed złośliwym kodem, monitorowanie w zakresie wykrywania włamań, przeglądy plików dziennika itp. Następnie organizacje powinny przyjrzeć się pozostałym zabezpieczeniom, które nie zostały przetestowane w tym okresie i w oparciu o ryzyko, znaczenie danego zabezpieczenia i datę ostatniego testu zdecydować, czy wykonać test coroczny.

P. Jakie czynniki powinny zostać uwzględnione podczas korzystania ze zautomatyzowanego narzędzia sprawozdawczości w zakresie oceny systemu?

O. Zautomatyzowanych narzędzi można używać do wsparcia procesu oceny i ułatwienia uzupełniania danych do sprawozdawczości wewnętrznej i zewnętrznej. Czynniki, które należy uwzględnić podczas używania zautomatyzowanych narzędzi to:

- zapewnienie kompletności funkcjonalności narzędzia pod kątem wsparcia wszystkich komponentów wymienionych w dokumencie NSC 800-53A;
- ustalenie kto będzie miał dostęp do tych narzędzi, w tym ustalenie konkretnych ról i obowiązków;
- dopilnowanie, aby narzędzie przetwarzające zostało zabezpieczone oraz certyfikowane i akredytowane;
- zapewnienie osobom używającym narzędzia/narzędzi odpowiedniego przeszkolenia;
- ustanowienie zdolności wsparcia technicznego.

P. Jakie działania związane z bezpieczeństwem powinny zostać zrealizowane przed przeprowadzeniem oceny systemu?

O. Przed przeprowadzeniem oceny systemu należy zrealizować szereg kluczowych działań związanych bezpieczeństwem. Należy przeprowadzić inwentaryzację całego systemu, a następnie skategoryzować wszystkie systemy zgodnie z ich wpływem na misję organizacji. W dalszej kolejności należy poczynić ustalenia co do granic systemu, uwzględniając wpływ jaki mają informacje przechowywane w systemie/systemach i przez ten system/te systemy przetwarzane lub przesyłane. Ukończony plan bezpieczeństwa systemu ogólnego wsparcia lub aplikacji głównej, powinien opisywać granice systemu, poziom wpływu danych oraz wdrożone lub planowane zabezpieczenia systemu.

P. Czy organizacja może dostosować formularz sprawozdawczy systemu do swoich uwarunkowań?

O. Tak. Formularz sprawozdawczy system może zostać dostosowany przez organizację. Organizacja może dodać więcej zabezpieczeń niż podano w każdej kategorii zabezpieczeń, wymagać bardziej opisowych informacji, a nawet w stosownych przypadkach wstępnie zaznaczyć pewne zabezpieczenia. Można dodać dodatkowe kolumny pokazujące stan zabezpieczenia, np. datę planowanego działania lub miejsce, w którym znajduje się dokumentacja.

B.9 NABYWANIE USŁUG I PRODUKTÓW BEZPIECZEŃSTWA - PODSUMOWANIE NAJCZĘŚCIEJ ZADAWANYCH PYTAŃ

P. Co należy uwzględnić podczas zarządzania projektem dotyczącym usług bezpieczeństwa?

P. Jakie są etapy cyklu życia usług bezpieczeństwa?

P. Co powinno poprzedzić wybór usługi bezpieczeństwa?

P. Czy istnieją kategorie usług bezpieczeństwa?

P. Czym jest organizacyjny konflikt interesów?

P. Czym jest umowa o świadczenie usług?

P. Dlaczego należy używać produktów bezpieczeństwa?

P. Jakie ważne kroki należy podjąć przy wyborze produktu bezpieczeństwa?

P. Kto powinien uczestniczyć w procesie wyboru produktu bezpieczeństwa?

P. Co należy uwzględnić podczas zarządzania projektem dotyczącym usług bezpieczeństwa?

O. Nie można lekceważyć systematycznego zarządzania procesem usług bezpieczeństwa informacji ze względu na potencjalny wpływ na organizację, jaki może mieć nieodpowiednie rozważenie wielu związanych z nim kwestii oraz brak zarządzania ryzykami organizacyjnymi. Decydenci zajmujący się bezpieczeństwem informacji muszą myśleć nie tylko o kosztach i wymaganiach bezpieczeństwa, ale też o wpływie podejmowanych przez siebie decyzji na misję, działalność, funkcje strategiczne i personel organizacji oraz na ustalenia z dostawcami usług.

P. Jakie są etapy cyklu życia usług bezpieczeństwa?

O. Cykl życia usług bezpieczeństwa informacji dostarcza ram, w których różni decydenci zajmujący się bezpieczeństwem informacji mogą organizować swoje działania w tym zakresie—od ich zainicjowania aż do zamknięcia.

Etapy tego cyklu życia to:

1. Faza inicjacji: ustalenie potrzeby.
2. Faza oceny: identyfikacja realnych rozwiązań.
3. Faza rozwiązania: określenie właściwego rozwiązania.
4. Faza wdrożenia: zaangażowanie właściwego źródła.
5. Faza użytkowania: zapewnienie sukcesu operacyjnego.
6. Faza zakończenia: zapewnienie pomyślnego zakończenia.

P. Co powinno poprzedzić wybór usługi bezpieczeństwa?

O. Przed wyborem konkretnych usług organizacje powinny dokonać przeglądu stanu swoich programów bezpieczeństwa oraz planowanych lub wdrożonych zabezpieczeń mających chronić informacje i systemy informacyjne. Organizacje powinny użyć procesu zarządzania ryzykiem do zidentyfikowania najskuteczniejszego połączenia zabezpieczeń zarządczych, operacyjnych i technicznych, które mitygują ryzyko do akceptowalnego poziomu. Liczba i rodzaj odpowiednich zabezpieczeń oraz związane z nimi usługi bezpieczeństwa informacji mogą się różnić na przestrzeni całego cyklu życia usług danego systemu. Na rodzaje odpowiednich zabezpieczeń wpływ może mieć względna dojrzałość architektury bezpieczeństwa wdrożonej w danej organizacji.

P. Czy istnieją kategorie usług bezpieczeństwa?

O. Tak. Usługi bezpieczeństwa dzielą się na trzy kategorie: zarządcze, operacyjne i techniczne. Poniżej przedstawiono charakterystykę każdej z nich:

- Usługi zarządcze to techniki i zagadnienia, którymi w programie bezpieczeństwa komputerowego danej organizacji zazwyczaj zajmuje się kierownictwo. Skupiają się one na zarządzaniu programem bezpieczeństwa komputerowego i ryzyku występującym w obrębie organizacji.
- Usługi operacyjne skupiają się na zabezpieczeniach wdrożonych i wykonywanych przez ludzi (w przeciwieństwie do systemów).

Często wymagają wiedzy specjalistycznej lub technicznej i polegają na działaniach kierownictwa i zabezpieczeniach.

- Usługi techniczne skupiają się na zabezpieczeniach wykonywanych przez system informacyjny. Ich skuteczność zależy od odpowiedniego działania systemu.

P. Czym jest organizacyjny konflikt interesów?

O. Organizacyjny konflikt interesów może wystąpić, kiedy strona umowy ma przeszły, obecny lub przyszły interes dotyczący pracy, która została lub ma zostać wykonana, który to interes może zmniejszyć zdolność do świadczenia bezstronnej, technicznie prawidłowej i obiektywnej obsługi albo skutkuje powstaniem nieuczciwej przewagi konkurencyjnej. Naturalnie najlepiej jest w ogóle nie dopuszczać do wystąpienia organizacyjnych konfliktów interesów.

P. Czym jest umowa o świadczenie usług?

O. Umowa o świadczenie usług to umowa między usługodawcą i organizacją oczekującą usługi. W miarę jak uzgodnienia dotyczące świadczenia usług stają się coraz bardziej złożone i zaczynają angażować usługodawców komercyjnych, sformalizowanie takich umów powinno być coraz większe. Na przykład, w pełni uzewnętrznione uzgodnienia dotyczące usług poczynione z podmiotem komercyjnym będą wymagały formalnego kontraktu umożliwiającego osobom zarządzającym rozliczanie usługodawców z ich działań.

P. Dlaczego należy używać produktów bezpieczeństwa?

O. Wybór i użycie produktów bezpieczeństwa w ramach ogólnego programu organizacji ma służyć zarządzaniu projektem, rozwojem i utrzymaniem jej infrastruktury bezpieczeństwa informacji oraz ochronie poufności, integralności i dostępności informacji o krytycznym znaczeniu dla jej misji.

P. Jakie ważne kroki należy podjąć przy wyborze produktu bezpieczeństwa?

O. Wybierając produkty bezpieczeństwa ważne jest, aby przeprowadzić analizę wydajności kosztów. W ramach analizy wydajności kosztów należy oszacować koszt cyklu życia dla stanu istniejącego i każdej zidentyfikowanej alternatywy.

Oprócz oszacowania cyklu kosztu życia należy określić korzyści związane z każdą alternatywą oraz, tak dalece jak to wykonalne, podać kwoty oszczędności lub unikniętych kosztów. Po zidentyfikowaniu niezbędnych zabezpieczeń, można określić produkty bezpieczeństwa informacji mające umożliwić ich wdrożenie.

P. Kto powinien uczestniczyć w procesie wyboru produktu bezpieczeństwa?

O. W wyborze produktu uczestniczy wiele osób z całej organizacji. W zależności od swoich potrzeb, organizacja może zaangażować wszystkie lub część z następujących osób stosownie do konkretnych potrzeb dotyczących bezpieczeństwa informacji: kierownik ds. programu bezpieczeństwa informacji, CIO, komisja oceny inwestycji informacyjnych (lub jej odpowiednik), kierownik ds. programu/właściciel systemu/właściciel danych/osoba inicjująca zamówienia, personel obsługujący zakupy, osoba ds. zamówień, przedstawiciel techniczny osoby ds. zamówień, SSO.

B.10 REAGOWANIE NA INCYDENTY - PODSUMOWANIE NAJCZĘŚCIEJ ZADAWANYCH PYTAŃ

P. Jakie są cztery fazy cyklu życia reagowania na incydenty?

P. Jakie są niektóre praktyki mogące zapobiegać incydentom?

P. Czym charakteryzuje się zdolność do reagowania na incydenty?

P. Dlaczego posiadanie zdolności do reagowania na incydenty jest ważne?

P. Za co odpowiedzialne są organizacje w zakresie sprawozdawczości incydentów dotyczących bezpieczeństwa?

P. Czy możliwe jest przygotowanie do reagowania na incydenty?

P. Co należy zawrzeć w politykach reagowania na incydenty?

P. Jakie elementy należy uwzględnić przy wyborze struktury zespołu i modelu obsady personelem?

P. Jakie są cztery fazy cyklu życia reagowania na incydenty?

O. Według dokumentu NSC 800-61, cztery fazy cyklu życia reagowania na incydenty to:

- przygotowanie,
- detekcja i analiza,
- powstrzymanie, usunięcie i odtworzenie,
- aktywność po incydencie.

P. Jakie są niektóre praktyki mogące zapobiegać incydentom?

O. Przykładowe praktyki pomagające zapobiegać incydentom to:

- posiadanie programu zarządzania poprawkami pomagającego administratorom systemu w identyfikowaniu, nabywaniu, testowaniu i stosowaniu poprawek eliminujących znane podatności systemów i aplikacji;

- odpowiednie ograniczenie (*ang. hardening*[108]) wszystkich hostów w celu wyeliminowania podatności i słabości konfiguracji;
- takie skonfigurowanie obwodu sieci, aby odrzucać wszelkie działania, które nie są w sposób wyraźny dozwolone;
- wprowadzenie w całej organizacji oprogramowania wykrywającego i zatrzymującego złośliwy kod;
- uświadomienie użytkowników w zakresie polityk i procedur dotyczących odpowiedniego użytkowania sieci, systemów i aplikacji.

P. Dlaczego posiadanie zdolności do reagowania na incydenty jest ważne?

O. Zgodnie z regulacjami prawnymi, organizacje[109] mają obowiązek posiadania zdolności pomagania użytkownikom w przypadku wystąpienia w systemie incydentu bezpieczeństwa oraz wymiany informacji na temat powszechnych podatności i zagrożeń.

P. Dlaczego posiadanie zdolności do reagowania na incydenty jest ważne?

O. Dobrze zdefiniowana zdolność reagowania na incydenty pomaga organizacji szybko wykrywać incydenty, minimalizować straty i zniszczenia, identyfikować słabości i bezzwłocznie przywracać operacje IT.

P. Za co odpowiedzialne są organizacje w zakresie sprawozdawczości incydentów dotyczących bezpieczeństwa?

O. Organizacje[110] mają obowiązek identyfikowania i zgłaszania ogólnej liczby udanych incydentów w następujących kategoriach: nieautoryzowany dostęp, ataki polegające na odmowie świadczenia usługi, złośliwy kod, niewłaściwe wykorzystanie lub inne (pomocna jest publikacja NSC 800-61). Incydenty należy rejestrować i zgłaszać wewnętrznie oraz, w zależności od ich dotkliwości, do

---

108 Potoczna nazwa – „utwardzanie".

109 Dotyczy podmiotów objętych Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2022 r. poz. 1863 z późn. zm.).

110 Tamże.

właściwych organów (np. CSIRT, organy ścigania). nieautoryzowany dostęp: w ciągu jednej (1) godziny od odkrycia i/lub wykrycia;

Specyficzny dla systemu plan reagowania na incydenty jest uważany za integralną część kompletnego pakietu certyfikacji i akredytacji.

P. Czy możliwe jest przygotowanie do reagowania na incydenty?

O. Tak. Aby przygotować się do reagowania na incydenty, organizacja powinna:

- stworzyć właściwą dla niej definicję „incydentu", wyraźnie określającą zakres tego terminu;
- stworzyć zasady reagowania na incydenty;
- opracować procedury reagowania na incydenty i zgłaszania ich;
- ustanowić wytyczne w zakresie komunikowania się z podmiotami zewnętrznymi;
- ustalić usługi świadczone przez zespół reagowania na incydenty;
- wybrać strukturę zespołu i model obsady personelem;
- obsadzić personelem i przeszkolić zespół reagowania na incydenty.

P. Co należy zawrzeć w zasadach reagowania na incydenty?

O. Zasady reagowania na incydenty powinny definiować, które zdarzenia należy uznawać za incydenty, ustanawiać strukturę organizacyjną reagowania na incydenty, definiować role i obowiązki oraz podawać wymagania dotyczące zgłaszania incydentów.

P. Jakie elementy należy uwzględnić przy wyborze struktury zespołu i modelu obsady personelem?

O. Organizacje powinny wybierać odpowiednią strukturę zespołu i model obsadzenia personelem w oparciu o kilka czynników, w tym wielkość organizacji, zróżnicowanie geograficzne najważniejszych zasobów obliczeniowych, potrzebę dostępności przez całą dobę siedem dni w tygodniu, koszt oraz wiedzę specjalistyczną posiadaną przez personel.

ZAŁĄCZNIK C ZARZĄDZANIE KONFIGURACJĄ - PODSUMOWANIE NAJCZĘŚCIEJ ZADAWANYCH PYTAŃ

P. Czym jest zarządzanie konfiguracją?

P. Dlaczego zarządzanie konfiguracją jest ważne?

P. Co należy rozważyć i uwzględnić podczas opracowywania procesu zarządzania konfiguracją?

P. Jakie kroki należy podjąć przed wdrożeniem zmiany?

P. Czy zarządzanie konfiguracją jest funkcją bezpieczeństwa?

P. Jakie są kroki w procesie zarządzania konfiguracją?

P. Co stanowi „zmianę”?

P. Co należy ocenić podczas analizy wpływu proponowanej zmiany?

P. Właśnie wprowadzono zmianę. Czy oznacza to koniec zadania?

P. Czym jest zarządzanie konfiguracją?

O. Według dokumentu NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*, „Procedury zarządzania konfiguracją i jej kontroli są kluczowe dla ustanowienia początkowego bazowego poziomu komponentów sprzętu komputerowego, oprogramowania i oprogramowania układowego dla danego systemu informacyjnego, a następnie do kontrolowania i utrzymania dokładnego wykazu wszystkich zmian w systemie. Zmiany dotyczące sprzętu komputerowego, oprogramowania lub oprogramowania sprzętowego mogą mieć znaczący wpływ na bezpieczeństwo systemu (...) zmiany powinny być dokumentowane, a ich ewentualny wpływ na bezpieczeństwo regularnie oceniany”.

P. Dlaczego zarządzanie konfiguracją jest ważne?

O. Zważywszy na złożoność i niepowtarzalność każdego systemu informacyjnego (często wynikającą z istnienia wielu kont i uprawnień użytkowników, używanego oprogramowania lub osobistych preferencji użytkowników), trudno jest identycznie skonfigurować każdy system względem pozostałych w danej sieci. Zadaniem zarządzania konfiguracją jest minimalizacja skutków jakie dla systemu informacyjnego lub sieci powodują te zmiany lub różnice w konfiguracji.
W przypadku wielu platform systemowych, każdy różniący się element (sprzęt komputerowy lub oprogramowanie) tworzy potencjalną podatność, która może zostać skompromitowana i w znaczącym stopniu wpłynąć na sieć.

P. Co należy rozważyć i uwzględnić podczas opracowywania procesu zarządzania konfiguracją?

O. Każda organizacja musi uwzględnić koszty i wydatki, wymagane planowanie i harmonogramowanie oraz niezbędne szkolenia związane z drobiazgowym i skutecznym procesem zarządzania konfiguracją.

P. Jakie kroki należy podjąć przed wdrożeniem zmiany?

O. Bardzo ważne jest przetestowanie możliwych zmian w konfiguracji przed ich wprowadzeniem. Przewidziane zmiany powinny zostać przetestowane w kontrolowanym

P. Czy zarządzanie konfiguracją jest funkcją bezpieczeństwa?

O. Nie. Chociaż nie jest tradycyjnie uznawane za funkcję bezpieczeństwa, zarządzanie konfiguracją musi zostać włączone do cyklu życia systemu ze względu na silne implikacje dla bezpieczeństwa. Zarządzanie konfiguracją to tylko jeden z komponentów stanu bezpieczeństwa systemu informacyjnego. Wchodzi ono w zakres zabezpieczeń operacyjnych systemu informacyjnego i jest wzajemnie powiązane z licznymi innymi dziedzinami bezpieczeństwa, takimi jak zarządzanie projektami, zarządzanie ryzykiem, certyfikacja i akredytacja oraz uświadamianie i szkolenia w zakresie bezpieczeństwa.

P. Jakie są kroki w procesie zarządzania konfiguracją?

O. W procesie zarządzania konfiguracją wyróżnia się kroki wymagane dla zapewnienia właściwego wnioskowania, oceniania i autoryzowania wszystkich zmian. Proces zarządzania konfiguracją dostarcza również szczegółowej procedury, która krok po kroku opisuje identyfikowanie, przetwarzanie, śledzenie i dokumentowanie zmian. Na proces zarządzania konfiguracją składają się następujące kroki:

- identyfikacja zmiany,
- ocena wniosku o zmianę,
- decyzja o realizacji,
- realizacja zatwierdzonego wniosku o zmianę ,
- ciągłe monitorowanie.

P. Co stanowi „zmianę”?

O. Na zmianę mogą składać się różne rzeczy: od aktualizacji pól lub rekordów bazy danych aż po modernizację systemu operacyjnego z najnowszymi poprawkami.

P. Co należy ocenić podczas analizy wpływu proponowanej zmiany?

O. Podczas analizy wpływu należy mieć na uwadze następujące kwestie:

- Czy zmiana jest opłacalna i poprawia działanie lub bezpieczeństwo systemu.
- Czy zmiana jest technicznie prawidłowa, konieczna i wykonalna w ramach ograniczeń systemu.
- Czy zmiana będzie miała wpływ na bezpieczeństwo systemu.
- Czy uwzględniono koszty związane z wdrożeniem zmiany oraz
- Czy zmiana ma wpływ na komponenty bezpieczeństwa.

P. Właśnie wprowadzono zmianę. Czy oznacza to koniec zadania?

O. Nie. System powinien być w sposób ciągły monitorowany, aby zapewnić, że działa zgodnie z zamierzeniami oraz że wprowadzone zmiany nie mają negatywnego wpływu na jego funkcjonowanie. Weryfikację i audyty konfiguracji należy przeprowadzać na tym etapie, aby zapewnić, że aktualizacje systemu nie mają na niego negatywnego wpływu. Weryfikacja i audyty polegają na zbadaniu cech systemu i dokumentacji pomocniczej w celu zweryfikowania, czy konfiguracja spełnia potrzeby użytkowników oraz czy obecna konfiguracja jest zatwierdzoną bazową konfiguracją systemu.

ZAŁĄCZNIK D REFERENCJE[111]

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[112]	
NSC 199	Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199
NSC 200	Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych – na podstawie FIPS 200
NSC 800-30	Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne – na podstawie NIST SP 800-30
NSC 800-34	Poradnik planowania awaryjnego – na podstawie NIST SP 800-34
NSC 800-37	Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu – na podstawie NIST SP 800-37
NSC 800-39	Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego – na podstawie NIST SP 800-39
NSC 800-53	Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53
NSC 800-53A	Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informacyjnych oraz organizacji. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A
NSC 800-53B	Zabezpieczenia bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B

[111] Referencje anglojęzyczne umieszczone zostały na w poszczególnych rozdziałach.

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