Ministerstwo Cyfryzacji

NARODOWY STANDARD CYBERBEZPIECZEŃSTWA
NSC 800-137 wer. 1.0

17 maja 2024

Strategia ciągłego monitorowania bezpieczeństwa informacji (ISCM) systemów informacyjnych i organizacji

Publikacja dostępna pod adresem:

Narodowe Standardy Cyberbezpieczeństwa

PREAMBUŁA

Szanowni Państwo,

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

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

Niniejsza publikacja **NSC 800-137 wer. 1.0, *Strategia ciągłego monitorowania bezpieczeństwa informacji (ISCM) systemów informacyjnych i organizacji***, opracowana została za zgodą National Institute of Science and Technology (NIST) na podstawie specjalnej publikacji NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.*

Przytaczane i cytowane w publikacji przepisy, okólniki, rozporządzenia wykonawcze, dyrektywy, normy, standardy, polityki, memoranda itp. odnoszą się, o ile nie zaznaczono inaczej, do prawodawstwa i rynku amerykańskiego. Jeżeli cytowany fragment ma przełożenie lub odpowiednik w polskim porządku prawnym lub normalizacyjnym, wówczas informacje te wskazane są bezpośrednio w tekście lub w przypisach.

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.

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[1]. Do wszystkich tych ról / funkcji zastosowano akronimy terminologii angielskiej.

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

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.

[1] Kluczowi uczestnicy zarządzania ryzykiem - patrz NSC 800-18; NSC 800-37, NSC 7298.

WSPÓLNE FUNDAMENTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

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

NIST kontynuuje współpracę z sektorem publicznym i prywatnym w celu stworzenia map i relacji pomiędzy opracowanymi przez siebie standardami i wytycznymi, a tymi, które zostały opracowane przez inne organizacje (m. in. ISO[2]), co zapewnia zgodność w przypadku, gdy regulacje wymagają stosowania 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.

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

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

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.

KLAUZULA PRAWNA

Niniejsza publikacja została opracowana przez NIST w celu realizacji jego ustawowych obowiązków wynikających z Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. NIST jest odpowiedzialny za opracowywanie standardów i wytycznych dotyczących bezpieczeństwa informacji, w tym minimalnych wymagań dla federalnych systemów informacyjnych, ale takie standardy i wytyczne nie mają zastosowania do systemów bezpieczeństwa narodowego bez wyraźnej zgody odpowiednich urzędników federalnych sprawujących władzę zwierzchnią nad takimi systemami. Niniejsze wytyczne są zgodne z wymogami Okólnika A-130 Biura Zarządzania i Budżetu (Office of Management and Budget, OMB), sekcja 8b(3), Zabezpieczanie systemów informacyjnych agencji, jak przeanalizowano w Okólniku A-130, Załącznik IV: Analiza kluczowych sekcji. Informacje uzupełniające znajdują się w Okólniku A-130, Dodatek III.

Żadna część niniejszej publikacji nie może stanowić podstawy do uznania za nieobowiązujące normy i wytyczne dotyczące agencji federalnych, ustanowionych przez Sekretarza ds. Handlu na mocy stosownych uprawnień ustawowych. Wytyczne zawarte w niniejszej publikacji nie zmieniają ani nie powinny być uznawane za nadrzędne względem uprawnień Sekretarza ds. Handlu, Dyrektora Biura ds. Zarządzania i Budżetu (OMB) lub jakiegokolwiek innego urzędnika federalnego. Niniejsza publikacja może być wykorzystywana przez organizacje pozarządowe na zasadzie dobrowolności i nie jest objęta prawami autorskimi na terytorium Stanów Zjednoczonych. NIST uprasza jednak o wskazanie autorstwa dokumentu.

Niektóre podmioty komercyjne, sprzęt lub materiały mogą być zidentyfikowane w niniejszym dokumencie w celu odpowiedniego opisania procedury eksperymentalnej lub koncepcji. Taka identyfikacja nie ma na celu rekomendacji lub poparcia przez NIST, ani nie ma na celu sugerowania, że dane podmioty, materiały lub sprzęt są najlepszymi dostępnymi do tego celu.

Niniejsza publikacja może zawierać odniesienia do innych dokumentów opracowywanych obecnie przez NIST zgodnie z przypisanymi mu obowiązkami statutowymi. Informacje zawarte w niniejszej publikacji, w tym koncepcje i metodologie, mogą być wykorzystywane przez organizacje nawet przed ukończeniem takich publikacji. W związku z tym, do czasu ukończenia każdej publikacji, aktualne wymagania, wytyczne i procedury, tam gdzie istnieją, pozostają obowiązujące. Do celów planowania i transformacji organizacje powinny uważnie śledzić rozwój tych nowych publikacji opracowywanych przez NIST.

Organizacje są zachęcane do przeglądu wszystkich projektów publikacji podczas publicznych okresów komentowania i dostarczania informacji zwrotnych do NIST. Wszystkie publikacje NIST są dostępne na stronie http://csrc.nist.gov/publications.

Spis treści

Spis ilustracji

PODSUMOWANIE

We współczesnym świecie, w którym wiele kluczowych obszarów większości organizacji jest uzależnionych od technologii informacyjnych, możliwości w zakresie zarządzania tą technologią oraz zapewnienia poufności, integralności i dostępności informacji nabiera krytycznego znaczenia. Projektując architekturę korporacyjną i odpowiadającą jej architekturę bezpieczeństwa, organizacja dąży do bezpiecznego zaspokojenia potrzeb infrastruktury IT związanych ze strukturą zarządzania, realizowanymi zadaniami i podstawowymi procesami biznesowymi. Bezpieczeństwo informacji to dynamiczny proces, który wymaga skutecznego i proaktywnego zarządzania, aby umożliwić organizacji identyfikację oraz reagowanie na nowe podatności i zagrożenia oraz stale zmieniającą się architekturę korporacyjną i środowisko operacyjne organizacji.

Opracowane przez NIST ramy zarządzania ryzykiem (*ang. Risk Management Framework – RMF*)[3] opisują zdyscyplinowany i ustrukturyzowany proces, który integruje bezpieczeństwo informacji i działania dot. zarządzania ryzykiem z cyklem życia systemu. Nieustanne monitorowanie jest kluczową częścią procesu zarządzania ryzykiem. Ponadto ogólna architektura bezpieczeństwa organizacji i towarzyszący jej program bezpieczeństwa winny być monitorowane w celu zapewnienia, że operacje w całej organizacji charakteryzują się akceptowalnym poziomem ryzyka, nawet w obliczu wszelkich zmian. Bieżące, istotne i dokładne informacje mają kluczowe znaczenie, zwłaszcza gdy zasoby są ograniczone, a organizacje muszą ustalać priorytety swoich działań.

> Strategia ciągłego monitorowania bezpieczeństwa informacji (*ang. Information security continuous monitoring - ISCM*) zakłada utrzymywanie ciągłej świadomości bezpieczeństwa informacji, podatności w zabezpieczeniach i zagrożeń w celu podejmowania decyzji dotyczących zarządzania ryzykiem w organizacji.

[3] Dokument NIST Special Publication (SP) 800-37 z późniejszymi zmianami, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Wersja polskojęzyczna publikacji, patrz: NSC 800-37.

Wszystkie działania oraz procesy mające na celu wspieranie ciągłego monitorowania bezpieczeństwa informacji w całej organizacji rozpoczyna się od zdefiniowania przez kierownictwo kompleksowej strategii ISCM obejmującej technologię, procesy, procedury, środowiska operacyjne i pracowników. Strategia ta:

- Opiera się na jasnym zrozumieniu tolerancji ryzyka organizacyjnego i pomaga przedstawicielom organizacji w ustalaniu priorytetów i zarządzaniu ryzykiem w sposób spójny dla całej organizacji.
- Obejmuje wskaźniki, które pozwalają na określanie stanu bezpieczeństwa na wszystkich szczeblach organizacyjnych.
- Zapewnia nieustającą skuteczność wszystkich zabezpieczeń.
- Umożliwia weryfikację zgodności z wymogami bezpieczeństwa informacji wynikającymi z misji organizacji oraz jej pionów biznesowych, przepisów prawa, dyrektyw, rozporządzeń, zasad(polityk) oraz norm i wytycznych.
- Opiera się na wiedzy i informacjach wszystkich pracowników IT organizacji i pomaga zapewnić wgląd w bezpieczeństwo wszystkich zasobów.
- Zapewnia wiedzę i kontrolę nad zmianami w systemach organizacyjnych i środowiskach operacyjnych.
- Zapewnia ciągłą świadomość podatności i zagrożeń.

Program ciągłego monitorowania bezpieczeństwa informacji powinien zostać ustanowiony w celu gromadzenia informacji zgodnie z wcześniej ustalonymi wskaźnikami, w oparciu o informacje łatwo dostępne częściowo dzięki wdrożonym środkom bezpieczeństwa. Osoby odpowiedzialne w organizacji gromadzą i analizują dane regularnie i tak często, jak to konieczne, aby zarządzać ryzykiem odpowiednio dla każdego szczebla organizacji. Proces ten obejmuje całą organizację, od kierownictwa wyższego szczebla odpowiedzialnego za zarządzanie i ustalanie strategii, aż po osoby opracowujące, wdrażające i obsługujące poszczególne systemy wspierające podstawowe misje i procesy biznesowe organizacji. Na tej podstawie podejmowane są decyzje dotyczące tego, czy należy wdrożyć działania łagodzące, czy też odrzucić, przenieść lub zaakceptować ryzyko.

Architektury bezpieczeństwa organizacji, operacyjne możliwości w zakresie bezpieczeństwa i procesy monitorowania będą z czasem ulepszane i udoskonalane, by umożliwić lepsze reagowanie na dynamiczne zmiany w zakresie zagrożeń i podatności. Strategia i program ciągłego monitorowania bezpieczeństwa informacji organizacji są rutynowo sprawdzane pod kątem użyteczności i aktualności, a w razie potrzeby powinny być korygowane w celu zapewnienia dostępności zasobów i świadomości podatności. Umożliwia to zapewnianie bezpieczeństwa infrastruktury informacyjnej organizacji w oparciu o dane i zwiększa jej odporność.

Monitorowanie całej organizacji nie może być skutecznie realizowane jedynie za pomocą ręcznych lub wyłącznie zautomatyzowanych procesów. W obszarach, w których stosowane są procesy ręczne, powinny one być powtarzalne i weryfikowalne, aby umożliwić ich spójne wdrożenie. Zautomatyzowane procesy, w tym wykorzystanie zautomatyzowanych narzędzi wsparcia (na przykład narzędzi do skanowania podatności bądź urządzeń do skanowania sieci) może sprawić, że proces ciągłego monitorowania będzie bardziej efektywny kosztowo, spójny i wydajny.

Wiele technicznych środków bezpieczeństwa opisanych w publikacji specjalnej NIST [NIST Special Publication (SP)] nr 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*[4] z późniejszymi zmianami, to dobre propozycje umożliwiające monitorowanie przy pomocy zautomatyzowanych narzędzi i technik. Monitorowanie w czasie rzeczywistym wdrożonych zabezpieczeń technicznych za pomocą zautomatyzowanych narzędzi może zapewnić organizacji znacznie bardziej dynamiczny wgląd w skuteczność tych środków oraz stan bezpieczeństwa organizacji. Ważne jest, aby pamiętać, że w przypadku każdego kompleksowego programu bezpieczeństwa informacji wszystkie wdrożone środki bezpieczeństwa, w tym zabezpieczenia w zakresie zarządzania oraz zabezpieczenia operacyjne muszą być regularnie oceniane pod kątem skuteczności, nawet jeśli monitorowanie takich zabezpieczeń nie może być zautomatyzowane lub nie jest łatwe do zautomatyzowania.

[4] Patrz: polskojęzyczna publikacja NSC 800-53. Przypis odnosi się do całego dokumentu.

Organizacje podejmują następujące kroki w celu ustanowienia, wdrożenia i utrzymania programu ciągłego monitorowania bezpieczeństwa informacji:

- **Określenie** (*ang. Define*) strategii ciągłego monitorowania bezpieczeństwa informacji.
- **Ustanowienie** (*ang. Establish*) programu ciągłego monitorowania bezpieczeństwa informacji.
- **Wdrożenie** (*ang. Implement*) programu ciągłego monitorowania bezpieczeństwa informacji.
- **Analiza** (*ang. Analyze*) danych i opracowywanie **sprawozdań** (*ang. Report*) z wynikami.
- **Reagowanie** (*ang. Respond*) na ustalenia.
- **Przegląd i aktualizacja** (*ang. Review and Update*) strategii i programu ciągłego monitorowania bezpieczeństwa informacji.

Solidny program ciągłego monitorowania bezpieczeństwa informacji umożliwia zatem organizacjom przejście od zarządzania ryzykiem opartego na zgodności do zarządzania ryzykiem opartego na danych, zapewniając im dostęp do informacji niezbędnych w celu podejmowania decyzji dotyczących reagowania na ryzyko, informacji o stanie bezpieczeństwa i ciągły wgląd w skuteczność środków bezpieczeństwa.

ROZDZIAŁ PIERWSZY

1 WPROWADZENIE

Strategia ciągłego monitorowania bezpieczeństwa informacji (ISCM) zakłada utrzymywanie ciągłej świadomości bezpieczeństwa informacji, wykrywania i usuwania podatności w zabezpieczeniach i zagrożeń w celu podejmowania decyzji dotyczących zarządzania ryzykiem w organizacji[5]. Niniejsza publikacja jest poświęcona w szczególności ocenie i analizie skuteczności zabezpieczeń oraz stanu bezpieczeństwa organizacji zgodnie z poziomem ryzyka tolerowanego przez dany podmiot. Skuteczność zabezpieczeń jest mierzona z punktu widzenia poprawności ich wdrożenia i tego, w jakim stopniu wdrożone zabezpieczenia spełniają potrzeby organizacyjne zgodnie z poziomem tolerowanego ryzyka, to znaczy czy dane zabezpieczenie zostało wdrożone zgodnie z planem bezpieczeństwa w celu przeciwdziałania zagrożeniom i czy plan bezpieczeństwa jest stosowny do okoliczności)[6]. Stan bezpieczeństwa organizacji jest określany przy użyciu wskaźników ustalonych przez organizację w celu jak najlepszego odzwierciedlenia stanu bezpieczeństwa informacji i systemów informacyjnych organizacji, a także odporności organizacji na znane zagrożenia. Wymaga to:

- Utrzymywanie świadomości sytuacyjnej dotyczącej wszystkich systemów działających w ramach całej organizacji.
- Aktualizacja wiedzy na temat zagrożeń i działań związanych z zagrożeniami.
- Poddawanie ocenie wszystkich zabezpieczeń.

---

[5] Terminy „ciągły” oraz „trwający” użyte w tym kontekście oznaczają, że zabezpieczenia i ryzyka organizacyjne są oceniane i analizowane z częstotliwością pozwalającą na wspieranie decyzji dotyczących bezpieczeństwa opartych na ryzyku w celu odpowiedniej ochrony informacji organizacji. Gromadzenie danych, niezależnie od częstotliwości, odbywa się w ustalonych odstępach czasu.

[6] Dokument NSC 800-53A z późniejszymi zmianami, definiuje skuteczność zabezpieczeń jako „zasięg, w jakim zabezpieczenia są wykonywane prawidłowo, działają zgodnie z przeznaczeniem i przynoszą pożądany rezultat w odniesieniu do spełnienia wymogów bezpieczeństwa i ochrony prywatności w systemie i organizacji”.

- Zbieranie, zestawianie i analizowanie informacji związanych z bezpieczeństwem.
- Zapewnienie skutecznego przepływu informacji na temat stanu bezpieczeństwa na wszystkich szczeblach organizacji.
- Aktywne zarządzanie ryzykiem przez przedstawicieli organizacji.

Komunikacja ze wszystkimi interesariuszami jest kluczowa w procesie opracowywania strategii i wdrażania programu. Niniejszy dokument opiera się na koncepcjach monitorowania opisanych po raz pierwszy na łamach dokumentu NIST SP 800-37[7] Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*: *A Security Life Cycle Approach*. Program ciągłego monitorowania bezpieczeństwa informacji (ISCM) pozwala zapewnić, że wdrożone mechanizmy i środki bezpieczeństwa spełniają skutecznie swoją rolę, a operacje realizowane są w ramach określonych poziomów tolerowanego ryzyka organizacyjnego pomimo nieuniknionych zmian zachodzących w czasie. W przypadkach, gdy środki bezpieczeństwa zostaną uznane za niewystarczające, programy ciągłego monitorowania bezpieczeństwa informacji ułatwiają podjęcie działań w zakresie bezpieczeństwa w oparciu o ryzyko.

Strategia ciągłego monitorowania bezpieczeństwa informacji jest ważna z punktu widzenia kontekstu szerszych potrzeb, celów lub strategii organizacyjnych, a także jako część szerszej strategii zarządzania ryzykiem, umożliwiając niezwłoczne podjęcie działań, a także przeprowadzenie oceny oraz reagowanie na nowe zagrożenia bezpieczeństwa. Informacje zebrane w ramach programu ciągłego monitorowania bezpieczeństwa informacji wspierają bieżące decyzje dotyczące autoryzacji[8].

Strategia ciągłego monitorowania bezpieczeństwa informacji, która stanowi kluczowy element ram zarządzania ryzykiem w organizacji, zapewnia jej kadrom kierowniczym dostęp do informacji związanych z bezpieczeństwem na żądanie, umożliwiając sprawne

[7] Patrz: polskojęzyczna publikacja NSC 800-37. Przypis odnosi się do całego dokumentu.

[8] Dla zainteresowanych: więcej informacji na temat ciągłej autoryzacji znajduje się w pytaniu nr 28 w dokumencie OMB Memoranda M-11-33 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf).

i niezwłoczne podejmowanie decyzji dotyczących zarządzania ryzykiem, w tym decyzji dotyczących autoryzacji. Pozwala także na częste aktualizacje planów bezpieczeństwa, sprawozdań z oceny bezpieczeństwa, planów działania i kamieni milowych, inwentaryzacji sprzętu i oprogramowania oraz innych informacji systemowych. Ciągłe monitorowanie bezpieczeństwa informacji jest najskuteczniejsze, gdy w miarę możliwości do gromadzenia danych i raportowania wykorzystywane są zautomatyzowane mechanizmy. Skuteczność jest jeszcze większa, gdy dane wyjściowe są sformatowane w celu dostarczenia informacji, które są konkretne, wymierne, przydatne, istotne i aktualne. Choć niniejszy dokument zachęca do korzystania z automatyzacji, autorzy mają świadomość, że wiele aspektów programów ciągłego monitorowania bezpieczeństwa informacji jest trudne do zautomatyzowania.

1.1. INFORMACJE OGÓLNE

Koncepcja monitorowania bezpieczeństwa systemów informacyjnych jest od dawna uznawana za dobrą praktykę zarządzania. W 1997 roku w załączniku III do okólnika A-130 Biura ds. Zarządzania i Budżetu (*ang. Office of Management and Budget - OMB*)[9] znalazł się zapis zobowiązujący organizacje do przeprowadzenia *przeglądu* zabezpieczeń swoich systemów informacyjnych i zapewnienia, że zmiany w systemach nie mają znaczącego wpływu na bezpieczeństwo, plany bezpieczeństwa są aktualne i skuteczne, a zabezpieczenia nadal działają zgodnie z przeznaczeniem.

Ustawa rządu federalnego dotycząca zarządzania bezpieczeństwem informacji (*ang. Federal Information Security Management Act – FISMA*) z 2002 roku dodatkowo podkreśliła znaczenie ciągłego monitorowania bezpieczeństwa systemów informacyjnych, wymagając od organizacji przeprowadzania ocen zabezpieczeń z częstotliwością odpowiednią do ryzyka, ale nie rzadziej niż raz w roku.

Wydane przez OMB memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (Instrukcje*

[9] Dla zainteresowanych: Okólnik OMB A-130 jest dostępny pod adresem http://www.whitehouse.gov/omb/circulars a130 a130trans4.

dotyczące sprawozdań za rok 2011 dotyczące federalnej ustawy o zarządzaniu bezpieczeństwem informacji i zarządzaniu prywatnością agencji)[10] zawiera instrukcje dotyczące corocznego składania raportów wymaganych przez ustawę FISMA i kładzie nacisk na ciągłe monitorowanie stanu bezpieczeństwa systemów informacyjnych z częstotliwością wystarczającą do podejmowania bieżących decyzji opartych na ryzyku.

Narzędzia wspierające zautomatyzowane monitorowanie niektórych aspektów systemów informacyjnych stały się skutecznym rozwiązaniem zarówno do gromadzenia danych, jak i ich analizy. Prostota użytkowania, dostępność i możliwość zastosowania tych rozwiązań do produktów różnych producentów i dostawców pomagają zapewnić, że narzędzia monitorujące mogą być łatwo wykorzystywane w celu wspierania podejmowania decyzji opartych na ryzyku w czasie zbliżonym do rzeczywistego.

1.2. POWIĄZANIA Z INNYMI PUBLIKACJAMI

NIST SP 800-39[11], *Managing Information Security Risk: Organization, Mission, and Information System View*, opisuje trzy kluczowe działania w zakresie ciągłego monitorowania bezpieczeństwa informacji w całej organizacji – monitorowanie skuteczności, monitorowanie zmian w systemach i środowiskach operacyjnych oraz monitorowanie zgodności. Dokument NIST SP 800-37 opisuje monitorowanie zabezpieczeń na poziomie systemu (etap 6 ram zarządzania ryzykiem), a także uwzględnia perspektywę całej organizacji, integrację z cyklem życia systemu oraz wsparcie dla ciągłych autoryzacji. Koncepcje przedstawione w dokumentach NIST SP 800-39 i NIST SP 800-37 zostały rozszerzone w celu opracowania wytycznych pozwalających na opracowanie strategii ciągłego monitorowania bezpieczeństwa informacji i wdrożenia programu ISCM.

Poziomy opisane w niniejszym dokumencie stanowią odzwierciedlenie kategorii opisanych w dokumentach NIST SP 800-37 i NIST SP 800-39, gdzie poziom pierwszy

[10] Dla zainteresowanych: Memorandum OMB M-11-33 jest dostępne pod adresem http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf.

[11] Patrz: polskojęzyczna publikacja NSC 800-39. Przypis odnosi się do całego dokumentu.

opisuje szczebel całej organizacji, poziom drugi dotyczy misji oraz procesów biznesowych, z kolei poziom trzeci obejmuje systemy informacyjne. W ramach dokumentu NIST SP 800-39 poziomy te są wykorzystywane w celu zarządzania ryzykiem z punktu widzenia różnych perspektyw w ramach organizacji. W niniejszym dokumencie poziomy te służą omawianiu perspektyw dotyczących ciągłego monitorowania bezpieczeństwa informacji dla każdego z nich. Polityki, procedury i obowiązki w zakresie ciągłego monitorowania bezpieczeństwa informacji obejmujące całą organizację są uwzględnione w opisach dotyczących poziomów organizacji, misji i procesów biznesowych, a także systemów informacyjnych. Automatyzacja powinna być wykorzystywana wszędzie tam, gdzie jest to możliwe. Z kolei ręczne (np. proceduralne) metody monitorowania powinny być wykorzystywane wyłącznie w kontekstach, w których zastosowanie automatyzacji nie jest praktyczne lub jest niemożliwe.

Program ciągłego monitorowania bezpieczeństwa informacji będzie podlegał zmianom wraz z upływem czasu oraz wraz z jego dopracowywaniem, a także dostępnością dodatkowych narzędzi i zasobów, nowym możliwościom dokonywania pomiarów oraz automatyzacji, a także wdrażania zmian w celu zapewnienia ciągłej poprawy stanu bezpieczeństwa organizacji i jej programu bezpieczeństwa. Strategia monitorowania jest regularnie weryfikowana pod kątem adekwatności i dokładności w zakresie tolerowania ryzyka przez organizację, poprawności pomiarów, użyteczności wskaźników i skuteczności we wspieraniu decyzji dotyczących zarządzania ryzykiem.

1.3. CEL

Celem niniejszych rekomendacji jest pomoc organizacjom w opracowaniu strategii ciągłego monitorowania bezpieczeństwa informacji (ISCM) i wdrożeniu programu ISCM, który zapewnia świadomość zagrożeń i słabych punktów (podatności), widoczność zasobów organizacji oraz skuteczność wdrożonych środków bezpieczeństwa. Strategia i program ciągłego monitorowania bezpieczeństwa informacji dają pewność, że zaplanowane i wdrożone środki bezpieczeństwa są

dostosowane do poziomu ryzyka tolerowanego przez organizację, a także zapewniają dostęp do informacji potrzebnych do niezwłocznego reagowania na ryzyko.

1.4. ODBIORCY DOCELOWI

Niniejsza publikacja jest przeznaczona dla osób[12] uczestniczących w procesach projektowania, opracowywania, wdrażania, obsługi, utrzymania, a także utylizacji systemów informacyjnych w organizacjach, w tym:

- Osób odpowiedzialnych za misje lub procesy biznesowe w ramach organizacji lub obowiązki powiernicze (np. kierowników jednostek organizacyjnych, dyrektorów organizacji).
- Osób odpowiedzialnych za rozwój i integrację systemów informacyjnych (w tym menedżerów programów, twórców komponentów systemów informacyjnych, twórców systemów informacyjnych, integratorów systemów informacyjnych, architektów systemów korporacyjnych, architektów systemów bezpieczeństwa informacji).
- Osób odpowiedzialnych za zarządzanie systemami informacyjnymi bądź sprawujących nadzór nad ich bezpieczeństwem (np. kierowników wyższego szczebla, kierowników ds. ryzyka, osób autoryzujących, CIO, CISO[13]);
- Osób odpowiedzialnych za ocenę i monitorowanie systemów i zabezpieczeń (np. ewaluatorów systemów, członków zespołów oceniających, niezależnych weryfikatorów i walidatorów, audytorów, osób odpowiedzialnych za systemy informacyjne); oraz
- Osób odpowiedzialnych za zapewnianie bezpieczeństwa informacji i obowiązki operacyjne (np. osób odpowiedzialnych za systemy informacyjne, dostawców

[12] Definicje ról organizacyjnych – patrz: NSC 800-37, NSC 7298.

[13] Na poziomie *jednostki organizacyjnej* osoby zatrudnione na tym stanowisku wykonują pracę kluczowej osoby odpowiedzialnej za bezpieczeństwo informacji (*ang. Senior Agency Information Security Officer - SAISO*). Organizacje mogą również określać to stanowisko mianem *Chief Information Security Officer – CISO*.

zabezpieczeń wspólnych, właścicieli informacji, osób odpowiedzialnych za misje lub procesy biznesowe, architektów bezpieczeństwa informacji, inżynierów oraz osób ds. bezpieczeństwa systemów informacyjnych).

1.5. ORGANIZACJA PUBLIKACJI

Pozostała część niniejszej publikacji została zorganizowana w następujący sposób:

- Rozdział 2 opisuje podstawy bieżącego monitorowania bezpieczeństwa informacji w celu wsparcia zarządzania ryzykiem;
- Rozdział 3 opisuje proces ciągłego monitorowania bezpieczeństwa informacji, w tym rekomendacje dotyczące wdrażania;
- Załączniki zawierają dodatkowe informacje dotyczące ciągłego monitorowania bezpieczeństwa informacji, w tym: (A) źródła ogólne (referencje); (B) słownik terminów; (C) glosariusz akronimów i skrótów; oraz (D) opisy technologii pozwalających na wdrożenie strategii ciągłego monitorowania bezpieczeństwa informacji.

ROZDZIAŁ DRUGI

2. PODSTAWY

BIEŻĄCE MONITOROWANIE WSPIERAJĄCE ZARZĄDZANIE RYZYKIEM

W niniejszym rozdziale opisano podstawowe koncepcje związane z ciągłym monitorowaniem bezpieczeństwa informacji w całej organizacji i stosowaniem zasad ISCM w celu wspierania decyzji dotyczących zarządzania ryzykiem organizacyjnym, w tym decyzji dotyczących reakcji na ryzyko, bieżących decyzji dotyczących autoryzacji systemu, planów i etapów działania (kamieni milowych), a także decyzji dotyczących zasobów i ustalania priorytetów oraz innych. Aby skutecznie stawić czoła coraz większym wyzwaniom związanym z bezpieczeństwem, dobrze zaprojektowana strategia ciągłego monitorowania bezpieczeństwa informacji obejmuje monitorowanie i ocenę zabezpieczeń pod kątem skuteczności oraz monitorowanie stanu bezpieczeństwa[14]. Obejmuje również procesy mające na celu zapewnienie, że działania naprawcze są podejmowane zgodnie z ustaleniami i akceptowanym poziomem ryzyka tolerowanego przez organizację, a także w celu zapewnienia, że wspomniane działania przynoszą zamierzone skutki.

Proces wdrażania ciągłego monitorowania bezpieczeństwa informacji opisany w rozdziale trzecim obejmuje następujące etapy:

- **Określenie** (*ang. Define*) strategii ciągłego monitorowania bezpieczeństwa informacji.
- **Ustanowienie** (*ang. Establish*) programu ciągłego monitorowania bezpieczeństwa informacji.
- **Wdrożenie** (*ang. Implement*) programu ciągłego monitorowania bezpieczeństwa informacji.
- **Analiza** (*ang. Analyze*) wyników i opracowywanie **sprawozdań** (*ang. Report*).

[14] Organizacje wdrażają procesy zarządzania bezpieczeństwem organizacyjnym i wskaźniki, które pozwalają na pomiar tych procesów, a tym samym stanu bezpieczeństwa organizacyjnego. Niektóre z tych procesów bezpieczeństwa są zgodne z poszczególnymi zabezpieczeniami, z kolei inne są zgodne z komponentami lub zbiorami zabezpieczeń. Omówienie wskaźników znajduje się w rozdziale 3.2.1 oraz w dokumencie NIST SP 800-55, *Performance Measurement Guide for Information Security*, z późniejszymi zmianami.

- **Reagowanie** (*ang. Respond*) na ustalenia.
- **Przegląd** i **aktualizacja** (*ang. Review and Update*) strategii i programu ciągłego monitorowania bezpieczeństwa informacji.

Strategie ciągłego monitorowania bezpieczeństwa informacji nieustannie zmieniają się zgodnie z czynnikami wpływającymi na podejmowanie decyzji opartych na ryzyku i wymaganiami dotyczącymi informacji. Wymagania te mogą pochodzić z dowolnego szczebla organizacji.

Organizacje realizują działania ISCM w oparciu o wymagania osób odpowiedzialnych za utrzymanie ciągłej kontroli stanu bezpieczeństwa organizacji w ramach tolerancji ryzyka. Wdrożenie jest standaryzowane w całej organizacji w największym możliwym zakresie, aby zminimalizować wykorzystanie zasobów (np. środków przeznaczonych na zakup narzędzi/aplikacji, połączeń danych, zasad/procedur/szablonów obejmujących całą organizację itp.) oraz zmaksymalizować możliwość wykorzystania informacji dotyczących bezpieczeństwa. Po przeanalizowaniu uzyskane informacje wpływają na poszczególne procesy wykorzystywane w celu zarządzania stanem bezpieczeństwa organizacji i ogólnym ryzykiem. ISCM pomaga zapewnić świadomość sytuacyjną dotyczącą bezpieczeństwa systemów organizacji w oparciu o informacje zebrane od pracowników, a także z procesów, składników technologicznych, elementów środowiska, a także umożliwia reagowanie na zmiany sytuacji.

ISCM to taktyka w ramach szerszej strategii zarządzania ryzykiem w całej organizacji[15]. Organizacje zwiększają świadomość sytuacyjną poprzez lepsze możliwości w zakresie monitorowania, a następnie zwiększają wgląd w procesy wykorzystywane w celu zarządzania bezpieczeństwem organizacyjnym i kontrolę nad nimi. Zwiększony wgląd w procesy bezpieczeństwa i lepsza kontrola z kolei zwiększają świadomość sytuacyjną. Z tego powodu proces wdrażania ISCM jest rekurencyjny. ISCM wpływa na zróżnicowane procesy bezpieczeństwa w organizacji i związane z nimi wymagania dotyczące informacji związanych z bezpieczeństwem, a także jest kształtowany przez te procesy. Za ilustrację niech posłuży poniższy przykład:

[15] W szerszym kontekście zarządzania ryzykiem w całej organizacji strategia ciągłego monitorowania bezpieczeństwa informacji została omówiona w dokumencie NIST SP 800-39.

Informacje związane z bezpieczeństwem odnoszące się do inwentaryzacji elementów systemu są wykorzystywane do określenia zgodności z wymogami zabezpieczenia CM-8 *Inwentaryzacja komponentów systemu*[16]. Informacje są analizowane w celu ustalenia, czy dane zabezpieczenie jest skuteczne (tzn. czy inwentaryzacja jest dokładna). Jeśli okaże się, że inwentaryzacja jest niedokładna, należy przeprowadzić analizę w celu ustalenia podstawowych przyczyn niedokładności – powodem może być na przykład zignorowanie procesu przyłączania komponentów do sieci, nieaktualny proces, nieprawidłowe działanie narzędzi do zarządzania zasobami, bądź atak na organizację. W oparciu o analizę podejmowane są odpowiednie działania (np. osoby odpowiedzialne aktualizują inwentaryzację i stosowne procesy organizacyjne, szkolą pracowników, odłączają niedziałające urządzenia itp.) Co więcej, informacje związane z bezpieczeństwem odnoszące się do inwentaryzacji komponentów systemu mogą być wykorzystywane w ramach wstępnie określonych wskaźników. Dokładniejsze inwentaryzacje komponentów systemu zapewniają lepszą skuteczność innych działań w zakresie bezpieczeństwa, takich jak zarządzanie poprawkami i zarządzanie podatnościami.

Ten przykład ilustruje, w jaki sposób dane zebrane podczas oceny zabezpieczeń są wykorzystywane do obliczania wskaźników i gromadzenia danych wejściowych na potrzeby różnych procesów organizacyjnych. Pokazuje również, że wykrycie problemu może uruchomić ocenę pojedynczych lub wielu zabezpieczeń w całej organizacji, aktualizacje stosownych informacji związanych z bezpieczeństwem, modyfikacje planu programu bezpieczeństwa organizacji i procesów bezpieczeństwa oraz poprawę zgodności z programem bezpieczeństwa i odpowiednim planem bezpieczeństwa systemu. Efektem końcowym jest lepsze zarządzanie ryzykiem w całej organizacji i ciągłe doskonalenie ograniczone jedynie szybkością, z jaką organizacja może gromadzić informacje i reagować na ustalenia.

[16] CM-8 to zabezpieczenie z kategorii zarządzania konfiguracją, wymienione w dokumencie NIST SP 800-53.

2.1. SPOJRZENIE NA STRATEGIĘ CIĄGŁEGO MONITOROWANIA BEZPIECZEŃSTWA INFORMACJI Z PERSPEKTYWY CAŁEJ ORGANIZACJI

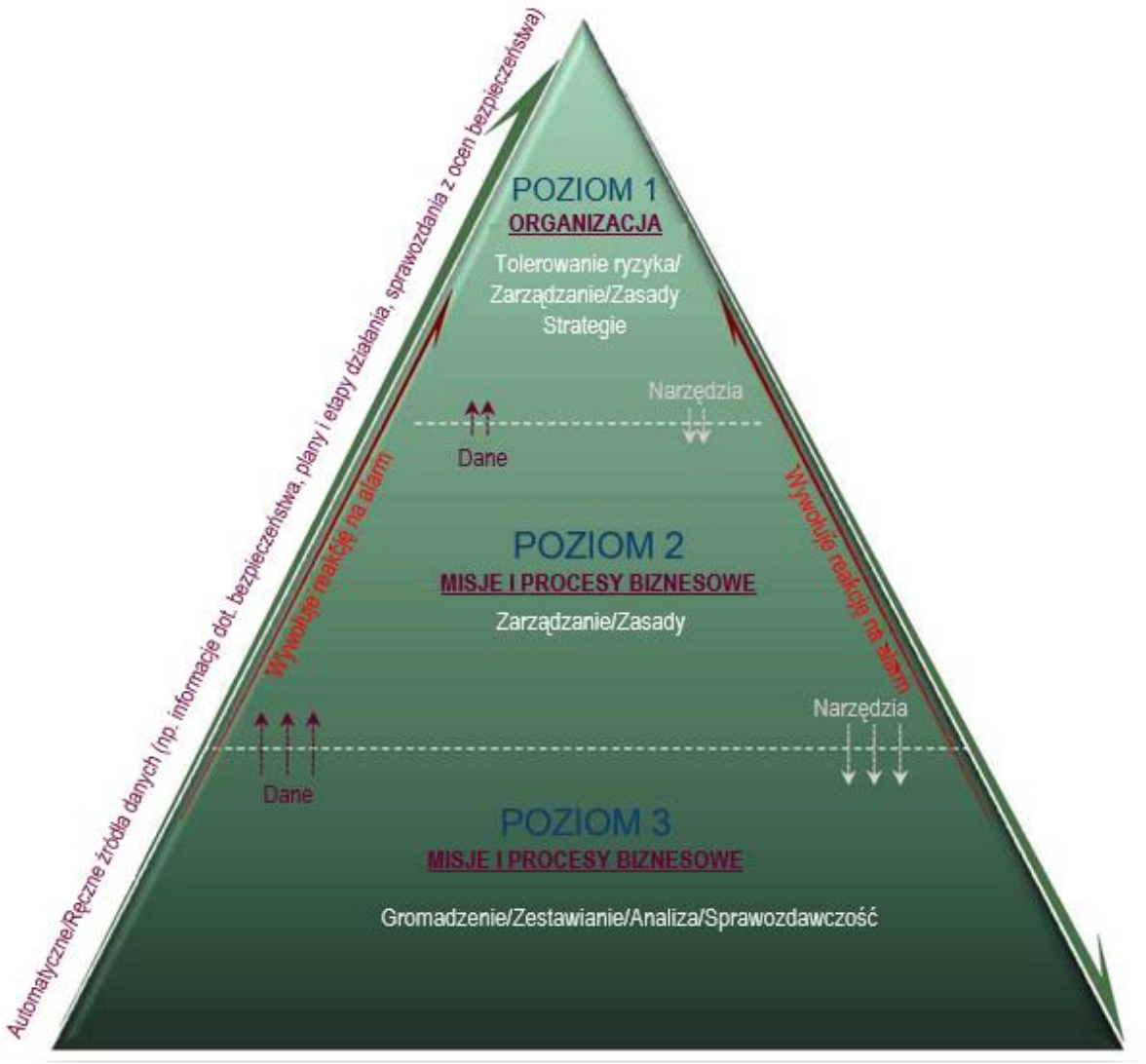
Uzyskanie stałego dostępu do aktualnych informacji na temat zagrożeń dla bezpieczeństwa informacji w całej organizacji jest złożonym, wieloaspektowym przedsięwzięciem. Wymaga to zaangażowania całej organizacji, od kierownictwa wyższego szczebla odpowiedzialnego za zarządzanie i ustalanie strategii, aż po osoby opracowujące, wdrażające i obsługujące poszczególne systemy wspierające podstawowe misje i procesy biznesowe organizacji. Rysunek 2-1 ilustruje wielopoziomowe podejście do ciągłego monitorowania bezpieczeństwa informacji w całej organizacji w celu wsparcia zarządzania ryzykiem. Zarządzanie na poziomie 1, cele zarządzania ryzykiem i tolerowanie ryzyka w organizacji stanowią podstawę strategii ciągłego monitorowania bezpieczeństwa informacji. Poziom tolerowanego ryzyka ustalony przez kierownictwo wyższego szczebla bądź liderów w ramach zarządzania ryzykiem[17] wpływa na zasady, procedury i działania wdrożeniowe dotyczące ISCM na wszystkich poziomach. Gromadzenie danych odbywa się głównie na poziomie systemów informacyjnych. Wskaźniki są zaprojektowane tak, aby przedstawiać informacje w kontekście, który ma znaczenie dla poszczególnych poziomów. Na przykład dane dotyczące ciągłego monitorowania bezpieczeństwa informacji zebrane na poziomie 3 mogą być zestawiane w celu określenia stanu bezpieczeństwa lub oceny ryzyka dla pojedynczego systemu, zbioru systemów, głównego procesu biznesowego lub całej organizacji. Zasady, procedury i narzędzia mogą być ustanawiane na dowolnym poziomie; jednak gdy są ustanawiane na poziomie 1 lub 2, ułatwiają spójne wdrażanie strategii ciągłego monitorowania bezpieczeństwa informacji w całej organizacji i lepiej wspierają ponowne wykorzystanie danych i rozsądne wykorzystanie zasobów.

[17] Omówienie ról i obowiązków w zakresie zarządzania ryzykiem znajduje się w rozdziale 2.4.

Gromadzenie danych, analizy i sprawozdania powinny być w miarę możliwości zautomatyzowane[18]. Dzięki zastosowaniu automatyzacji możliwe jest monitorowanie większej liczby wskaźników bezpieczeństwa przy wykorzystaniu mniejszej ilości zasobów, zwiększenie częstotliwości kontroli, gromadzenie większych próbek niż jest to możliwe przy użyciu procesów ręcznych[19] oraz zapewnienie większej spójności i niezawodności niż w przypadku procesów ręcznych. Organizacje regularnie dokonują przeglądu strategii ciągłego monitorowania bezpieczeństwa informacji, aby upewnić się, że wybrane wskaźniki pozostają istotne, znaczące, wymierne i służą do wspierania decyzji dotyczących zarządzania ryzykiem podejmowanych przez przedstawicieli organizacji na wszystkich szczeblach.

[18] Należy zachować ostrożność przy określaniu najlepszego sposobu wykorzystania informacji związanych z bezpieczeństwem z poszczególnych systemów informacyjnych oraz obliczania wskaźników dotyczących bezpieczeństwa i ryzyka w organizacji. Pulpity nawigacyjne i wskaźniki, zaprojektowane w celu zapewnienia świadomości sytuacyjnej w zakresie bezpieczeństwa i ryzyka, mogą zapewnić fałszywe poczucie bezpieczeństwa, jeśli są używane bez zapewnienia użyteczności i istotności wskaźników.

[19] Jeśli organizacja nie ma zasobów lub infrastruktury niezbędnej do oceny każdego istotnego obiektu w ramach swojej infrastruktury informacyjnej, próbkowanie jest podejściem, które może być przydatne w zmniejszaniu poziomu wysiłku związanego z ciągłym monitorowaniem. Dodatkowe informacje znajdują się w rozdziale 3.1.4.



Rysunek 2-1. Strategia ciągłego monitorowania bezpieczeństwa informacji w całej organizacji

Obejmujące całą organizację podejście do ciągłego monitorowania bezpieczeństwa informacji i systemów informacyjnych wspiera podejmowanie decyzji związanych z ryzykiem na poziomie *organizacji* (poziomie 1), na poziomie *misji lub procesów biznesowych* (poziomie 2) oraz na poziomie *systemów informacyjnych* (poziomie 3)[20].

[20] Publikacja specjalna NIST 800-39 z późniejszymi zmianami zawiera wskazówki dotyczące kompleksowego podejścia do zarządzania ryzykiem.

2.1.1. POZIOM 1 – ORGANIZACYJNY

Działania związane z zarządzaniem ryzykiem na poziomie 1 dotyczą zasad zarządzania bezpieczeństwem informacji na wysokim szczeblu, ponieważ odnoszą się do ryzyka dla organizacji jako całości, jej podstawowych misji i funkcji biznesowych. Na tym poziomie kryteria strategii ciągłego monitorowania bezpieczeństwa informacji są określane na podstawie strategii zarządzania ryzykiem organizacji, między innymi na podstawie tego, w jaki sposób organizacja planuje oceniać, reagować i monitorować ryzyko oraz zapewniać nadzór wymagany do zagwarantowania skuteczności strategii zarządzania ryzykiem. Środki bezpieczeństwa, stan bezpieczeństwa i inne wskaźniki zdefiniowane i monitorowane przez osoby odpowiedzialne na tym poziomie mają na celu dostarczanie informacji niezbędnych do podejmowania decyzji w zakresie zarządzania ryzykiem w celu wsparcia procesów zarządzania. Wskaźniki wykorzystywane na poziomie 1 są opracowywane w celu wspierania decyzji dotyczących zarządzania organizacją, jej podstawowymi misjami oraz funkcjami biznesowymi. Wskaźniki poziomu 1 mogą być obliczane na podstawie informacji związanych z bezpieczeństwem pochodzących z ogólnych, hybrydowych i specyficznych zabezpieczeń systemów. Wskaźniki i częstotliwość, z jaką są monitorowane[21] i uwzględniane w sprawozdaniach, są określone przez wymagania dotyczące utrzymania ryzyka związanego z operacjami w ramach tolerowanego ryzyka. W ramach ogólnej struktury zarządzania ustanowionej przez organizację, strategia zarządzania ryzykiem na poziomie 1 i związane z nią wymagania dotyczące monitorowania są przekazywane poziomom 2 i 3.

2.1.2. POZIOM 2 - MISJA I PROCESY BIZNESOWE

Przedstawiciele organizacji odpowiedzialni za misje jako całość, kluczowe misje lub procesy biznesowe ponoszą również odpowiedzialność za nadzorowanie powiązanych działań związanych z zarządzaniem ryzykiem dla tych misji lub procesów. Kryteria poziomu 2 dotyczące ciągłego monitorowania bezpieczeństwa informacji są określone

[21] Monitorowanie wskaźników określonych przez organizację jest określane w tym dokumencie jako monitorowanie stanu bezpieczeństwa.

przez priorytety przypisywane poszczególnym kluczowym misjom i procesom biznesowym w odniesieniu do ogólnych celów i zadań organizacji, rodzajów informacji potrzebnych do pomyślnej realizacji określonej misji lub wykonania procesów biznesowych oraz strategii bezpieczeństwa informacji w całej organizacji. Zabezpieczenia z rodziny programów zarządzania (PM) stanowią przykłady środków bezpieczeństwa poziomu 2. Środki te pozwalają na ustanowienie i realizację programów bezpieczeństwa informacji organizacji.

Zabezpieczenia poziomu 2 są wdrażane w całej organizacji i obejmują wszystkie systemy informacyjne. Mogą one być monitorowane na poziomach 2 lub 1. Częstotliwość, z jaką środki bezpieczeństwa poziomu 2 są poddawane ocenie, a także monitorowanie stanu bezpieczeństwa lub innych wskaźników, zależy częściowo od celów i priorytetów misji lub procesu biznesowego oraz możliwości dokonywania pomiarów dostępnych w ramach infrastruktury[22]. Dane dotyczące bezpieczeństwa mogą pochodzić z zabezpieczeń wspólnych, hybrydowych i specyficznych dla systemu. Wskaźniki i pulpity nawigacyjne mogą być użyteczne na poziomach 1 i 2 w celu oceny, normalizacji, komunikacji i korelacji znaczących działań monitorujących poniżej poziomu misji oraz procesów biznesowych.

2.1.3. POZIOM 3 - SYSTEMY INFORMACYJNE

Działania w zakresie ciągłego monitorowania bezpieczeństwa informacji na poziomie 3 dotyczą zarządzania ryzykiem z perspektywy *systemu informacyjnego*. Działania te obejmują zapewnienie, że wszystkie środki bezpieczeństwa na poziomie systemu (techniczne, operacyjne i zarządzania) są prawidłowo wdrożone, działają zgodnie z przeznaczeniem, przynoszą pożądane rezultaty w odniesieniu do spełnienia wymogów bezpieczeństwa systemu i pozostają skuteczne pomimo upływu czasu. Działania w zakresie ciągłego monitorowania bezpieczeństwa informacji na poziomie 3 obejmują również ocenę i monitorowanie hybrydowych i wspólnych zabezpieczeń wdrożonych na poziomie systemu. Sprawozdania ze stanu bezpieczeństwa na tym

[22] Wraz ze wzrostem możliwości technicznych i kapitału ludzkiego organizacji, zwiększeniu ulegają także możliwości monitorowania.

poziomie często obejmują między innymi alerty bezpieczeństwa, incydenty bezpieczeństwa i działania związane ze zidentyfikowanymi zagrożeniami[23]. Strategia ciągłego monitorowania bezpieczeństwa informacji dla poziomu 3 gwarantuje także, że informacje związane z bezpieczeństwem przyczyniają się do realizacji wymogów monitorowania dla innych szczebli organizacji. Dane oraz wyniki ocen zabezpieczeń na poziomie systemu (specyficznych dla systemu, hybrydowych lub wspólnych) wraz z powiązanymi raportami o stanie bezpieczeństwa, wspierają decyzje oparte na ryzyku na szczeblu organizacji oraz misji i procesów biznesowych. Informacje są dostosowane do każdego poziomu i dostarczane w sposób, który umożliwia podejmowanie decyzji opartych na ryzyku na wszystkich szczeblach organizacji. Wynikające z nich decyzje wpływają na strategię ciągłego monitorowania bezpieczeństwa informacji na poziomie systemów informacyjnych[24]. Wskaźniki ISCM uzyskane na poziomie systemów informacyjnych mogą być wykorzystywane do oceny i monitorowania ryzyka w całej organizacji, a także podejmowania działań. Bieżące działania monitorujące realizowane na poziomie systemów informacyjnych dostarczają informacji związanych z bezpieczeństwem osobom autoryzującym w celu wsparcia bieżących decyzji dotyczących autoryzacji systemu oraz osobom odpowiedzialnym za zarządzanie ryzykiem w celu wsparcia bieżącego zarządzania ryzykiem organizacyjnym.

Na poziomie 3 działania dotyczące monitorowania stanowiące etap 6 ram zarządzania ryzykiem oraz działania związane ze strategią ciągłego monitorowania bezpieczeństwa informacji są ściśle powiązane. Metody oceny dla wdrożonych zabezpieczeń są takie same, niezależnie od tego, czy oceny są przeprowadzane wyłącznie w celu autoryzacji systemu, czy też w celu umożliwienia szerszego, bardziej kompleksowego ciągłego monitorowania. Kierownicy i pracownicy zajmujący się systemami informacyjnymi przeprowadzają oceny i monitorowanie oraz na bieżąco analizują wyniki. Informacje są

[23] Działania związane z zagrożeniami obejmują złośliwe działania zaobserwowane w sieciach organizacji lub inne anomalie, które wskazują na niepożądane działania. Więcej informacji na temat zagrożeń można znaleźć w dokumencie NIST SP 800-30 (NSC 800-30) z późniejszymi zmianami.

[24] Strategia ciągłego monitorowania dotycząca pojedynczego systemu może również obejmować wskaźniki związane z jego potencjalnym wpływem na inne systemy.

wykorzystywane na poziomach organizacji, misji oraz procesów biznesowych i systemów informacyjnych w celu wsparcia zarządzania ryzykiem. Choć wymagania dotyczące częstotliwości mogą być różne, każdy poziom korzysta z informacji związanych z bezpieczeństwem, które są aktualne i związane z procesami, których dotyczą. Działania związane z etapem 6 ram zarządzania ryzykiem wykonywane w kontekście programu ciągłego monitorowania bezpieczeństwa informacji służą bieżącemu określaniu ryzyka dotyczącego systemu informacyjnego oraz jego akceptację, czyli realizacji etapu 5 ram zarządzania ryzykiem – autoryzacji.

2.2. CIĄGŁA AUTORYZACJA SYSTEMÓW

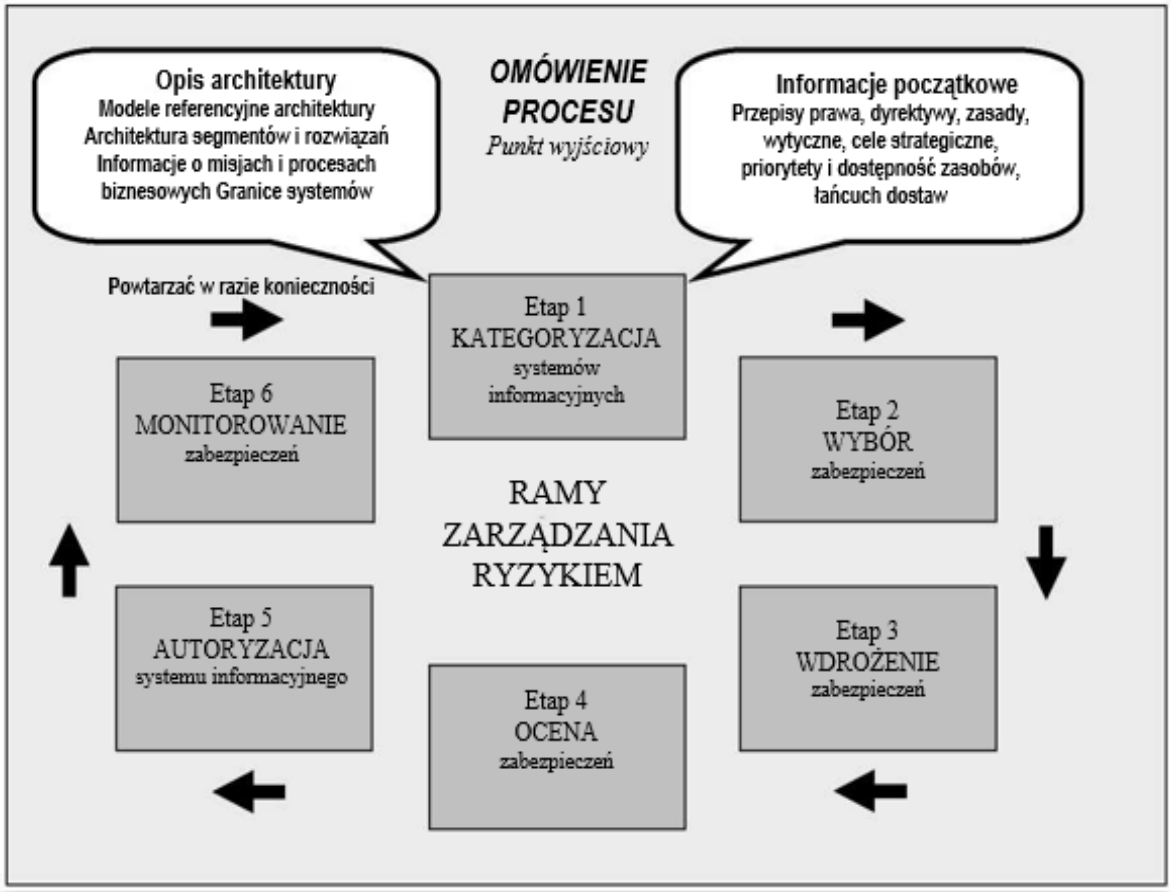
Wstępne upoważnienie do działania opiera się na danych dostępnych w danym momencie, jednak należy pamiętać, że systemy i środowiska eksploatacji ulegają zmianom. Bieżąca ocena skuteczności zabezpieczeń pozwala na przeprowadzanie autoryzacji bezpieczeństwa systemu w czasie w wysoce dynamicznych środowiskach operacyjnych, które charakteryzują zmienne zagrożenia, podatności, technologie, misje oraz procesy biznesowe. Dzięki ciągłemu monitorowaniu bezpieczeństwa informacji, informacje o zagrożeniach lub podatnościach są oceniane niezwłocznie, gdy tylko zostaną udostępnione, co pozwala organizacjom na dostosowanie wymagań bezpieczeństwa lub pojedynczych zabezpieczeń w razie potrzeby w celu utrzymania decyzji dotyczących autoryzacji. Proces uzyskiwania autoryzacji systemu, a także ogólnego zarządzania bezpieczeństwem informacji i ryzykiem związanym z systemem informacyjnym, składa się na ramy zarządzania ryzykiem[25].

Ramy zarządzania ryzykiem, przedstawione na rysunku 2-2, stanowią uporządkowany i ustrukturyzowany proces, który łączy działania związane z bezpieczeństwem systemu informacyjnego i zarządzaniem ryzykiem w cyklu życia systemu. Etap monitorowania (etap 6) ram zarządzania ryzykiem obejmuje interakcje między trzema poziomami, co jest widoczne w przeglądzie strategii ciągłego monitorowania

[25] Upoważnienie do działania może być częściowo zależne od oceny lub monitorowania oraz bieżącej autoryzacji bezpieczeństwa zabezpieczeń wspólnych. Dokument NIST SP 800-37 z późniejszymi zmianami zawiera informacje na temat autoryzacji bezpieczeństwa wspólnych zabezpieczeń.

bezpieczeństwa informacji na rysunku 2-1. Interakcja między poziomami obejmuje dane pochodzące od właścicieli systemów, dostawców zabezpieczeń wspólnych i osób autoryzujących z ocen zabezpieczeń i dotyczące autoryzacji systemu i zabezpieczeń wspólnych na potrzeby zarządzania ryzykiem[26]. Istnieje również proces rozpowszechniania zaktualizowanych informacji związanych z ryzykiem, takich jak dane dotyczące podatności i zagrożeń oraz tolerancji ryzyka organizacyjnego z poziomów 1 i 2, wśród osób autoryzujących i właścicieli systemów informacyjnych. Gdy ramy zarządzania ryzykiem są stosowane w organizacji, która wdrożyła również solidną strategię ciągłego monitorowania bezpieczeństwa informacji, przedstawiciele organizacji mają możliwość uzyskania na żądanie wglądu w stan jej bezpieczeństwa i wpływ każdego systemu na ten stan.

[26] Role i obowiązki przedstawicieli organizacji w ramach programu ciągłego monitorowania omówiono w rozdziale 2.4. Dokument NIST SP 800-37 z późniejszymi zmianami opisuje interakcje związane z zarządzaniem ryzykiem w kontekście ram zarządzania ryzykiem.



Rysunek 2-2. Ramy zarządzania ryzykiem

Wyniki zaprojektowanego w sposób strategiczny i dobrze zarządzanego programu ciągłego monitorowania bezpieczeństwa informacji w całej organizacji mogą być wykorzystywane do utrzymania upoważnienia systemów do działania oraz aktualizacji wymaganych informacji i danych dotyczących systemów (tj. planu bezpieczeństwa systemów wraz ze sprawozdaniami z oceny ryzyka, sprawozdaniami z oceny bezpieczeństwa oraz planów i etapów działania). Narzędzia do zarządzania bezpieczeństwem i raportowania mogą zapewniać funkcje automatyzacji aktualizacji kluczowych informacji potrzebnych do podejmowania bieżących decyzji dotyczących autoryzacji. Strategia ciągłego monitorowania bezpieczeństwa informacji ułatwia również podejmowanie decyzji opartych na ryzyku w odniesieniu do upoważnienia do działania systemów informacyjnych i autoryzacji bezpieczeństwa dla zabezpieczeń wspólnych poprzez dostarczanie na żądanie nowych informacji o zagrożeniach lub podatnościach. Proces oceny zabezpieczeń i określania ryzyka, który zwykle jest

statyczny pomiędzy autoryzacjami, jest w ten sposób przekształcany w dynamiczny proces, który wspomaga natychmiastowe działania w zakresie reagowania na ryzyko i przystępne cenowo, bieżące autoryzacje. Ciągłe monitorowanie zagrożeń, podatności i skuteczności zabezpieczeń zapewnia świadomość sytuacyjną i umożliwia podejmowanie bieżących decyzji autoryzacyjnych opartych na ryzyku. Odpowiednio zaprojektowana strategia i program ciągłego monitorowania bezpieczeństwa informacji pozwala na przeprowadzanie bieżących autoryzacji, w tym pojedynczych, łącznych i wspólnych autoryzacji[27].

Strategia ciągłego monitorowania bezpieczeństwa informacji wspierająca bieżącą ocenę i autoryzację może potencjalnie wymagać dużych zasobów i być niezwykle czasochłonna. Gromadzenie informacji związanych z bezpieczeństwem i ciągła ocena każdego aspektu wszystkich zabezpieczeń wdrożonych w organizacji jest podejściem niepraktycznym i nieefektywnym. Bardziej praktycznym podejściem jest ustalenie interwałów gromadzenia informacji związanych z bezpieczeństwem oraz przeprowadzanych ocen. Częstotliwość ocen powinna być wystarczająca do zapewnienia odpowiedniego bezpieczeństwa współmiernego do ryzyka, zgodnie z kategoryzacją systemu i wymaganiami strategii ciągłego monitorowania bezpieczeństwa informacji. Próbkowanie obiektów bezpieczeństwa systemów informacyjnych zastępujące kompleksowe kontrole może być również wydajnym i skutecznym sposobem monitorowania, szczególnie w przypadkach, gdy monitorowanie nie jest zautomatyzowane. Ważne zagadnienia dotyczące określania wielkości próby i częstotliwości monitorowania omówiono w rozdziale trzecim. Częstotliwości monitorowania (np. roczne, kwartalne, miesięczne, dzienne) nie powinny być statyczne i jednakowe dla wszystkich wskaźników. Częstotliwość oceny i monitorowania zabezpieczeń jest na przykład dostosowywana do zmian w organizacyjnych systemach informacyjnych lub ich środowiskach operacyjnych, w tym do pojawiających się informacji o zagrożeniach bezpieczeństwa i podatnościach. Priorytety strategii ciągłego monitorowania bezpieczeństwa

[27] Omówienie rodzajów autoryzacji znajduje się w dokumencie NIST SP 800-37 z późniejszymi zmianami.

informacji różnią się i są dostosowywane w odpowiedzi na incydenty związane z bezpieczeństwem, w celu zidentyfikowania problemów z wdrożonymi zabezpieczeniami lub w celu oceny zmian w systemach i komponentach systemów, które mają znaczący wpływ na bezpieczeństwo. Strategia ciągłego monitorowania bezpieczeństwa informacji może zapewniać dynamiczne aktualizacje danych związanych z bezpieczeństwem w celu obsługi autoryzacji systemu przeprowadzanych w dowolnych odstępach czasu.

Rozdział 3.2.2 zawiera pełniejsze omówienie czynników, które należy wziąć pod uwagę przy określaniu częstotliwości monitorowania.

2.3. ROLA AUTOMATYZACJI W STRATEGII CIĄGŁEGO MONITOROWANIA BEZPIECZEŃSTWA INFORMACJI

Wszędzie tam, gdzie istnieją takie możliwości, organizacje poszukują zautomatyzowanych rozwiązań, aby obniżyć koszty, zwiększyć wydajność i poprawić niezawodność monitorowania danych związanych z bezpieczeństwem. Bezpieczeństwo stanowi skutek połączonych działań personelu, procesów i technologii. Automatyzacja bezpieczeństwa informacji oznacza przede wszystkim automatyzację aspektów bezpieczeństwa, które wymagają niewielkiej interakcji ze strony człowieka. Zautomatyzowane narzędzia są często w stanie rozpoznać wzorce i powiązania, które mogą umknąć uwadze ludzkich analityków, zwłaszcza gdy analiza jest przeprowadzana na dużych zbiorach danych. Obejmuje to zagadnienia takie jak weryfikacja ustawień poszczególnych urządzeń końcowych w sieci oraz zapewnianie zgodności oprogramowania zainstalowanego na urządzeniu z polityką organizacyjną. Automatyzacja pozwala na rozszerzenie procesów bezpieczeństwa realizowanych przez specjalistów ds. bezpieczeństwa w organizacji i może zmniejszyć ilość czasu, jaki pracownicy poświęcają na wykonywanie zbędnych zadań, zwiększając tym samym ilość czasu, jaki wyszkolony specjalista może poświęcić na zadania wymagające ludzkiego punktu widzenia.

Strategia ciągłego monitorowania bezpieczeństwa informacji nie skupia się wyłącznie na informacjach związanych z bezpieczeństwem, które są łatwe do zebrania przez organizację lub zautomatyzowania. Kiedy program ciągłego monitorowania

bezpieczeństwa informacji jest wdrażany po raz pierwszy, w organizacji z dużym prawdopodobieństwem istnieje szereg aspektów programu bezpieczeństwa, które są monitorowane ręcznie. Możliwości organizacji w zakresie monitorowania z czasem ulegają rozwojowi i są rozszerzane. Wskaźniki zmieniają się wraz z wyciągniętymi wnioskami i lepszym wglądem w stan bezpieczeństwa organizacji, a także tolerancją ryzyka. Strategia ciągłego monitorowania bezpieczeństwa informacji koncentruje się na dostarczaniu odpowiednich danych na temat skuteczności zabezpieczeń i stanu bezpieczeństwa organizacji, umożliwiając przedstawicielom organizacji podejmowanie świadomych, terminowych decyzji dotyczących zarządzania ryzykiem. W związku z tym wdrażanie, skuteczność i adekwatność wszystkich zabezpieczeń są monitorowane wraz ze stanem bezpieczeństwa organizacyjnego.

Określając zakres automatyzacji praktyk związanych ze strategią ciągłego monitorowania bezpieczeństwa informacji, organizacje biorą pod uwagę możliwości wynikające ze standaryzacji procesów, które można uzyskać dzięki automatyzacji, a także potencjalną wartość (lub brak wartości) automatyzacji gromadzenia informacji związanych z bezpieczeństwem z perspektywy zarządzania ryzykiem. Ponadto organizacje biorą pod uwagę także kwestie takie jak potencjalna wartość przypisania pracowników do innych zadań oraz zwiększenie świadomości sytuacyjnej.

Choć automatyzacja niektórych zagadnień związanych z bezpieczeństwem informacyjnym może znacznie zmniejszyć ilość czasu poświęcanego przez ludzi na wykonywanie niektórych zadań, nie jest możliwe pełne zautomatyzowanie wszystkich zadań związanych z bezpieczeństwem informacji w organizacji. Na przykład technologie omówione w załączniku D do niniejszego dokumentu nadal wymagają analizy przez człowieka w celu wdrożenia i utrzymania narzędzi, a także odpowiedniej interpretacji wyników. Co więcej, narzędzia te działają w kontekście procesów zaprojektowanych, wdrożonych i utrzymywanych przez ludzi. Jeśli poszczególne osoby wykonują swoje obowiązki bez poszanowania dla bezpieczeństwa, skuteczność technologii spada, a bezpieczeństwo systemów, misji, procesów biznesowych oraz procesów organizacyjnych wspieranych przez te systemy jest zagrożone.

Automatyzacja sprawia, że informacje związane z bezpieczeństwem są łatwo dostępne w środowisku, w którym zmieniają się potrzeby dotyczące ciągłego monitorowania. Dlatego podczas wdrażania zabezpieczeń (etap 3 ram zarządzania ryzykiem) bierze się pod uwagę możliwości dostępnych technologii w zakresie wsparcia ciągłego monitorowania bezpieczeństwa informacji jako część kryteriów określających, w jaki sposób najlepiej wdrożyć dane zabezpieczenie.

W tym celu uwzględnia się narzędzia ISCM, które:

- gromadzą informacje z różnych źródeł (np. obiektów oceny[28]);
- używają otwartych specyfikacji, takich jak automatyczny protokół zabezpieczeń zawartości (*ang. Security Content Automation Protocol - SCAP*);
- zapewniają interoperacyjność z innymi produktami, takimi jak centrum pomocy, systemy zarządzania zapasami, systemy zarządzania konfiguracją i rozwiązania w zakresie reagowania na incydenty;
- zapewniają zgodność z obowiązującymi przepisami, rozporządzeniami wykonawczymi, dyrektywami, politykami, przepisami, normami, standardami i rekomendacjami;
- zapewniają możliwości przygotowywania sprawozdań z możliwością dostosowania danych wyjściowych i przechodzenia od wysokopoziomowych, zestawionych wskaźników do wskaźników na poziomie pojedynczych systemów; oraz
- umożliwiają konsolidację danych w narzędziach do zarządzania bezpieczeństwem informacji i zdarzeniami (*ang. Security Information and Event Management - SIEM*) oraz pulpitach nawigacyjnych.

Automatyzacja wspiera gromadzenie większej ilości danych, z większą częstotliwością oraz z szerszego zakresu produktów, technologii, procesów, środowisk oraz od większej liczby pracowników. Może zatem sprawić, że kompleksowa, bieżąca kontrola bezpieczeństwa informacji stanie się praktyczna i przystępna cenowo. Skuteczność organizacji

[28] Informacje na temat obiektów oceny znajdują się dokumencie NIST SP 800-53A (NSC 800-53A) z późniejszymi zmianami.

w wykorzystywaniu wyników monitorowania (uzyskanych w sposób ręczny lub zautomatyzowany) niezmiennie zależy jednak od strategii ciągłego monitorowania bezpieczeństwa informacji, w tym prawidłowości i kompleksowości wskaźników, a także procesów analizy wyników monitorowania i reagowania na ustalenia. Technologie umożliwiające automatyzację niektórych zadań w zakresie ciągłego monitorowania bezpieczeństwa informacji omówiono bardziej szczegółowo w załączniku D.

2.4. ROLE I OBOWIĄZKI ZWIĄZANE Z CIĄGŁYM MONITOROWANIEM BEZPIECZEŃSTWA INFORMACJI

Niniejszy rozdział zawiera opis ról i obowiązków kluczowych[29] uczestników zaangażowanych w program ciągłego monitorowania bezpieczeństwa informacji organizacji. Zróżnicowane misje i struktury organizacyjne mogą prowadzić do różnic w konwencjach nazewnictwa ról związanych z ciągłym monitorowaniem bezpieczeństwa informacji oraz sposobie przydzielania określonych obowiązków pracownikom organizacji – mogą wystąpić sytuacje, w których na przykład wiele osób będzie pełniło tę samą rolę, bądź jedna osoba będzie pełniła jednocześnie wiele ról.

Role i obowiązki powszechnie związane z ciągłym monitorowaniem bezpieczeństwa informacji:

Kierownik jednostki organizacyjnej *(ang. Head of Agency)* Kierownik jednostki organizacyjnej będzie z dużym prawdopodobieństwem zaangażowany w działania w zakresie ciągłego monitorowania bezpieczeństwa informacji w kontekście zarządzania ryzykiem.

Funkcja wykonawcza ds. ryzyka (ang. Risk Executive). Osoba odpowiedzialna za zarządzanie ryzykiem nadzoruje strategię i program ciągłego monitorowania bezpieczeństwa informacji organizacji. Osoba odpowiedzialna za zarządzanie ryzykiem dokonuje przeglądów sprawozdań powstałych w ramach procesu ciągłego monitorowania bezpieczeństwa informacji i traktuje je jako dane wejściowe do decyzji dotyczących postawy wobec ryzyka w zakresie bezpieczeństwa informacji i tolerancji ryzyka oraz przekazuje informacje

[29] Dodatkowe informacje w zakresie nazewnictwa ról i obowiązków – patrz NSC 800-37, NSC 7298.

jednostkom odpowiedzialnym za misje, procesy biznesowe oraz systemy informacyjne w zakresie strategii i wymagań ISCM; sprzyja współpracy między jednostkami organizacyjnymi, koordynuje udostępnianie informacji związanych z bezpieczeństwem; zapewnia dostępne dla całej organizacji forum pozwalające na analizę wszystkich źródeł ryzyka i dba o to, by informacje o ryzyku były brane pod uwagę przy podejmowaniu decyzji dotyczących ciągłego monitorowania.

Osoba odpowiedzialna za technologie informacyjne (ang. Chief Information Officer, CIO). CIO odpowiada za kierowanie programem ciągłego monitorowania bezpieczeństwa informacji w organizacji. CIO zapewnia ustanowienie i wdrożenie skutecznego programu ciągłego monitorowania bezpieczeństwa informacji w organizacji poprzez ustalenie oczekiwań i wymagań dotyczących programu ISCM w organizacji; ścisłą współpracę z osobami autoryzującymi w celu zapewnienia finansowania, personelu i innych zasobów wspierających realizację ISCM; a także zapewnia komunikację na wysokim szczeblu i relacje między grupami roboczymi poszczególnych jednostek organizacyjnych.

Kluczowa osoba odpowiedzialna za bezpieczeństwo informacji (ang. Senior Information Security Officer, SISO). SISO ustanawia, wdraża i utrzymuje program ciągłego monitorowania bezpieczeństwa informacji w organizacji, opracowuje wytyczne dotyczące programu organizacyjnego (zasady oraz procedury) w celu ciągłego monitorowania programu bezpieczeństwa i systemów informacyjnych; opracowuje wytyczne dotyczące zarządzania konfiguracją dla organizacji; konsoliduje i analizuje plany i etapy działania w celu określenia słabych punktów i braków w zabezpieczeniach organizacyjnych, odpowiada za nabywanie lub opracowanie i utrzymywanie zautomatyzowanych narzędzi do obsługi ISCM i bieżących autoryzacji; zapewnia szkolenia w zakresie programu i procesu ISCM w organizacji oraz zapewnia wsparcie osobom odpowiedzialnym za informacje i systemy informatyczne, a także dostawcom zabezpieczeń wspólnych w zakresie wdrażania ISCM na szczeblu systemów informacyjnych.

Osoba autoryzująca (ang. Authorizing Official). Osoba autoryzująca odpowiada za zapewnienie, że program ciągłego monitorowania bezpieczeństwa informacji w organizacji jest stosowany w odniesieniu do danego systemu informacyjnego. Osoba

autoryzująca zapewnia utrzymanie stanu bezpieczeństwa systemu informacyjnego, dokonuje przeglądów sprawozdań o stanie bezpieczeństwa i kluczowych dokumentów na temat bezpieczeństwa oraz określa, czy ryzyko dla organizacji związane z działaniem systemu informacyjnego pozostaje akceptowalne. Osoba ta określa również, czy znaczące zmiany w systemie informacyjnym wymagają ponownej autoryzacji i ponownie autoryzuje system informacyjny, gdy jest to wymagane.

Właściciel systemu informacyjnego/Właściciel informacji/Władający informacją *(ang. Information System Owner / Information Owner / Information Steward).* Właściciel systemu informacyjnego ustanawia procesy i procedury wspierające wdrożenie programu ciągłego monitorowania bezpieczeństwa informacji w organizacji na poziomie systemu. Obejmuje to opracowanie i udokumentowanie strategii ciągłego monitorowania bezpieczeństwa informacji dla danego systemu informacyjnego, udział w procesie zarządzania konfiguracją w organizacji; opracowanie i utrzymywanie spisu komponentów związanych z systemem informacyjnym, przeprowadzanie analiz wpływu na bezpieczeństwo zmian w systemie informacyjnym, przeprowadzanie lub odpowiedzialność za przeprowadzanie ocen zabezpieczeń zgodnie ze strategią ISCM, opracowywanie i składanie sprawozdań o stanie bezpieczeństwa zgodnie z polityką i procedurami organizacyjnymi; wdrażanie działań naprawczych niezbędnych do utrzymania autoryzacji systemu, wprowadzanie zmian do procesu monitorowania zabezpieczeń na poziomie systemu zgodnie z wymaganiami; przeglądanie sprawozdań dotyczących ciągłego monitorowania bezpieczeństwa informacji od dostawców zabezpieczeń wspólnych w celu sprawdzenia, czy zabezpieczenia te nadal zapewniają odpowiednią ochronę systemu informacyjnego oraz aktualizowanie krytycznych dokumentów dotyczących bezpieczeństwa w oparciu o wyniki procesu ciągłego monitorowania bezpieczeństwa informacji.

Dostawca zabezpieczeń wspólnych*[30]. *(ang. Common control provider) Dostawca zabezpieczeń wspólnych ustanawia procesy i procedury wspierające bieżące monitorowanie zabezpieczeń wspólnych. Dostawca zabezpieczeń wspólnych opracowuje i dokumentuje strategię ciągłego monitorowania bezpieczeństwa informacji dla przypisanych zabezpieczeń, uczestniczy w procesie zarządzania konfiguracją w organizacji, opracowuje i utrzymuje wykaz komponentów związanych z zabezpieczeniami wspólnymi; przeprowadza analizy wpływu na bezpieczeństwo zmian, które dotyczą zabezpieczeń wspólnych, zapewnia zgodność oceny zabezpieczeń ze strategią ISCM; przygotowuje i przedkłada raporty o stanie bezpieczeństwa zgodnie z zasadami oraz procedurami organizacyjnymi; w razie potrzeby wdraża działania naprawcze w celu utrzymania autoryzacji zabezpieczeń wspólnych; aktualizuje i usprawnia proces monitorowania zabezpieczeń wspólnych zgodnie z wymaganiami; aktualizuje krytyczne dokumenty dotyczące bezpieczeństwa w miarę pojawiania się zmian oraz przekazuje krytyczne dokumenty dotyczące bezpieczeństwa do poszczególnych właścicieli informacji/właścicieli systemów informacyjnych i innych liderów wyższego szczebla zgodnie z zasadami i procedurami obowiązującymi w organizacji.

Osoba odpowiedzialna za bezpieczeństwo systemu informacyjnego (ang. Information System Security Officer, ISSO). ISSO wspiera program ciągłego monitorowania bezpieczeństwa informacji w organizacji, pomagając właścicielowi systemu informacyjnego w wypełnianiu obowiązków wynikających z ISCM i uczestnicząc w procesie zarządzania konfiguracją.

[30] Organizacje mogą mieć wielu dostawców zabezpieczeń wspólnych.

Podmiot oceniający zabezpieczenia (ang. control assessor, CA). Podmiot oceniający zabezpieczenia przekazuje informacje dotyczące bezpieczeństwa zgromadzone w ramach procesów ciągłego monitorowania bezpieczeństwa informacji i ocenia zabezpieczenia systemu informacyjnego lub zarządzania programem ISCM w organizacji. Podmiot oceniający zabezpieczenia opracowuje plan oceny bezpieczeństwa dla wszystkich zabezpieczeń, przedkłada plan oceny bezpieczeństwa do zatwierdzenia przed przeprowadzeniem ocen; przeprowadza oceny zabezpieczeń zgodnie z planem oceny bezpieczeństwa; aktualizuje sprawozdanie z oceny bezpieczeństwa w miarę zmian zachodzących w ramach ciągłego monitorowania bezpieczeństwa informacji i aktualizuje bądź zmienia plan oceny bezpieczeństwa w razie potrzeby.

Organizacje mogą ustanawiać także inne role, na przykład administratora systemu informacyjnego bądź kierownika programu ISCM w zależności od potrzeb, by wspierać realizację procesu ciągłego monitorowania bezpieczeństwa informacji.

ROZDZIAŁ TRZECI

3. PROCES

OKREŚLANIE STRATEGII I WDRAŻANIE PROGRAMU CIĄGŁEGO MONITOROWANIA BEZPIECZEŃSTWA INFORMACJI

Niniejszy rozdział opisuje proces opracowywania strategii i wdrażania programu, ciągłego monitorowania bezpieczeństwa informacji, uwzględniając działania na poziomach organizacji, misji oraz procesów biznesowych, a także systemów informacyjnych. Dobrze zaprojektowana strategia ciągłego monitorowania bezpieczeństwa informacji obejmuje ocenę zabezpieczeń, monitorowanie stanu bezpieczeństwa i opracowywanie sprawozdań dotyczących stanu bezpieczeństwa w celu wspierania szybkiego podejmowania decyzji opartych na ryzyku w całej organizacji. Obejmuje również procesy zapewniające odpowiednią reakcję na ustalenia. Strategia działania organizacji uwzględniająca wykorzystanie zgromadzonych danych jest równie ważna, jeśli nie ważniejsza niż samo ich gromadzenie. Proces opracowywania strategii i wdrażania programu ciągłego monitorowania bezpieczeństwa informacji obejmuje następujące etapy:

- **Określenie** (*ang. Define*) strategii ciągłego monitorowania bezpieczeństwa informacji na podstawie poziomu tolerowanego ryzyka, która uwzględnia zasoby, świadomość podatności, aktualne informacje o zagrożeniach oraz wpływ na misje oraz procesy biznesowe.
- **Ustanowienie** (*ang. Establish*) programu ciągłego monitorowania bezpieczeństwa informacji określającego wskaźniki, częstotliwość monitorowania stanu bezpieczeństwa, częstotliwość oceny zabezpieczeń oraz architekturę techniczną.
- **Wdrożenie** (*ang. Implement*) programu ciągłego monitorowania bezpieczeństwa informacji oraz gromadzenie informacji związanych z bezpieczeństwem na potrzeby wskaźników, ocen i sprawozdań. Automatyzacja gromadzenia, analizy i przygotowywania sprawozdań z danych tam, gdzie to możliwe.

- **Analiza** (*ang. Analyze*) zgromadzonych danych oraz przygotowywanie **Sprawozdań** (*ang. Report*) określających stosowne reakcje i działania. Na tym etapie konieczne może być zebranie dodatkowych informacji w celu wyjaśnienia lub uzupełnienia istniejących danych z monitoringu.
- **Reagowanie** (*ang. Respond*) na ustalenia za pomocą technicznych, zarządczych i operacyjnych działań łagodzących lub akceptacji ryzyka, przeniesienia go lub podzielenia się nim z innym podmiotem, bądź też unikania lub odrzucenia ryzyka.
- **Przegląd i aktualizacja** (*ang. Review and Update*) programu monitorowania, dostosowanie strategii ciągłego monitorowania bezpieczeństwa informacji i rozwój działań pomiarowych w celu zwiększenia widoczności zasobów i świadomości podatności, umożliwienia kontroli nad bezpieczeństwem infrastruktury informacyjnej organizacji w oparciu o dane oraz zwiększenia odporności organizacji.

Proces ten został przedstawiony poniżej na rysunku 3-1.

Rysunek 3-1. Proces ciągłego monitorowania bezpieczeństwa informacji

Tolerowanie ryzyka, architektura korporacyjna, architektura bezpieczeństwa, konfiguracje bezpieczeństwa, plany zmian w architekturze korporacyjnej i dostępne informacje o zagrożeniach dostarczają danych, które mają fundamentalne znaczenie dla realizacji poszczególnych etapów i bieżącego zarządzania ryzykiem związanym z bezpieczeństwem informacji. Informacje związane z bezpieczeństwem są analizowane pod kątem ich znaczenia dla zarządzania ryzykiem organizacyjnym na wszystkich trzech poziomach.

Pozostała część tego rozdziału omawia proces ciągłego monitorowania bezpieczeństwa informacji i dostarcza szczegółowych informacji dotyczące zagadnień, których nie obejmują istniejące zalecenia, a w stosownych przypadkach odwołuje się do istniejących rekomendacji. Główne role, role pomocnicze, oczekiwane dane wejściowe i oczekiwane wyniki dotyczące każdego etapu powinny być traktowane jako wskazówki. Role i obowiązki mogą różnić się w zależności od organizacji, podobnie jak szczegóły wdrożeniowe programu ciągłego monitorowania bezpieczeństwa informacji.

3.1. OKREŚLENIE STRATEGII CIĄGŁEGO MONITOROWANIA BEZPIECZEŃSTWA INFORMACJI

Skuteczne działania w zakresie ciągłego monitorowania bezpieczeństwa informacji rozpoczynają się od opracowania strategii, która odnosi się do wymagań i działań w zakresie ciągłego monitorowania bezpieczeństwa informacji na każdym szczeblu organizacji – organizacyjnym, misji i procesów biznesowych, a także systemów informacyjnych. Każdy poziom odpowiada za monitorowanie wskaźników bezpieczeństwa i ocenę skuteczności zabezpieczeń w określonych interwałach, a także przeprowadza oceny oraz przygotowuje sprawozdania dotyczące stanu zabezpieczeń dostosowane w celu wsparcia podejmowania decyzji na poszczególnych poziomach. Zasady, procedury, narzędzia i szablony wdrażane z poziomów 1 i 2 lub które są zarządzane zgodnie z wytycznymi z poziomów 1 i 2 w największym stopniu wspierają wykorzystanie danych w ramach poziomów oraz między nimi. Niższe poziomy mogą wymagać większej liczby informacji w porównaniu z wyższymi poziomami, w związku z czym mogą opracować strategie dotyczące danego poziomu,

spójne ze strategiami stosowanymi na wyższych poziomach i spełniające wymagania danego poziomu w zakresie podejmowania decyzji. W zależności od organizacji, zadania i działania wykonywane na poszczególnych poziomach mogą się pokrywać.

Poniższe wskazówki, choć nie mają charakteru nakazowego, pomagają w opracowaniu podejścia do ciągłego monitorowania bezpieczeństwa informacji w całej organizacji, które najlepiej wykorzystuje znormalizowane metodologie i spójne praktyki, a tym samym maksymalizuje skuteczność i możliwości wykorzystania danych związanych z bezpieczeństwem. W miarę zachodzących zmian strategia ciągłego monitorowania bezpieczeństwa informacji jest weryfikowana pod kątem adekwatności, odzwierciedlania tolerancji ryzyka organizacyjnego, poprawności pomiarów i użyteczności wskaźników. Nieodłączną częścią każdej strategii ciągłego monitorowania bezpieczeństwa informacji jest włączenie kryteriów opisujących warunki, które powodują konieczność przeprowadzenia jej przeglądu lub aktualizacji innych niż audyty i kontrole przeprowadzane w ustalonych odstępach czasowych. Organizacja określa kryteria i procedury aktualizacji programu ciągłego monitorowania bezpieczeństwa informacji w oparciu o zmienioną strategię ISCM.

3.1.1. STRATEGIA CIĄGŁEGO MONITOROWANIA BEZPIECZEŃSTWA INFORMACJI NA POZIOMIE ORGANIZACJI (POZIOM 1) ORAZ POZIOMIE MISJI I PROCESÓW BIZNESOWYCH (POZIOM 2)

Osoba odpowiedzialna za zarządzanie ryzykiem określa ogólną tolerancję na ryzyko organizacyjne i strategię ograniczania ryzyka na poziomie organizacji[31]. Strategia ciągłego monitorowania bezpieczeństwa informacji jest opracowywana i wdrażana w celu wspomagania zarządzania ryzykiem zgodnie z tolerancją ryzyka organizacyjnego. Chociaż strategia, polityka i procedury ciągłego monitorowania bezpieczeństwa informacji mogą być opracowywane na dowolnym poziomie organizacji, zazwyczaj strategia ISCM obejmująca całą organizację i związana z nią polityka są opracowywane na poziomie organizacji, a ogólne procedury wdrożeniowe są wypracowywane na poziomie misji i procesów biznesowych. Jeśli strategia obejmująca całą organizację jest opracowywana na poziomie misji i procesów

[31] Informacje na temat ról i obowiązków osoby odpowiedzialnej za zarządzanie ryzykiem znajdują się w dokumencie NIST SP 800-39 z późniejszymi zmianami.

biznesowych, osoby odpowiedzialne na poziomie 1 dokonują przeglądu strategii, a następnie zatwierdzają ją, by zapewnić uwzględnienie tolerancji ryzyka dla całej organizacji we wszystkich misjach i procesach biznesowych. Informacje te są przekazywane pracownikom na poziomach misji i procesów biznesowych oraz systemów informacyjnych oraz uwzględniane w strategii, politykach i procedurach na tych poziomach.

Poniższe polityki, procedury i szablony, opracowane na poziomach 1 bądź 2, umożliwiają realizację standardowych procesów wspierających strategię ciągłego monitorowania bezpieczeństwa informacji w całej organizacji:

- Polityki określające kluczowe wskaźniki.
- Polityki wprowadzania zmian do strategii monitorowania oraz jej utrzymywania.
- Polityki i procedury oceny skuteczności zabezpieczeń (wspólnych, hybrydowych oraz poszczególnych systemów).
- Polityki i procedury monitorowania stanu bezpieczeństwa.
- Polityki i procedury w zakresie sprawozdań dotyczących stanu bezpieczeństwa (monitorowanie skuteczności i stanu zabezpieczeń).
- Polityki i procedury oceny ryzyka oraz uzyskiwania informacji o zagrożeniach.
- Polityki i procedury zarządzania konfiguracjami oraz analizy wpływu na bezpieczeństwo[32].
- Polityki i procedury dotyczące wdrażania narzędzi w całej organizacji oraz ich wykorzystania.
- Polityki i procedury dotyczące ustalania częstotliwości monitorowania.
- Polityki i procedury dotyczące określania wielkości prób i grup docelowych oraz doborem prób.

[32] Więcej informacji na temat zarządzania konfiguracją z punktu widzenia bezpieczeństwa znajduje się w dokumencie NIST SP 800-128 z późniejszymi zmianami.

- Procedury dotyczące wyznaczania wskaźników w zakresie bezpieczeństwa i źródeł danych.
- Szablony oceny ryzyka.
- Szablony sprawozdań dotyczących stanu bezpieczeństwa (skuteczności zabezpieczeń oraz monitorowania stanu bezpieczeństwa).

Polityki, procedury i szablony muszą bezwzględnie uwzględniać ręczne i zautomatyzowane metodologie monitorowania. Dodatkowo na tych poziomach organizacje ustanawiają polityki oraz procedury w zakresie szkolenia pracowników odpowiedzialnych za zadania związane z ciągłym monitorowaniem bezpieczeństwa informacji. Może to obejmować szkolenie w zakresie obsługi i korzystania ze zautomatyzowanych narzędzi, ustalania poziomów bazowych i dostrajania pomiarów w celu zapewnienia dokładnego monitorowania środowisk operacyjnych. Może również obejmować szkolenie w zakresie rozpoznawania i odpowiedniego reagowania na informacje oraz alarmy ze wskaźników wskazujących na ryzyko przekraczające dopuszczalne limity, a także wewnętrznych lub zewnętrznych wymogów w zakresie sprawozdawczości. Szkolenie to może być uwzględnione w istniejących wymaganiach szkoleniowych dotyczących poszczególnych ról dla osób odpowiedzialnych w znaczący sposób za bezpieczeństwo lub może stanowić oddzielne szkolenie w zakresie wdrażania polityki i procedur ciągłego monitorowania bezpieczeństwa informacji w organizacji.

Podczas wdrażania zasad, procedur i szablonów opracowanych na wyższych poziomach, pracownicy niższych poziomów uzupełniają wszelkie luki związane z procesami dotyczące zagadnień dotyczących danego poziomu. Decyzje i działania podejmowane przez osoby na poziomach 1 i 2 mogą być ograniczone przez takie czynniki, jak potrzeby misji lub procesów biznesowych, ograniczenia dotyczące infrastruktury lub zasobów ludzkich, niezmienne zasady zarządzania i czynniki zewnętrzne.

Podstawowe role: Osoba odpowiedzialna za zarządzanie ryzykiem, CIO, SISO, osoby autoryzujące.

Role wspierające: Właściciel systemu informacyjnego, dostawca zabezpieczeń wspólnych.

Oczekiwane informacje: Ocena ryzyka organizacyjnego i informacje na temat tolerowanego ryzyka, informacje o zagrożeniach, oczekiwania i priorytety organizacji, narzędzia dostępne z linii biznesowych OMB bądź od dostawców zewnętrznych.

Oczekiwane wyniki: Zaktualizowane informacje na temat tolerowanego ryzyka, strategia ciągłego monitorowania bezpieczeństwa informacji dla organizacji oraz powiązane polityki, procedury, szablony i narzędzia.

3.1.2. STRATEGIA CIĄGŁEGO MONITOROWANIA BEZPIECZEŃSTWA INFORMACJI NA POZIOMIE SYSTEMU INFORMACYJNEGO (POZIOM 3)

Strategia ciągłego monitorowania bezpieczeństwa informacji na poziomie systemu informacyjnego jest opracowywana i wdrażana w celu wspierania zarządzania ryzykiem, nie tylko na poziomie systemów informacyjnych, ale na *wszystkich trzech poziomach*, zgodnie z tolerancją ryzyka dotyczącego systemów oraz organizacji. Mimo że strategia może zostać określona na poziomach 1 lub 2, poziom 3 może opracować polityki dotyczące poszczególnych systemów oraz procedury wdrożeniowe. Informacje związane z bezpieczeństwem na poziomie systemu obejmują dane oceny dotyczące zabezpieczeń na poziomie systemu oraz dane wskaźników *uzyskane z* zabezpieczeń na poziomie systemu. Właściciele systemu ustanawiają strategię ciągłego monitorowania bezpieczeństwa informacji na poziomie systemu, biorąc pod uwagę takie czynniki, jak architektura systemu i środowisko operacyjne, a także wymagania, zasady, procedury i szablony opracowane na szczeblach organizacji oraz misji[33].

Ciągłe monitorowanie bezpieczeństwa informacji na poziomie systemu dotyczy oceniania zabezpieczeń pod kątem skuteczności, monitorowania stanu bezpieczeństwa i przygotowywania sprawozdań z ustaleń. Na tym poziomie ocenie należy poddawać co najmniej wszystkie zabezpieczenia, w tym zabezpieczenia wspólne oraz hybrydowe wdrożone na poziomie systemów pod kątem ewentualnych poprawek. Właściciele systemów określają częstotliwość oceny zabezpieczeń na

[33] Celem strategii ciągłego monitorowania bezpieczeństwa informacji jest zapewnienie, że zagrożenia dla architektury bezpieczeństwa są obsługiwane w sposób pozwalający na ograniczenie lub minimalizację wpływu na funkcje biznesowe i misję.

podstawie informacji ze wszystkich trzech poziomów. Pełne omówienie czynników, które należy wziąć pod uwagę przy określaniu częstotliwości oceny i monitorowania, można znaleźć w rozdziale 3.2.2. Informacje związane z bezpieczeństwem na poziomie systemu są wykorzystywane do określenia stanu bezpieczeństwa na wszystkich trzech poziomach. Wykorzystanie informacji związanych z bezpieczeństwem na poziomie systemu w wskaźnikach służących do określania stanu bezpieczeństwa zostało omówione w rozdziale 3.2.1.

Strategia ciągłego monitorowania bezpieczeństwa informacji na poziomie systemów informacyjnych wspiera również bieżącą autoryzację. Bieżąca autoryzacja oznacza powtarzające się aktualizacje informacji o decyzjach autoryzacyjnych zgodnie z częstotliwością oceny i monitorowania. Wyniki oceny z monitorowania zabezpieczeń wspólnych wdrażanych oraz zarządzanych na szczeblu organizacji lub misji i procesów biznesowych mogą być zestawiane z informacjami generowanymi na poziomie systemów informacyjnych w celu dostarczenia osobie autoryzującej kompletnego zestawu niezależnie wygenerowanych danych.[34] Dane z ocen realizowanych w ramach ciągłego monitorowania bezpieczeństwa informacji powinny być przekazywane osobie autoryzującej tak często, jak wymagają tego zasady w organizacji.

Podstawowe role: Właściciel systemu informacyjnego, dostawca zabezpieczeń wspólnych, ISSO.

Role wspierające: SISO, osoba autoryzująca, oceniający środki bezpieczeństwa.

Oczekiwane informacje: Informacje dotyczące tolerowanego ryzyka organizacyjnego, strategia ciągłego monitorowania bezpieczeństwa informacji w organizacji, polityki, procedury, szablony, informacje o zagrożeniach dotyczących systemów oraz informacje na

[34] Szczegółowe wymagania dotyczące niezależności osoby oceniającej zostały opisane w dokumencie NIST SP 800-53, w opisie zabezpieczenia rozszerzonego CA-2. Niezależność oceniających powinna dotyczyć wyłącznie działania systemu. Z tego względu osoby oceniające mogą być wyznaczane na poziomie organizacji bądź misji i procesów biznesowych, a także pochodzić z jednostek wewnętrznych lub zewnętrznych niezależnych względem organizacji. Wyniki ocen przeprowadzonych przez operatorów systemów mogą być wykorzystane, jeśli zostały zatwierdzone przez niezależnych oceniających.

temat systemów, w tym plany bezpieczeństwa, sprawozdania z oceny bezpieczeństwa, plany i etapy działania, plany oceny bezpieczeństwa, szacowanie ryzyka itp.[35].

Oczekiwane wyniki: Strategia ciągłego monitorowania bezpieczeństwa informacji na poziomie systemu, która uzupełnia strategie opracowane na poziomach 1 i 2 oraz program bezpieczeństwa organizacji, zarazem dostarczając informacji na temat stanu bezpieczeństwa wszystkich poziomów oraz informacje w czasie rzeczywistym dotyczące bieżących decyzji w zakresie autoryzacji systemów zgodnie z zaleceniami organizacyjnej strategii ISCM.

3.1.3. ROLE I OBOWIĄZKI ZWIĄZANE Z PROCESEM

Przedstawiciele poziomów 1 i 2 realizują obowiązki dotyczące całego procesu ciągłego monitorowania bezpieczeństwa informacji, w tym:

- Wkład w rozwój organizacyjnej strategii ciągłego monitorowania bezpieczeństwa informacji, w tym ustanowienie wskaźników, polityk i procedur, zestawianie i korelowanie danych zgromadzonych na poziomie 3 z informacjami związanymi z bezpieczeństwem wykorzystywanymi na poziomach 1 i 2, ustalanie zasad dotyczących częstotliwości oceny i monitorowania oraz reguł zapewniających wystarczającą głębokość i zakres ocen, gdy wykorzystywane są metodologie próbkowania [Etapy ISCM: Określanie, Ustanowienie, Wdrożenie].
- Dokonywanie przeglądów wyników monitorowania (informacji związanych z bezpieczeństwem) w celu określenia stanu bezpieczeństwa zgodnie z polityką organizacyjną i definicjami [Etap ISCM: Analiza/Sprawozdawczość].
- Analiza potencjalnego wpływu na bezpieczeństwo organizacji oraz misji i procesów biznesowych wynikającego ze zmian w systemach informacyjnych i ich środowiskach eksploatacji, a także wpływu na bezpieczeństwo architektury korporacyjnej wynikającego z wdrażania lub utylizacji systemów informacyjnych [Etap ISCM: Analiza/Sprawozdawczość].

[35] Opisane informacje dotyczące systemu stanowią rezultat ram zarządzania ryzykiem. Znormalizowane cyfrowe szablony i systemy zarządzania dokumentami pozwalają na częste aktualizacje danych generowanych przez programy ciągłego monitorowania.

- Ustalenie, czy obecny poziom ryzyka mieści się w granicach tolerancji ryzyka ustalonych przez organizację [Etapy ISCM: Analiza/Sprawozdawczość, Przegląd/Aktualizacja].
- Podejmowanie działań w celu reagowania na ryzyko, gdy pojawi się taka potrzeba, w tym między innymi stwierdzenie konieczności ustanowienia nowych lub zmienionych wskaźników, przeprowadzenia dodatkowych lub zmienionych ocen, modyfikacji istniejących zabezpieczeń wspólnych lub ustanowienia nowych zabezpieczeń w oparciu o wyniki bieżących działań w zakresie monitorowania i oceny ryzyka [Etap ISCM: Reagowanie].
- Aktualizacja stosownej dokumentacji dotyczącej bezpieczeństwa [Etap ISCM: Reagowanie].
- Przegląd nowych lub zmodyfikowanych przepisów, dyrektyw, zasad i innych dokumentów pod kątem wszelkich zmian w wymaganiach dotyczących bezpieczeństwa [Etap ISCM: Przegląd/Aktualizacja].
- Przegląd wyników monitorowania w celu ustalenia, czy plany i zasady organizacyjne wymagają dostosowania lub aktualizacji [Etap ISCM: Przegląd/Aktualizacja].
- Przegląd wyników monitorowania w celu zebrania nowych informacji na temat podatności [Etap ISCM: Przegląd/Aktualizacja].
- Przegląd informacji o nowych lub pojawiających się zagrożeniach, o których świadczą widoczne w wynikach monitorowania wskaźniki zagrożeń, modelowanie zagrożeń (oparte na zasobach i atakach), przegląd klasyfikowanych i jawnych informacji o zagrożeniach, sprawozdań CERT i innych informacji dostępnych z zaufanych źródeł, wymiana między organizacjami i źródłami rządowymi [Etap ISCM: Przegląd/Aktualizacja].

Przedstawiciele poziomu 3 realizują obowiązki dotyczące całego procesu ciągłego monitorowania bezpieczeństwa informacji, w tym między innymi:

- Zapewnianie wkładu w opracowywanie oraz wdrażanie strategii ciągłego monitorowania bezpieczeństwa informacji obejmującej całą organizację wraz

z rozwojem i wdrażaniem strategii ISCM na poziomie systemu [Etapy ISCM: Określanie, Ustanowienie, Wdrożenie, etap ram zarządzania ryzykiem: Wybór].

- Wspieranie planowania i wdrażania zabezpieczeń, narzędzi automatyzacji oraz mechanizmów łączności między tymi narzędziami w związku z realizacją strategii ciągłego monitorowania bezpieczeństwa informacji [Etap ISCM: Wdrożenie; Etap ram zarządzania ryzykiem: Wybór].
- Określenie wpływu zmian w systemie informacyjnym i jego środowisku eksploatacji, w tym zmian związanych z uruchomieniem lub wycofaniem systemu z eksploatacji, na bezpieczeństwo [Etap ISCM: Analiza/Sprawozdawczość]; Etap ram zarządzania ryzykiem: Monitorowanie].
- Bieżąca ocena skuteczności zabezpieczeń [Etap ISCM: Wdrożenie; Etapy ram zarządzania ryzykiem: Ocena[36], Monitorowanie].
- Podejmowanie działań w celu reagowania na ryzyko, gdy pojawi się taka potrzeba, w tym między innymi stwierdzenie konieczności przeprowadzenia dodatkowych lub zmienionych ocen, modyfikacji istniejących zabezpieczeń lub ustanowienia nowych zabezpieczeń w oparciu o wyniki bieżących działań w zakresie monitorowania i oceny ryzyka, a także zadań do wykonania w ramach planu i etapów działania [Etap ISCM: Reagowanie; Etap ram zarządzania ryzykiem: Monitorowanie].
- Ciągłe przekazywanie informacji na potrzeby planu bezpieczeństwa, sprawozdań z ocen bezpieczeństwa oraz planów i etapów działania w oparciu o wyniki procesu ISCM [Etap ISCM: Reagowanie; Etap ram zarządzania ryzykiem: 6].
- Opracowywanie sprawozdań na temat stanu bezpieczeństwa systemów informacyjnych, w tym danych wymaganych na potrzeby wskaźników na poziomach 1 i 2 [Etap ISCM: Analiza/Sprawozdawczość; Etap ram zarządzania ryzykiem: Ocena, Monitorowanie].

[36] Przed uzyskaniem wstępnej autoryzacji system nie jest objęty programem ciągłego monitorowania w organizacji. Odniesienie do etapu czwartego ram zarządzania ryzykiem staje się istotne po uruchomieniu systemu, gdy w ramach procesu bieżącej autoryzacji następuje przejście przez ten etap.

- Przegląd wynikającego ze sprawozdań stanu bezpieczeństwa systemu informacyjnego w celu ustalenia, czy ryzyko dla systemu i organizacji pozostaje w granicach tolerancji ryzyka [Etap ISCM: Analiza/ Sprawozdawczość; Etap ram zarządzania ryzykiem: Autoryzacja, Monitorowanie].

3.1.4. OKREŚLANIE ZAKRESU PRÓBY

Organizacje mogą uznać, że zbieranie danych z każdego obiektu będącego składnikiem każdego systemu działającego w organizacji może być niepraktyczne lub zbyt kosztowne. Próbkowanie to metodyka, którą można stosować zarówno w przypadku ręcznego, jak i automatycznego monitorowania, co może sprawić, że działania w zakresie ciągłego monitorowania bezpieczeństwa informacji będą bardziej przystępne cenowo. Ryzyko związane z próbkowaniem polega na tym, że zakres wybranej próby może nie pozwolić na dostrzeżenie wszystkich różnic w wynikach oceny, które zostałyby uzyskane w wyniku oceny wszystkich elementów i składników. Może to skutkować niedokładnym oszacowaniem skuteczności zabezpieczeń i stanu bezpieczeństwa organizacji.

Dokument NIST SP 800-53A[37] z późniejszymi zmianami zawiera szczegółowe informacje na temat uzyskiwania zadowalającego pokrycia przy określaniu zakresu prób dla trzech wymienionych metod oceny – badania, wywiadu i testu. Zawarte w dokumencie NIST SP 800-53A wytyczne dotyczące podstawowych, ukierunkowanych i kompleksowych testów[38] pozwalają na zaspokojenie zapotrzebowania na „reprezentatywną próbę obiektów oceny" lub „wystarczająco dużej próby obiektów oceny". Do ilościowego określenia wielkości próby można wykorzystać narzędzia statystyczne.

Dokument NIST 800-53A obejmuje rekomendacje, których celem jest rozwiązanie problemu próbkowania, a w szczególności kwestii pokrycia. Przy doborze zakresu próby odpowiednie pokrycie można zapewnić poprzez uwzględnienie trzech kryteriów:

[37] Patrz: polskojęzyczna publikacja NSC 800-53A. Przypis odnosi się do całego dokumentu.

[38] Por. załącznik D do dokumentu NIST SP 800-53A z późniejszymi zmianami.

- **Rodzaje obiektów oceny** – należy zapewnić dostateczną różnorodność rodzajów obiektów oceny.
- **Liczba obiektów każdego rodzaju** – należy dobrać dostateczną liczbę obiektów każdego rodzaju, aby zagwarantować, że ocena dodatkowych obiektów doprowadzi do uzyskania spójnych ustaleń.
- **Określone obiekty dla każdego ocenianego rodzaju** – biorąc pod uwagę wszystkie istotne obiekty w całej organizacji, które mogą zostać ocenione, należy uwzględnić dostateczną liczbę obiektów dla każdego rodzaju w próbce, aby w wystarczającym stopniu uwzględnić znaną lub przewidywaną zmienność wyników oceny.

Pomiary wybranej próby są podsumowywane w postaci statystyki (np. średniej dla próby), a obserwowana wartość jest porównywana z dopuszczalną wartością ustaloną na podstawie tolerancji ryzyka w organizacji. Statystyki obliczone na postawie próbkowania mogą nie być wiarygodne dla wszystkich systemów, jeśli próba nie jest dobierana losowo i jeśli wielkość próby (ocenianych obiektów) jest niedostateczna[39]. Jak czytamy w podręczniku NIST Engineering Statistics Handbook, przy podejmowaniu decyzji o liczbie obiektów uwzględnianych w próbie do oceny, należy uwzględnić następujące kwestie[40]:

- Oczekiwane informacje (pytania, na które odpowiedzią będą pomiary).
- Koszt i praktyczność przeprowadzenia oceny.
- Znane informacje na temat obiektów, organizacji lub środowisk operacyjnych.
- Przewidywana zmienność w całej grupie.

[39] Centralne twierdzenie graniczne jest kluczowym twierdzeniem, które pozwala założyć, że statystyka (np. średnia) obliczona na podstawie próby losowej charakteryzuje się rozkładem normalnym ilustrowanym krzywą dzwonową niezależnie od rozkładu grupy obiektów, z której pobierane są poszczególne próbki. W przypadku prób o małej liczebności (poniżej 30 obiektów) założenie dotyczące rozkładu normalnego sprawdza się wyłącznie wtedy, gdy rozkład grupy obiektów, z której pobierane są losowe próbki, jest zbliżony do normalnego.

[40] Szczegółowe informacje na temat doboru wielkości próby znajdują się pod adresem http://www.itl.nist.gov/div898/handbook/ppc/section3/ppc333.htm.

- Oczekiwane zaufanie do wynikowych statystyk i wniosków wyciągniętych na temat całej grupy. Sposoby na osiągnięcie większej pewności, że dane zabezpieczenie zostało wdrożone prawidłowo i że działa zgodnie z przeznaczeniem w całej organizacji obejmują zadawanie bardziej ukierunkowanych pytań, zwiększanie liczby rodzajów ocenianych obiektów i zwiększanie liczby obiektów ocenianych w ramach każdego rodzaju.

Stosując powyższe kryteria organizacje mogą również wybierać konkretne obiekty do oceny oprócz próby losowej. Metody doboru próby inne niż losowe należy jednak stosować ostrożnie, aby uniknąć tendencyjności pomiarów. Zautomatyzowane gromadzenie i analiza danych mogą zmniejszyć zapotrzebowanie na próbkowanie.

Podstawowe role: Właściciel systemu informacyjnego, dostawca zabezpieczeń wspólnych, ISSO, oceniający środki bezpieczeństwa.

Role wspierające: Osoba odpowiedzialna za zarządzanie ryzykiem, osoba autoryzująca, CIO, SISO.

Oczekiwane informacje: Zasady i procedury na poziomie organizacyjnym i systemów informacyjnych dotyczące strategii ciągłego monitorowania bezpieczeństwa informacji, wskaźników i planu oceny bezpieczeństwa zaktualizowane o interwały ocen i monitorowania.

Oczekiwane wyniki: Dokumentacja dotycząca planu oceny bezpieczeństwa obejmująca informacje na temat dopuszczalnych prób, informacje związane z bezpieczeństwem.

3.2. USTANOWIENIE PROGRAMU CIĄGŁEGO MONITOROWANIA BEZPIECZEŃSTWA INFORMACJI

Organizacje ustanawiają program wdrażania strategii ciągłego monitorowania bezpieczeństwa informacji. Program ten pozwala na podejmowanie decyzji opartych na ryzyku i prowadzenie operacji w ramach ustalonych tolerancji ryzyka. Cele obejmują wykrywanie anomalii i zmian w środowiskach eksploatacji i systemach informacyjnych organizacji, zwiększanie widoczności zasobów, świadomość podatności, zwiększanie wiedzy o zagrożeniach, zapewnianie skuteczności

zabezpieczeń i weryfikację stanu bezpieczeństwa, w tym zgodności zabezpieczeń z przepisami. Wskaźniki są projektowane, a częstotliwości określane w celu zapewnienia dostępności informacji wymaganych w celu zarządzania ryzykiem w ramach tolerancji ryzyka. Narzędzia, technologie oraz ręczne lub zautomatyzowane metody są wdrażane w kontekście architektury zaprojektowanej w celu dostarczania wymaganych informacji w odpowiednim kontekście i z odpowiednią częstotliwością.

3.2.1. OKREŚLANIE WSKAŹNIKÓW

Organizacje określają wskaźniki wykorzystywane do oceny i kontroli bieżącego ryzyka dla organizacji. Wskaźniki obejmujące wszystkie informacje związane z bezpieczeństwem pochodzą z ocen i monitorowania opartego na zautomatyzowanych narzędziach i procesach ręcznych, są łączone w celu uzyskania przydatnych informacji w celu wspierania podejmowania decyzji i realizacji wymogów dotyczących sprawozdawczości. Wskaźniki powinny być oparte na konkretnych celach w zakresie utrzymania lub poprawy stanu bezpieczeństwa. Wskaźniki są opracowywane dla danych na poziomie systemu, aby nadać im znaczenie w kontekście zarządzania ryzykiem misji, procesu biznesowego lub organizacji.

Wskaźniki mogą wykorzystywać informacje związane z bezpieczeństwem pozyskiwane z różną częstotliwością, a zatem z różnymi opóźnieniami. Wskaźniki mogą być obliczane na podstawie połączenia procesów monitorowania stanu zabezpieczeń, danych z oceny środków bezpieczeństwa oraz danych zebranych z poszczególnych zabezpieczeń. Wskaźniki mogą być określane na dowolnym poziomie lub dla całej organizacji. Wybrane przykłady wskaźników to między innymi liczba i waga ujawnionych i naprawionych podatności, liczba prób uzyskania nieautoryzowanego dostępu, informacje o poziomie bazowym konfiguracji, daty i wyniki testów planów awaryjnych oraz liczba pracowników, którzy są na bieżąco z wymaganiami dotyczącymi szkoleń uświadamiających, progi tolerancji ryzyka dla organizacji oraz ocena ryzyka związana z daną konfiguracją systemu.

Wskaźnik, którego organizacja może używać do monitorowania stanu autoryzowanych i nieautoryzowanych komponentów w sieci, może opierać się na powiązanych wskaźnikach, takich jak fizyczne lokalizacje zasobów, logiczne lokalizacje zasobów (podsieci/adresy IP), adresy MAC, powiązania oraz zasady i procedury

dotyczące łączności sieciowej. Wskaźniki będą odświeżane z różną częstotliwością zgodnie ze strategią ciągłego monitorowania bezpieczeństwa informacji. Wskaźniki mogą być obliczane co godzinę, codziennie lub co tydzień. Choć informacje dotyczące zasobów logicznych mogą zmieniać się każdego dnia, istnieje duże prawdopodobieństwo, że zasady i procedury dotyczące łączności sieciowej będą weryfikowane lub zmieniane nie częściej niż raz w roku. Wskaźniki te mają jedynie charakter informacyjny, a ich stosowanie nie jest zalecane. Zostały one uwzględnione, aby zilustrować koncepcję wskaźników stosowanych na różnych poziomach. Organizacje definiują własne wskaźniki oraz powiązane z nimi interwały i częstotliwości monitorowania. W celu obliczenia wskaźników, zabezpieczenia oraz powiązane z nimi obiekty są oceniane i monitorowane z częstotliwością zgodną z wymaganiami czasowymi dla danego wskaźnika.

Warto zauważyć, że wskaźniki zasadniczo nie spełnią swoich założeń bez pewności, że *wszystkie* zabezpieczenia zostały wdrożone prawidłowo. Wskaźniki są określone lub obliczane zgodnie z informacjami wynikającymi z architektury zabezpieczeń. Zbieranie wskaźników z architektury zabezpieczeń obejmującej zabezpieczenia, które nie zostały poddane ocenie, jest równoznaczne z użyciem uszkodzonej lub nieskalibrowanej wagi. Interpretacja wskaźników i danych, które z nich wynikają, zakłada prawidłowe wdrożenie zabezpieczeń bezpośrednio i pośrednio wykorzystywanych w celu obliczeń wskaźników oraz ich działanie zgodnie z oczekiwaniami. Jeśli dany wskaźnik wskazuje na problem, jego pierwotną przyczyną może być wiele czynników. Bez zapewnienia prawidłowego wdrożenia i ciągłej skuteczności zabezpieczeń, które *nie* są powiązane z danym wskaźnikiem, analiza przyczyn źródłowych będzie utrudniona, ponadto może zostać niewłaściwie zawężona do wcześniej określonej listy, co może spowodować przeoczenie rzeczywistego problemu. Szczegółowe informacje na temat ustalania wskaźników można znaleźć w dokumencie NIST SP 800-55 z późniejszymi zmianami.

Podstawowe role: Osoba odpowiedzialna za zarządzanie ryzykiem, CIO, SISO.

Role wspierające: Osoby autoryzujące, właściciel systemu informacyjnego, dostawca zabezpieczeń wspólnych.

Oczekiwane informacje: Ocena ryzyka w organizacji, tolerancja ryzyka organizacyjnego, aktualne informacje o zagrożeniach, wymagania dotyczące sprawozdawczości, aktualne informacje o podatnościach.

Oczekiwane wyniki: Wskaźniki ustanowione w celu zilustrowania stanu bezpieczeństwa i skuteczności zabezpieczeń na wszystkich trzech poziomach oraz zapewnienia odbiorcom oraz użytkownikom sprawozdań wglądu w zasoby, świadomości podatności i wiedzy o zagrożeniach.

3.2.2. USTALENIE CZĘSTOTLIWOŚCI MONITOROWANIA I OCEN

Określenie częstotliwości monitorowania stanu bezpieczeństwa i oceny zabezpieczeń to kluczowy element programu ciągłego monitorowania bezpieczeństwa informacji w organizacji. Dla niektórych organizacji pulpity nawigacyjne i bieżące oceny stanowią odejście od modelu kompleksowej oceny zabezpieczeń przeprowadzanej w określonym momencie. Aby zmiana ta była konstruktywna i skuteczna z punktu widzenia bezpieczeństwa, wiarygodności oraz wykorzystania zasobów, organizacje określają częstotliwość, z jaką *wszystkie* zabezpieczenia lub elementy zabezpieczeń są oceniane pod kątem skuteczności oraz z jaką monitorowane są *poszczególne* wskaźniki.

Skuteczność zabezpieczeń na danym poziomie lub w całej organizacji może być traktowana jako wskaźnik bezpieczeństwa i w związku z tym także może być monitorowana z określoną częstotliwością. Choć częstotliwości monitorowania i oceny są określane dla każdego indywidualnego wskaźnika i zabezpieczenia, organizacje wykorzystują te dane z różnymi opóźnieniami, aby uzyskać całościowy przegląd bezpieczeństwa każdego systemu, a także wgląd w bezpieczeństwo architektury organizacji. W miarę dojrzewania programu, częstotliwość monitorowania i oceny staje się ważna w kontekście sposobu wykorzystania danych, a pytanie *Kiedy system otrzymał upoważnienie do działania?* stanie się mniej ważne niż *Jak odporny jest dany system?*

Rozważania dotyczące określania częstotliwości oceny i monitorowania.

Przy ustalaniu częstotliwości monitorowania wskaźników lub częstotliwości oceny zabezpieczeń organizacje biorą pod uwagę następujące kryteria:

- **Zmienność zabezpieczeń**. Zmienne zabezpieczenia powinny być oceniane częściej, niezależnie od tego, czy celem jest ustalenie skuteczności zabezpieczeń, czy też

wsparcie obliczeń wskaźników[41]. Dobrym przykładem zmiennych zabezpieczeń są zabezpieczenia dotyczące zarządzania konfiguracją (CM) opisane w dokumencie NIST SP 800-53. Konfiguracje systemów informacyjnych zazwyczaj podlegają nieustannym zmianom. Nieautoryzowane lub niezweryfikowane zmiany w konfiguracji systemu często sprawiają, że system jest podatny na naruszenia. W związku z tym stosowne zabezpieczenia, takie jak CM-6 – Ustawienia konfiguracji oraz CM-8 – Inwentaryzacja komponentów systemu informacyjnego, mogą wymagać częstszej oceny i monitorowania, najlepiej przy użyciu zautomatyzowanych narzędzi zweryfikowanych w ramach automatycznego protokołu zabezpieczeń zawartości, które zapewniają dostęp do alarmów oraz informacji na temat stanu na żądanie. Z kolei zabezpieczenia takie jak PS-2 – Określanie ryzyka dla stanowiska pracy czy PS-3 – Dobór personelu należące do kategorii „Bezpieczeństwo osobowe" zabezpieczeń opisanych w dokumencie NIST SP 800-53, nie są zmienne w większości środowisk organizacyjnych. Wręcz przeciwnie, ze względu na tendencję do niezmienności w dłuższej perspektywie czasowej zwykle wymagają one rzadszych ocen.

- **Kategoryzacje systemów/Poziomy wpływu**. Zabezpieczenia dotyczące systemów sklasyfikowanych jako systemy o dużym poziomie wpływu winny być monitorowane częściej niż zabezpieczenia systemów o umiarkowanym poziomie wpływu, które z kolei są monitorowane częściej niż zabezpieczenia systemów o niskim poziomie wpływu[42].
- **Zabezpieczenia lub określone obiekty oceny zapewniające funkcje krytyczne**. Zabezpieczenia lub obiekty oceny, które zapewniają kluczowe funkcje bezpieczeństwa (np. serwer zarządzania dziennikami, zapory sieciowe) powinny być monitorowane z większą częstotliwością. Ponadto poszczególne obiekty

[41] Zmienność zabezpieczeń wskazuje na prawdopodobieństwo zmiany danego zabezpieczenia po jego wdrożeniu.

[42] Poziomy wpływu systemu są ustalane zgodnie z normami FIPS 199 (polskojęzyczna publikacja NSC 199) i NIST SP 800-60 (polskojęzyczna publikacja NSC 800-60).

oceny, które obsługują krytyczne funkcje bezpieczeństwa bądź są uważane za kluczowe dla systemu (zgodnie z analizą wpływu na działalność)[43] lub dla organizacji, powinny być monitorowane z większą częstotliwością.

- **Zabezpieczenia ze znanymi podatnościami.** Istniejące zagrożenia udokumentowane w sprawozdaniach z ocen bezpieczeństwa wymagają częstszego monitorowania w celu zapewnienia, że ryzyko pozostaje w granicach tolerancji. Podobnie, zabezpieczenia wymienione w planach i etapach działania posiadające podatności winne być monitorowane z większą częstotliwością do czasu ich usunięcia. Należy pamiętać, że nie wszystkie podatności wymagają takiego samego poziomu monitorowania. Na przykład, podatności opisane w sprawozdaniach z ocen bezpieczeństwa jako związane z nieznacznym lub niskim ryzykiem dla systemu lub organizacji mogą być monitorowane rzadziej niż podatności stanowiące większe zagrożenie dla systemu lub organizacji.
- **Tolerowanie ryzyka w organizacji**[44]**.** Organizacje o niskiej tolerancji na ryzyko, w tym między innymi organizacje przetwarzające, przechowujące lub przesyłające duże ilości informacji wrażliwych bądź danych osobowych, organizacje z licznymi systemami o wysokim poziomie wpływu, a także podmioty stawiające czoła trwałym zagrożeniom powinny przeprowadzać czynności w zakresie monitorowania częściej niż organizacje o wyższej tolerancji na ryzyko, w tym organizacje wykorzystujące systemy o niskim lub umiarkowanym poziome wpływu, przetwarzające, przesyłające lub przechowujące niewielkie ilości danych osobowych lub informacji wrażliwych.
- **Informacje o zagrożeniach**. W procesie ustalania częstotliwości monitorowania organizacje biorą pod uwagę aktualne wiarygodne informacje o zagrożeniach, w tym znanych podatnościach oraz wzorcach ataków[45]. Przykładowo, jeśli

[43] Por. dokument NIST SP 800-34 *Contingency Planning Guide for Federal Information Systems*, maj 2010 z późniejszymi zmianami (polskojęzyczna publikacja NSC 800-34).

[44] Więcej informacji na temat określania tolerancji ryzyka organizacyjnego można znaleźć w dokumencie NIST SP 800-39 z późniejszymi zmianami.

[45] Wzorce ataków to informacje o typowych metodach wykorzystywania podatności w oprogramowaniu w oparciu o dogłębną analizę konkretnych przykładów ataków w świecie

zostanie opracowany konkretny atak, który wykorzystuje podatność w zabezpieczeniach technologii wykorzystywanej przez organizację, tymczasowe lub stałe zwiększenie częstotliwości monitorowania powiązanych zabezpieczeń lub wskaźników może pomóc w zapewnieniu ochrony przed zagrożeniem.

- **Informacje o podatnościach[46].** Ustalając częstotliwość monitorowania, organizacje biorą pod uwagę aktualne informacje o podatnościach dotyczące komponentów systemu informacyjnego. Na przykład, jeśli producent określonego produktu co miesiąc dostarcza poprawki do oprogramowania, organizacja może rozważyć przeprowadzanie skanowania luk w zabezpieczeniach tego produktu co najmniej z taką samą częstotliwością.
- **Wyniki szacowania ryzyka**. W procesie ustalania częstotliwości monitorowania analizowane są i brane pod uwagę wyniki ocen ryzyka (formalnych lub nieformalnych) na poziomie organizacji oraz poszczególnych systemów. Przykładowo, jeśli ocena ryzyka dotycząca określonego systemu wykaże potencjalne zagrożenia i podatności związane z utrzymaniem zdalnym (Zabezpieczenie MA-4 w dokumencie NIST SP 800-53), organizacja może wdrożyć częstsze monitorowanie dokumentacji dotyczącej utrzymania zdalnego oraz działań diagnostycznych. Jeśli w organizacji istnieje program oceny ryzyka, jego wyniki mogą być wykorzystane jako uzasadnienie dla zwiększenia lub zmniejszenia częstotliwości monitorowania powiązanych zabezpieczeń.
- **Wyniki przeglądów strategii monitorowania**. Zagadnienia przeglądu i dostosowania strategii monitorowania zostały szczegółowo omówione w rozdziale 3.6.
- **Wymogi dotyczące sprawozdawczości**. Wymogi dotyczące sprawozdawczości nie wpływają na strategię ciągłego monitorowania bezpieczeństwa informacji, ale mogą odgrywać rolę w ustalaniu częstotliwości monitorowania. Na przykład, jeśli polityki wymagają kwartalnych sprawozdań na temat liczby wykrytych nieautoryzowanych komponentów i podjętych działań naprawczych, organizacja

rzeczywistym. Więcej informacji można znaleźć w witrynie internetowej Common Attack Pattern Enumeration and Classification (CAPEC) pod adresem http://capec.mitre.org/.

[46] Aktualne informacje na temat luk w zabezpieczeniach można znaleźć w witrynach internetowych http://www.kb.cert.org/vuls oraz http://nvd.nist.gov/.

musi monitorować system pod kątem nieautoryzowanych komponentów co najmniej raz na kwartał.

Organizacje koncentrują się na gromadzeniu wymaganych danych z określoną częstotliwością i odpowiednio wykorzystują swoje zasoby ludzkie i kapitał. W miarę zwiększania automatyzacji oraz zasobów, organizacje mogą rozważyć zwiększenie częstotliwości monitorowania. W przypadku spadku dostępności zasobów, organizacja może uwzględnić dostosowanie częstotliwości monitorowania, aby zapewnić, że informacje związane z bezpieczeństwem są odpowiednio analizowane przy jednoczesnym spełnianiu wymogów w zakresie zarządzania ryzykiem organizacyjnym.

Wiele zabezpieczeń zawartych w katalogu dokumentu NIST SP 800-53 charakteryzuje wiele wymagań wdrożeniowych, podobnie jak zabezpieczenia rozszerzone, z którymi wiąże się podobna liczba wymagań. Konieczna może być ocena lub monitorowanie indywidualnych wymogów zabezpieczeń lub zabezpieczeń rozszerzonych z różną częstotliwością. Przykładowo, zabezpieczenie AC-2 — Zarządzanie kontami obejmuje dziesięć oddzielnych wymogów, oznaczonych literami od a do j, w przypadku podstawowego zabezpieczenia, a także cztery zabezpieczenia rozszerzone oznaczone cyframi od 1 do 4. Częstotliwość monitorowania może być różna dla każdego wymogu. Zabezpieczenie AC-2a obejmuje wskazanie rodzajów kont. W przypadku typowego systemu informacyjnego, po określeniu i udokumentowaniu typów kont, zwykle nie będą one ulegać zbyt częstym zmianom. Z tego powodu monitorowanie zabezpieczenia AC-2a może być przeprowadzane stosunkowo rzadko. Zabezpieczenia AC-2h dotyczy dezaktywacji kont tymczasowych i kont zwolnionych lub przeniesionych użytkowników. Ze względu na fakt, że zatrudnianie nowych pracowników oraz zwolnienia są regularnym wydarzeniem w typowej organizacji, zabezpieczenie to wymaga znacznie większej częstotliwości monitorowania niż w przypadku zabezpieczenia AC-2a. Zabezpieczenie rozszerzone AC- 2 (3) wymaga automatycznego wyłączania kont po określonym czasie braku aktywności. Jako zautomatyzowane zabezpieczenie charakteryzujące się wysoką zmiennością, AC-2 (3) wymaga stosunkowo częstego monitorowania, a także może służyć do automatyzacji monitorowania wybranych wymogów podstawowych zabezpieczeń, by można je było

monitorować częściej zgodnie ze strategią ciągłego monitorowania bezpieczeństwa informacji organizacji.

Poziomy organizacji oraz misji i procesów biznesowych.

Na poziomie misji oraz procesów biznesowych organizacja ustala minimalną częstotliwość monitorowania oraz oceny każdego zabezpieczenia oraz wskaźnika. Ustalenia te dotyczą wszystkich systemów w organizacji oraz wspólnych zabezpieczeń i opierają się na kryteriach opisanych w niniejszym rozdziale. Zabezpieczenia wspólne, hybrydowe i specyficzne są uwzględniane w politykach i procedurach na poziomie organizacji oraz misji i procesów biznesowych. Zabezpieczenia wspólne często dotyczą dużej liczby systemów w organizacji. Zbiorcze znaczenie takich zabezpieczeń może wymagać przeprowadzania ocen z większą częstotliwością niż w przypadku podobnych zabezpieczeń odpowiadających za ochronę pojedynczego systemu. Co więcej, określenie częstotliwości oceny zabezpieczeń wspólnych wymaga także określenia przez organizację wiarygodności dostawcy zabezpieczeń wspólnych. Zabezpieczenia wspólne dotyczące procesów, na przykład procedury lub szablony, a także zabezpieczenia należące do kategorii programów zarządzania (PM) nie są w większości przypadków zmienne i zazwyczaj są trudne do automatyzacji. Mimo to organizacja powinna brać pod uwagę zmienność takich zabezpieczeń, a także powiązane informacje o zagrożeniach przy ustalaniu częstotliwości ocen.

Podstawowe role: CIO, SISO.

Role wspierające: Osoba odpowiedzialna za zarządzanie ryzykiem, osoby autoryzujące, dostawca zabezpieczeń wspólnych, właściciel systemu informacyjnego.

Oczekiwane informacje: Ocena ryzyka w organizacji, tolerancja ryzyka organizacyjnego, aktualne informacje o zagrożeniach, wymagania dotyczące sprawozdawczości, aktualne informacje o podatnościach, informacje z przeglądów strategii monitorowania.

Oczekiwane wyniki: Zasady i procedury obowiązujące w całej organizacji, zalecane częstotliwości ocen oraz monitorowania zabezpieczeń i wskaźników.

Poziom systemów informacyjnych.

Na poziomie systemów informacyjnych właściciele systemów dokonują przeglądu minimalnych częstotliwości monitorowania oraz ocen ustanowionych w zasadach na poziomie organizacji lub misji i procesów biznesowych, aby określić, czy minimalne częstotliwości są odpowiednie dla danego systemu informacyjnego. W przypadku niektórych systemów informacyjnych konieczna może okazać się ocena określonych zabezpieczeń lub wskaźników z większą częstotliwością niż zalecana przez organizację zgodnie z kryteriami opisanymi w niniejszym rozdziale. Właściciele systemów powinni również uwzględnić przygotowanie listy wybranych komponentów systemu, które mogą wymagać częstszego monitorowania niż inne komponenty systemu. Mogą znaleźć się na niej między innymi serwery publiczne, urządzenia ochrony granic systemów, a także komponenty uznane za krytyczne w analizie wpływu na działalność.

Podstawowe role: Właściciel systemu informacyjnego, ISSO.

Role wspierające: Osoba autoryzująca, SISO, właściciel informacji/władający informacją.

Oczekiwane informacje: Strategia dla organizacji wraz z wymogami dotyczącymi częstotliwości ocen, aktualne informacje o zagrożeniach, wymagania dotyczące sprawozdawczości, aktualne informacje na temat podatności, wyniki przeglądów strategii monitorowania, plany oceny bezpieczeństwa.

Oczekiwane wyniki: Plany oceny bezpieczeństwa zaktualizowane w celu odzwierciedlenia częstotliwości monitorowania wskaźników i oceny zabezpieczeń specyficznych systemów.

Oceny wynikające ze zdarzeń.

W organizacji mogą mieć miejsce zdarzenia wywołujące natychmiastową potrzebę oceny zabezpieczeń lub weryfikacji stanu bezpieczeństwa poza wymaganiami określonymi w strategii ciągłego monitorowania bezpieczeństwa informacji. Może to wymagać przeprowadzenia nieplanowanej oceny określonej w strategii ciągłego monitorowania bezpieczeństwa informacji lub niestandardowej oceny dostosowanej do nowych potrzeb, na przykład zmiany sposobu planowanej oceny lub częstotliwości monitorowania. Przykładowo, jeśli do systemu dodawana jest aplikacja internetowa,

istniejący proces ciągłego monitorowania bezpieczeństwa informacji, który obejmuje zarządzanie konfiguracją i zabezpieczeniami, analizy wpływu na bezpieczeństwo, analizowanie podatności i inne elementy może być wystarczający do oceny zabezpieczeń wdrożonych dla nowej aplikacji internetowej.

Podczas określania kryteriów ocen wynikających ze zdarzeń, organizacje winny brać pod uwagę zdarzenia takie jak incydenty, pojawienie się nowych informacji o zagrożeniach, znaczące zmiany w systemach i środowiskach eksploatacji, nowe lub dodatkowe obowiązki związane z misją oraz wyniki analizy wpływu na bezpieczeństwo lub oceny ryzyka.

W zależności od znaczenia zdarzenia, ocena oparta na zdarzeniu może wymagać ponownej autoryzacji jednego lub wielu systemów.

Podstawowe role: Właściciel systemu informacyjnego, dostawca zabezpieczeń wspólnych, osoba autoryzująca, ISSO.

Role wspierające: Osoba odpowiedzialna za zarządzanie ryzykiem, SISO, oceniający środki bezpieczeństwa.

Oczekiwane informacje: Ocena ryzyka organizacyjnego, tolerancja ryzyka organizacyjnego, bieżące informacje o zagrożeniach, bieżące informacje o podatnościach, priorytety i oczekiwania organizacji.

Oczekiwane wyniki: Udokumentowane kryteria i progi wywołujące przeprowadzenie oceny lub autoryzacji, na przykład procedury dotyczące znaczących zmian, polityki i procedury dotyczące autoryzacji związanych ze zdarzeniami.

3.2.3. OPRACOWANIE ARCHITEKTURY CIĄGŁEGO MONITOROWANIA BEZPIECZEŃSTWA INFORMACJI

Organizacja określa, w jaki sposób informacje będą gromadzone wewnątrz organizacji oraz przekazywane w ramach poszczególnych poziomów oraz między poziomami, uwzględniając także informacje zewnętrzne. Podstawowe wymagania wobec architektury wykorzystywanej w ramach wsparcia ciągłego monitorowania bezpieczeństwa informacji obejmują gromadzenie i przechowywanie danych, ich

analizę oraz możliwości wyszukiwania i prezentacji do celów sprawozdawczości. Metodyki są znormalizowane w celu zapewnienia większej sprawności, uproszczenia wymiany informacji w ramach poziomów oraz pomiędzy nimi, a także umożliwienia korelowania danych oraz analiz.

Organizacje wykorzystują zautomatyzowane narzędzia, technologie i metodyki wszędzie tam, gdzie jest to wskazane, by zwiększyć sprawność oraz poprawić wgląd w uzyskane wnioski oparte na gromadzeniu, analizie i rozpowszechnianiu dużych ilości danych z różnych źródeł. Architektura i związane z nią zasady i procedury powinny zostać zaprojektowane tak, aby zminimalizować liczbę wywołań danych i zmaksymalizować ich ponowne wykorzystanie[47]. Dane pochodzą z wielu źródeł, w tym z pakietów autoryzacyjnych, dokumentacji szkoleń oraz dzienników systemowych, a także uwzględniają punkty widzenia różnych interesariuszy. Interoperacyjne specyfikacje, takie jak na przykład SCAP bądź XML, umożliwiają jednorazowe gromadzenie danych i ich wielokrotne wykorzystywanie. Odpowiedzialność za różne aspekty stanu bezpieczeństwa może spoczywać na różnych rolach lub funkcjach w organizacji, w związku z czym może wymagać wykorzystania surowych danych na potrzeby różnych wskaźników, w różnych kontekstach oraz w różnych odstępach czasu, na przykład na potrzeby ocen bezpieczeństwa oraz autoryzacji, zwiększania świadomości użytkowników, prowadzenia szkoleń oraz kontroli dostępu. Także misje oraz funkcje biznesowe organizacji mają różne wymagania w zakresie sprawozdawczości oraz różne wskazania do podjęcia działań, na przykład zmiany tolerancji ryzyka, zmiany w środowiskach eksploatacji, nowe zagrożenia, zmiany w architekturze bezpieczeństwa oraz potrzeby w zakresie sprawozdawczości dotyczącej bezpieczeństwa.

[47] Przykład architektury ciągłego monitorowania bezpieczeństwa informacji można znaleźć w wersji roboczej dokumentu NISTIR 7756 *CAESARS Framework Extension*: *An Enterprise Continuous Monitoring Technical Reference Architecture (Draft)*.

3.3. WDROŻENIE PROGRAMU CIĄGŁEGO MONITOROWANIA BEZPIECZEŃSTWA INFORMACJI

Ciągłe monitorowanie bezpieczeństwa informacji jest wdrażane zgodnie ze strategią. Informacje i dane związane z bezpieczeństwem są gromadzone zgodnie z wymaganiami dotyczącymi uprzednio określonych wskaźników, przeprowadzane są oceny zabezpieczeń, a uzyskane informacje związane z bezpieczeństwem są przekazywane zgodnie z zasadami i procedurami organizacyjnymi. *Wszystkie* klasy zabezpieczeń (zarządcze, operacyjne i techniczne) oraz ich rodzaje (wspólne, hybrydowe i specyficzne dla systemu) są uwzględnione w organizacyjnym programie ciągłego monitorowania. Wszystkie zabezpieczenia są monitorowane pod kątem skuteczności i wykorzystywane w celu monitorowania stanu bezpieczeństwa. Źródła danych obejmują pracowników, procesy, technologie, środowisko obliczeniowe, a także wszelkie istniejące sprawozdania z oceny zabezpieczeń.

Gromadzenie, analiza i raportowanie danych powinny być w miarę możliwości zautomatyzowane. Niezależnie od tego, czy dane są gromadzone ręcznie, czy automatycznie, powinny być zestawione w celu analizy i przekazywane osobom odpowiedzialnym za ich korelację i analizę na potrzeby działań związanych z zarządzaniem ryzykiem. Jak wskazano w powyższych przykładach, może to oznaczać gromadzenie danych z różnych źródeł w różnych punktach w czasie, a także zestawianie ich na potrzeby wykorzystania przez osoby otrzymujące je w momencie, gdy jest to wymagane. Częścią etapu wdrażania procesu ciągłego monitorowania jest skuteczne organizowanie i dostarczanie danych z procesu ciągłego monitorowania bezpieczeństwa informacji interesariuszom zgodnie z wymogami decyzyjnymi. Narzędzia i metodologie dobierane z myślą o architekturze ciągłego monitorowania bezpieczeństwa informacji obejmującej całą organizację powinny pozwalać na zapewnienie, że decyzje oparte na ryzyku są oparte na dokładnych, aktualnych danych dotyczących bezpieczeństwa.

Procesy dotyczące bezpieczeństwa wpływają na dane z procesu ciągłego monitorowania bezpieczeństwa informacji i opierają się na tych danych. Organizacje wykorzystują również dane z ciągłego monitorowania bezpieczeństwa informacji w procesach, które nie są wykorzystywane w celu ograniczania ryzyka związanego z bezpieczeństwem

informacji. Dane z tych procesów mogą być również wykorzystywane na potrzeby procesu ciągłego monitorowania bezpieczeństwa informacji. Przykłady takich procesów obejmują między innymi zarządzanie poprawkami, zasobami, licencjami, konfiguracją, podatnościami i autoryzację systemów.

Jak opisano w rozdziale drugim, dane wyjściowe dotyczące ciągłego monitorowania bezpieczeństwa informacji z jednego procesu mogą służyć jako dane wejściowe dla wielu innych procesów.

Podstawowe role: Właściciel systemu informacyjnego, dostawca zabezpieczeń wspólnych, ISSO, oceniający środki bezpieczeństwa.

Role wspierające: Osoba odpowiedzialna za zarządzanie ryzykiem, osoba autoryzująca, CIO, SISO.

Oczekiwane informacje: Zasady i procedury na poziomie organizacyjnym i systemów informacyjnych dotyczące strategii ciągłego monitorowania bezpieczeństwa informacji, wskaźników i planu oceny bezpieczeństwa zaktualizowane o interwały ocen i monitorowania, specyfikacje automatyzacji.

Oczekiwane wyniki: Informacje związane z bezpieczeństwem.

3.4. ANALIZA DANYCH I OPRACOWYWANIE SPRAWOZDAŃ Z WYNIKAMI

Organizacje opracowują procedury analizy oraz sprawozdań z wyników procesów oceny i monitorowania. Proces ten obejmuje określonych pracowników oraz określone role otrzymujące sprawozdania dotyczące ciągłego monitorowania bezpieczeństwa informacji, treść i format sprawozdań, częstotliwość ich opracowywania oraz wszelkie narzędzia, które mają być używane w ramach tego zadania. Obejmuje także wymagania dotyczące analizowania i raportowania wyników oceny zabezpieczeń, których automatyzacja jest szczególnie trudna. Konieczne może być zebranie dodatkowych danych w celu uzupełnienia lub wyjaśnienia analizowanych informacji związanych z bezpieczeństwem lub dostarczonych we wstępnych sprawozdaniach. Pracownicy na poziomach systemów

informacyjnych oraz misji i procesów biznesowych opracowują i przekazują sprawozdania zgodnie z wymaganiami zasad i procedur obowiązujących na poziomach organizacji oraz misji i procesów biznesowych.

3.4.1. ANALIZA DANYCH

Organizacje analizują informacje związane z bezpieczeństwem wynikające z ciągłego monitorowania bezpieczeństwa informacji. Konieczne może być zebranie dodatkowych danych w celu uzupełnienia lub wyjaśnienia analizowanych informacji związanych z bezpieczeństwem. Informacje do analizy są dostarczane przedstawicielom organizacji w ramach sprawozdań cyklicznych, sprawozdań automatycznych, sprawozdań „ad hoc", w źródeł danych oraz baz danych. Informacje związane z bezpieczeństwem wynikające z ciągłego monitorowania bezpieczeństwa informacji są analizowane w kontekście określonych tolerancji ryzyka, potencjalnego wpływu podatności na systemy informacyjne, misję i procesy biznesowe, a także organizację jako całość oraz potencjalnego wpływu opcji łagodzących. Nawet w przypadku gromadzonych w czasie rzeczywistym lub zbliżonym do rzeczywistego informacji dotyczących bezpieczeństwa organizacji i systemów informacyjnych, analiza zawsze uwzględnia zmieniające się dane dotyczące podatności i zagrożeń. Przedstawiciele organizacji dokonują przeglądu przeanalizowanych sprawozdań w celu ustalenia, czy należy wdrożyć działania łagodzące, czy też przenieść, odrzucić lub zaakceptować ryzyko. W niektórych przypadkach osoby autoryzujące mogą stwierdzić, że zaakceptowanie określonego ryzyka jest lepszym rozwiązaniem niż wdrożenie działań łagodzących. Uzasadnieniem dla takich wniosków może być tolerancja ryzyka organizacyjnego, negatywny wpływ na misję lub procesy biznesowe, a także brak opłacalności lub zwrotu z inwestycji w daną technologię. Rozwiązanie problemu ryzyka i uzasadnienie decyzji jest dokumentowanie zgodnie z zasadami i procedurami organizacyjnymi.

Podstawowe role: Osoba odpowiedzialna za zarządzanie ryzykiem, CIO, SISO, osoba autoryzująca, oceniający środki bezpieczeństwa.

Role wspierające: Właściciele systemów informacyjnych, dostawca zabezpieczeń wspólnych, specjaliści ds. bezpieczeństwa systemów.

Oczekiwane informacje: Informacje związane z bezpieczeństwem, organizacyjna strategia ciągłego monitorowania bezpieczeństwa informacji, tolerancja ryzyka organizacyjnego, wymagania dotyczące sprawozdawczości.

Oczekiwane wyniki: Analiza informacji o stanie bezpieczeństwa dla wszystkich poziomów; zaktualizowany plan bezpieczeństwa systemu, sprawozdanie z oceny bezpieczeństwa oraz plan i etapy działania, zmienione decyzje dotyczące zarządzania ryzykiem w organizacji.

3.4.2. SPRAWOZDANIE Z OCENY ZABEZPIECZEŃ

Organizacje opracowują sprawozdania z oceny skuteczności wszystkich wdrożonych zabezpieczeń zgodnie z wymogami organizacyjnymi. Informacje związane z bezpieczeństwem pochodzące z ocen mogą być przekazywane w szablonach lub arkuszach kalkulacyjnych lub gromadzone i raportowane w sposób zautomatyzowany. Na poziomie systemów informacyjnych, informacje związane z bezpieczeństwem pochodzące z ocen bezpośrednio wspierają bieżące decyzje dotyczące autoryzacji i planów działania oraz tworzenie i śledzenie planów i etapów działania. Niektóre zabezpieczenia lub ich elementy z definicji stanowią wskaźniki bezpieczeństwa, na przykład SI-4 – Monitorowanie systemu. W związku z tym ocena skuteczności tych zabezpieczeń stanowi zarazem przykład monitorowania stanu bezpieczeństwa oraz powiązanego wskaźnika. Pracownicy przekazują wyniki oceny zgodnie z zasadami i procedurami obowiązującymi w organizacji. Organizacje wyższego szczebla mogą wymagać przekazywania informacji na temat dodatkowych wskaźników bądź wyników oceny. Organizacje określają wymagania dotyczące raportowania stanu bezpieczeństwa w strategii ciągłego monitorowania bezpieczeństwa informacji. Proces ten obejmuje określonych pracowników oraz określone role otrzymujące sprawozdania dotyczące ciągłego monitorowania bezpieczeństwa informacji, treść i format sprawozdań, częstotliwość ich opracowywania oraz wszelkie narzędzia, które mają być używane w ramach tego zadania.

Przedstawiciele poziomu 3 sporządzają sprawozdania ze swoimi ustaleniami, dokumentują wszelkie wdrożone działania na poziomie systemów bądź przedstawiają zalecenia przedstawicielom poziomów 1 i 2. Przedstawiciele

organizacji na poziomach 1 i 2 dokonują przeglądu sprawozdań z poziomu 3 w celu określenia stanu bezpieczeństwa oraz skuteczności i adekwatności *wszystkich zabezpieczeń* w zakresie spełniania wymagań dotyczących bezpieczeństwa informacji związanych z misją, procesami biznesowymi i organizacją. Informacje zawarte w sprawozdaniach będą się różnić w zależności od jego odbiorców, częstotliwości, celu, obsługiwanych zestawów narzędzi i stosowanych wskaźników. Na przykład osoba odpowiedzialna za zarządzanie ryzykiem może otrzymywać ogólny raport na temat wszystkich systemów raz do roku oraz szczegółowy raport na temat konkretnych systemów o wysokim poziomie wpływu raz na kwartał. Sprawozdania przekazywane CIO i SISO mogą zawierać bardziej szczegółowe dane techniczne dotyczące wszystkich systemów kwartalnie, a osoba autoryzująca może otrzymywać miesięczne kompleksowe sprawozdania dotyczące systemów, za które odpowiada. Zespół reagowania na incydenty komputerowe (CIRT) może otrzymywać raporty o wyjątkach, gdy generowane są alarmy, a administratorzy sieci mogą przeglądać pulpity nawigacyjne pokazujące aktywność sieci, które są aktualizowane co minutę, a także podsumowania wskaźników aktualizowane co godzinę lub codziennie[48]. Organizacje mogą uwzględnić możliwość przygotowywania częstszych sprawozdań w przypadku określonych zabezpieczeń o większej zmienności lub zabezpieczeń, w przypadku których wystąpiły podatności lub brak zgodności.

Organizacje określają również wymagania dotyczące sprawozdań obejmujących działanie zabezpieczeń, w tym między innymi zabezpieczeń z kategorii PM, których analiza jest trudna do zautomatyzowania. Organizacje opracowują procedury gromadzenia wyników procesów oceny i monitorowania, w tym wyników uzyskanych przy pomocy metod ręcznych, opracowywania sprawozdań, a także gromadzenia informacji z planów i etapów działań, które mogą być wykorzystywane do określania częstotliwości, raportowania stanu i przeglądu strategii monitorowania.

Podstawowe role: Właściciel systemu, dostawca zabezpieczeń wspólnych, oceniający środki bezpieczeństwa, SSO.

[48] Podane w niniejszym rozdziale interwały służą wyłącznie celom ilustracyjnym.

Role wspierające: Osoba odpowiedzialna za zarządzanie ryzykiem, CIO, CISO, osoba autoryzująca.

Oczekiwane informacje: Informacje związane z bezpieczeństwem (wyniki oceny); zasady i procedury ciągłego monitorowania bezpieczeństwa informacji w organizacji, wymagania dotyczące raportowania przekazane przez osobę autoryzującą, CIO, CISO lub osobę odpowiedzialną za zarządzanie ryzykiem.

Oczekiwane wyniki: Sprawozdania z wyników oceny zgodnie z wymaganiami zasad i procedur ciągłego monitorowania bezpieczeństwa informacji w organizacji oraz osoby autoryzującej w celu wsparcia bieżącej autoryzacji (lub ponownej autoryzacji).

3.4.3. SPRAWOZDANIE Z MONITOROWANIA STANU BEZPIECZEŃSTWA

Organizacje opracowują procedury opracowywania sprawozdań z monitorowania stanu bezpieczeństwa. Dane dotyczące stanu bezpieczeństwa pochodzą z monitorowania wstępnie określonych wskaźników w całej organizacji na podstawie danych wyjściowych generowanych przez narzędzia obejmujące całą organizację, często wdrażanych jako zabezpieczenia wspólne. Narzędzia obejmujące całą organizację mogą być częścią określonego systemu lub systemów, jednak wytwarzane informacje związane z bezpieczeństwem mogą nie dotyczyć wyłącznie określonego systemu.

Podstawowe role: Właściciel systemu, dostawca zabezpieczeń wspólnych, oceniający środki bezpieczeństwa, SSO.

Role wspierające: Osoba odpowiedzialna za zarządzanie ryzykiem, CIO, CISO, osoba autoryzująca.

Oczekiwane informacje: Informacje związane z bezpieczeństwem (dane dotyczące stanu bezpieczeństwa), zasady i procedury ciągłego monitorowania bezpieczeństwa informacji w organizacji, wymagania dotyczące raportowania przekazane przez osobę autoryzującą, CIO, CISO lub osobę odpowiedzialną za zarządzanie ryzykiem.

Oczekiwane wyniki: Sprawozdania dotyczące stanu bezpieczeństwa zgodnie z wymaganiami zasad i procedur ciągłego monitorowania bezpieczeństwa informacji w organizacji oraz osoby autoryzującej w celu wsparcia bieżącej autoryzacji (lub ponownej autoryzacji).

3.5. REAKCJA NA USTALENIA

Informacje związane z bezpieczeństwem uzyskane w wyniku monitorowania są analizowane i wywołują odpowiednie reakcje. Reakcja na ustalenia na wszystkich poziomach może obejmować ograniczanie ryzyka, akceptację ryzyka, unikanie lub odrzucenie ryzyka lub dzielenie się ryzykiem, a także jego przekazywanie zgodnie z wymogami organizacji w zakresie tolerancji na ryzyko[49].

Reakcje są skoordynowane z odpowiednimi działaniami związanymi z zarządzaniem bezpieczeństwem, takimi jak program zarządzania konfiguracją zorientowanego na bezpieczeństwo. Na poziomie 1 reakcja na ustalenia może skutkować zmianami w zasadach bezpieczeństwa związanych z ładem organizacji oraz jej zarządzaniem. Jednocześnie reakcja ta może być ograniczona przez misje i procesy biznesowe oraz ograniczenia architektury korporacyjnej (w tym czynników ludzkich), niezmienne zasady zarządzania lub inne czynniki zewnętrzne. Na poziomie 2 reakcja na ustalenia może obejmować prośby o dodatkowe informacje związane z bezpieczeństwem, nowe lub zmodyfikowane wskaźniki, zmiany w misjach i procesach biznesowych oraz wymaganiach dotyczących sprawozdawczości na poziomie 3, a także zmiany we wspólnych zabezpieczeniach lub ich uzupełnienie. Reakcję na poziomie 2 mogą ograniczać zasady organizacji oraz strategie zarządzania, a także cele i zadania misji i procesów biznesowych oraz ograniczenia dotyczące zasobów i infrastruktury organizacyjnej. Na poziomie 3 działania łagodzące mają bezpośredni i natychmiastowy wpływ na ryzyko na poziomie systemów, a reakcje na ustalenia mogą obejmować wdrożenie dodatkowych zabezpieczeń, modyfikacje wcześniej wdrożonych zabezpieczeń, usunięcie upoważnienia do działania, zmiany częstotliwości

[49] Szczegółowy opis procesu reagowania na ryzyko znajduje się w dokumencie NIST SP 800-39 z późniejszymi zmianami.

monitorowania, a także przeprowadzenie dodatkowych lub bardziej szczegółowych analiz informacji związanych z bezpieczeństwem. Takie działania na poziomie systemów są wprowadzane w ramach ograniczeń określonych przez zasady, wymagania i strategie poziomów 1 i 2, aby zapewnić, że nie wpłynie to negatywnie na procesy organizacyjne.

Strategie reagowania mogą być wdrażane przez pewien okres, a wszelkie zmiany powinny być dokumentowane w planie i etapach działania dla systemu. Po wykryciu podatności działania powinny być ocenione, a działania łagodzące powinny być wdrożone natychmiast lub dodane do planów i etapów działania. Inne kluczowe dokumenty dotyczące systemu powinny zostać odpowiednio aktualizowane. Zabezpieczenia modyfikowane, ulepszane lub dodawane w ramach etapu reagowania w procesie ciągłego monitorowania, powinny być oceniane w celu zapewnienia, że nowe lub zmienione zabezpieczenia są skuteczne[50].
W przyszłości nowe lub zmienione zabezpieczenia powinny zostać uwzględnione w ogólnej strategii ciągłego monitorowania.

Podstawowe role: Właściciel systemu, dostawca zabezpieczeń wspólnych, SSO.

Role wspierające: Osoba autoryzująca, SISO, właściciel informacji/władający informacją.

Oczekiwane informacje: Sprawozdania dotyczące stanu bezpieczeństwa, sprawozdania z wyników ocen (np. sprawozdania z ocen bezpieczeństwa), oceny ryzyka na poziomie organizacji i systemu, plany oceny bezpieczeństwa, plany bezpieczeństwa systemu, procedury i szablony dla organizacji.

Oczekiwane wyniki: Decyzje dotyczące reagowania na ryzyko, zaktualizowane informacje o bezpieczeństwie systemu (np. plany bezpieczeństwa systemu, plany i etapy działania, sprawozdania z oceny bezpieczeństwa), zaktualizowane sprawozdania o stanie bezpieczeństwa.

[50] Zmiany w zabezpieczeniach winny być wdrażane po pełnym przetestowaniu, weryfikacji i przeglądzie w środowisku testowym.

3.6. PRZEGLĄD I AKTUALIZACJA PROGRAMU I STRATEGII MONITOROWANIA

Strategie i programy ciągłego monitorowania bezpieczeństwa informacji nie są statycznymi dokumentami. Oceny zabezpieczeń, wskaźniki stanu bezpieczeństwa oraz częstotliwość monitorowania i oceny zmieniają się wraz z potrzebami organizacji. Strategia ciągłego monitorowania powinna być poddawana przeglądowi w celu upewnienia się, że w wystarczającym stopniu pozwala organizacji na działalność w ramach akceptowalnych poziomów tolerancji ryzyka, że wskaźniki pozostają istotne, a dane są aktualne i kompletne. Przegląd strategii pozwala także na określenie sposobów poprawy wglądu w stan bezpieczeństwa, skutecznie wspiera świadome podejmowanie decyzji w zakresie zarządzania ryzykiem i bieżące autoryzacje oraz poprawia zdolność organizacji do reagowania na znane i nowe zagrożenia.

Organizacja ustanawia procedurę przeglądu i modyfikacji wszystkich aspektów strategii ciągłego monitorowania bezpieczeństwa informacji, w tym weryfikacji użyteczności ogólnej strategii, dokładności w odzwierciedlaniu tolerancji ryzyka organizacyjnego, dokładności i poprawności pomiarów i przydatności wskaźników, wymagań dotyczących sprawozdawczości oraz częstotliwości monitorowania i oceny. Jeśli którekolwiek z gromadzonych danych nie są wymagane do celów sprawozdawczości lub nie są przydatne z punktu widzenia utrzymania lub poprawy stanu bezpieczeństwa organizacji, wówczas organizacja może rozważyć możliwość zaoszczędzenia zasobów poprzez zaprzestanie gromadzenia tych konkretnych danych. Czynniki powodujące zmiany w strategii monitorowania mogą obejmować między innymi:

- Zmiany w podstawowych misjach lub procesach biznesowych.
- Znaczące zmiany w architekturze korporacyjnej (w tym dodanie nowych lub wyłączenie istniejących systemów).
- Zmiany w tolerancji ryzyka organizacyjnego.
- Nowe informacje o zagrożeniach.
- Nowe informacje o podatnościach.

- Zmiany w systemach informacyjnych (w tym zmiany dotyczące kategorii bezpieczeństwa lub poziomu wpływu).
- Zwiększenie lub zmniejszenie liczby planów i etapów działania związanych z określonymi zabezpieczeniami.
- Analizy trendów na podstawie sprawozdań.
- Nowe przepisy lub regulacje.
- Zmiany w wymogach dotyczących sprawozdawczości.

Przedstawiciele organizacji analizują zestawienia planów i etapów działania w celu ustalenia, czy istnieją wspólne podatności lub braki dotyczące systemów informacyjnych organizacji, a następnie proponują rozwiązania lub wnioskują o ich wypracowanie. Zestawienia informacji z planów i etapów działania są wykorzystywane w celu organizacji zasobów ograniczających ryzyko w całej organizacji oraz do wprowadzania zmian w strategii monitorowania. Z kolei sprawozdania o stanie bezpieczeństwa i wskaźniki są analizowane w celu określenia, czy istnieją jakiekolwiek trendy w zakresie bezpieczeństwa, które sugerują, że konieczne mogą być zmiany w strategii monitorowania. Na przykład, jeśli cotygodniowe oceny inwentaryzacji komponentów w okresie sześciu miesięcy wskazują, że w danym tygodniu wprowadzanych jest bardzo niewiele zmian, a zmiany, które *zostały* wprowadzone, są dokładnie odzwierciedlone w inwentaryzacjach, organizacja może podjąć decyzję o zmniejszeniu częstotliwości monitorowania inwentaryzacji komponentów do dwutygodniowej lub miesięcznej.

Z kolei jeśli cotygodniowe analizy sprawozdań z ocen w okresie sześciu miesięcy wskazują na wzrost liczby anomalii, organizacja może postanowić zwiększyć częstotliwość przeglądów, by odbywały się raz w tygodniu.

Strategia ciągłego monitorowania bezpieczeństwa informacji organizacji zmienia się wraz z rozwojem programów bezpieczeństwa i możliwości monitorowania. W przypadku dojrzałego programu gromadzenie i analiza informacji związanych z bezpieczeństwem odbywa się przy użyciu znormalizowanych metod w całej

organizacji, stanowi integralną część misji i procesów biznesowych oraz jest zautomatyzowana w możliwie najszerszym zakresie. W tym przypadku program bezpieczeństwa jest wystarczająco dojrzały, aby zapewnić, że istniejące procesy i procedury skutecznie zabezpieczają architekturę korporacyjną zgodnie z tolerancją ryzyka organizacyjnego oraz pozwalają na gromadzenie, korelowanie, analizowanie wskaźników bezpieczeństwa i przygotowywanie stosownych sprawozdań[51].

Proces ciągłego monitorowania bezpieczeństwa informacji jest procesem rekurencyjnym – strategia monitorowania jest stale udoskonalana w miarę powtarzania kolejnych etapów procesu. Co więcej, zastosowanie ciągłego monitorowania bezpieczeństwa informacji w całej organizacji odbywa się w wyniku działań na poziomach misji i procesów biznesowych oraz systemów. Innymi słowy, wyniki ciągłego monitorowania bezpieczeństwa informacji na poziomie 3 stanowią wkład w realizację programów ISCM na poziomach 1 i 2. Przechodząc od szczytu piramidy na rysunku 2-1 (poziom 1) do jej podstawy (poziom 3) widzimy, że strategie monitorowania wyższego poziomu określają parametry dla programów monitorowania na niższych poziomach, a obserwacje poczynione na niższych poziomach mogą skutkować zmianami w strategiach monitorowania wyższego poziomu. Sam program ciągłego monitorowania bezpieczeństwa informacji musi być monitorowany, aby mógł rozwijać się wraz ze zmianami w misjach i celach organizacyjnych, środowiskach operacyjnych i zagrożeniach.

Podstawowe role: SISO, osoba autoryzująca, właściciel systemu informacyjnego, dostawca zabezpieczeń wspólnych.

Role wspierające: Osoba odpowiedzialna za zarządzanie ryzykiem, CIO, ISSO.

Oczekiwane informacje: Analizy trendów na podstawie monitorowania, informacje o tolerancji ryzyka w organizacji, informacje o nowych przepisach, regulacjach, wymogach dotyczących sprawozdawczości, bieżące informacje o zagrożeniach

[51] Więcej informacji na temat wskaźników związanych z bezpieczeństwem znajduje się w dokumencie NIST SP 800-55 z późniejszymi zmianami.

i podatnościach, inne informacje dotyczące organizacji zgodne z wymogami, aktualizacje specyfikacji automatyzacji.

Oczekiwane wyniki: Zmieniona strategia ISCM lub krótkie sprawozdanie zawierające informacje na temat szczegółów przeglądu wraz z informacją, że zmiany strategii nie były konieczne (zgodnie z ustalonym procesem przeglądu).

ZAŁĄCZNIK A – BIBLIOGRAFIA

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[52]	
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

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

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[52]	
NSC 800-53B	Zabezpieczenia bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B
NSC 800-53 MAP	Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 Patrz: SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)
NSC 800-60	Wytyczne w zakresie określania kategorii bezpieczeństwa informacji I kategorii bezpieczeństwa systemu informacyjnego – na podstawie NIST SP 800-60
NSC 800-61	Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego – na podstawie NIST SP 800-61

PUBLIKACJE ANGLOJĘZYCZNE[53]	
PRZEPISY	
1.	E-Government Act [obejmuje ustawę FISMA] (P.L. 107-347), grudzień 2002 roku.
ZASADY, DYREKTYWY, INSTRUKCJE	
1.	Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, listopad 2000.
2.	Office of Management and Budget Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, październik 2001.
3.	Cyber Security Research and Development Act, 2002.
WYTYCZNE	
1.	National Institute of Standards and Technology Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, październik 1995.
2.	National Institute of Standards and Technology Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, maj 2010.
3.	National Institute of Standards and Technology Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*: *A Security Life Cycle Approach*, luty 2010.
4.	National Institute of Standards and Technology Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, marzec 2011.
5.	National Institute of Standards and Technology Special Publication 800-40, Version 2, *Creating a Patch and Vulnerability Management Program*, listopad 2005.
6.	National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, sierpień 2009.

[53] Publikacje angielskojęzyczne zostały wymienione w celach uzupełniających dla osób zainteresowanych.

7. National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*: *Building Effective Security Assessment Plans*, czerwiec 2010.
8. National Institute of Standards and Technology Special Publication 800-55, Revision 1, *Performance Measurement Guide for Information Security*, lipiec 2008.
9. National Institute of Standards and Technology Special Publication 800-92, *Guide to Computer Log Management*, wrzesień 2006.
10. National Institute of Standards and Technology Special Publication 800-126, Revision 1, *The Technical Specification for the Security Content Automation Protocol (SCAP)*: *SCAP Version 1.1*, luty 2011.
11. National Institute of Standards and Technology Special Publication 800-128, Guide for Security-Focused Configuration Management of Information Systems, sierpień 2011.
12. National Institute of Standards and Technology Interagency Report 7756, DRAFT, CAESARS Framework Extension: an Enterprise Continuous Monitoring Technical Reference Architecture, luty 2011.

INNE

1. Common Vulnerabilities and Exposures (CVE), http://cve.mitre.org/about/index.html.
2. Common Vulnerability Scoring System (CVSS), http://www.first.org/cvss/.

ZAŁĄCZNIK B – SŁOWNIK

PODSTAWOWE TERMINY I DEFINICJE

Niniejszy załącznik zawiera definicje terminologii związanej z bezpieczeństwem, używanej w publikacji NIST SP 800-137. Terminy w słowniku są spójne z terminami używanymi w pakiecie norm i wytycznych w zakresie bezpieczeństwa związanych z ustawą FISMA opracowanych przez NIST. O ile nie zaznaczono inaczej, wszystkie terminy użyte w niniejszej publikacji są również zgodne z definicjami zawartymi w Instrukcji CNSS 4009: *National Information Assurance Glossary*.

Dodatkowo patrz: NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*.

Terminologia angielska	Terminologia polska	Definicja
Activities [NISTIR 7298]	Działania [NISTIR 7298]	Obiekt oceny, który obejmuje określone działania związane z ochroną lub działania wspierające system informacyjny, które obejmują pracowników, na przykład tworzenie kopii zapasowych systemu, monitorowanie ruchu sieciowego.
Adequate Security [OMB Circular A-130, Appendix III]	Stosowne bezpieczeństwo [OMB Circular A-130, Załącznik III]	Bezpieczeństwo współmierne do ryzyka i skali szkód wynikających z utraty, modyfikacji, nadużycia lub nieautoryzowanego dostępu do informacji. Obejmuje zapewnienie, że systemy i aplikacje używane przez organizację działają skutecznie i zapewniają odpowiednią poufność, integralność i dostępność danych poprzez wykorzystanie stosownych i efektywnych kosztowo zabezpieczeń w zakresie zarządzania, operacyjnych, technicznych oraz personelu.
Advanced Persistent	Zaawansowane zagrożenie trwałe	Adwersarz, który posiada zaawansowany poziom wiedzy specjalistycznej i znaczne zasoby, co

Terminologia angielska	Terminologia polska	Definicja
Threats [NIST SP 800-39]	[NIST SP 800-39]	pozwala mu stwarzać okazje do osiągania swoich celów przy użyciu wielu wektorów ataku (np. cyberataku, ataku bezpośredniego i podstępu). Do celów tych należy zazwyczaj ustanowienie/rozszerzenie dostępu do infrastruktury informatycznej organizacji będących celem ataku w celu wydostania informacji, podważenia lub utrudnienia krytycznych aspektów misji, programu lub organizacji, lub też pozycjonowanie się w celu realizacji tych celów w przyszłości. Zaawansowane trwałe zagrożenie realizuje wielokrotnie swoje cele w dłuższym okresie; dostosowuje się do wysiłków obrońców próbujących mu się przeciwstawić oraz jest zdeterminowane, aby utrzymać poziom interakcji niezbędny do realizacji swoich celów.
Agency	Jednostka organizacyjna/ organizacja	Wyspecjalizowana jednostka organizacyjna o dowolnej wielkości, złożoności lub pozycjonowaniu w ramach struktury organizacyjnej (np. przedsiębiorstwo, urząd, itp., lub w stosownych przypadkach, którykolwiek z elementów operacyjnych przedsiębiorstwa, urzędu, itp.)

Terminologia angielska	Terminologia polska	Definicja
Allocation [NISTIR 7298]	Alokacja/ przydział [NISTIR 7298]	Proces stosowany przez organizację w celu określenia, czy zabezpieczenia są zdefiniowane jako specyficzne dla systemu, hybrydowe czy wspólne. Proces stosowany przez organizację w celu przypisania zabezpieczeń do określonych komponentów systemu informacyjnego odpowiedzialnych za zapewnienie określonej funkcji bezpieczeństwa, takich jak router, serwer, zdalny czujnik.
Application [NISTIR 7298]	Aplikacja [NISTIR 7298]	Program obsługiwany przez system informacyjny.
Assessment	Ocena	Por. *Ocena środków bezpieczeństwa*.
Assessment Findings [NISTIR 7298]	Wyniki oceny [NISTIR 7298]	Wyniki oceny uzyskane w wyniku zastosowania procedury oceny do zabezpieczeń lub zabezpieczeń rozszerzonych w celu uzyskania celu oceny; ustalenie dokonane przez osobę oceniającą w ramach procedury oceny, które skutkuje uzyskaniem stanu *spełniającego wymogi* lub innym niż *spełniający wymogi*.
Assessment Method [NISTIR 7298]	Metoda oceny [NISTIR 7298]	Jeden z trzech rodzajów działań (badanie, wywiad, test) podejmowanych przez oceniających w celu gromadzenia dowodów podczas oceny.
Assessment Object [NISTIR 7298]	Obiekt oceny [NISTIR 7298]	Element (specyfikacje, mechanizmy, działania, osoby), do którego stosuje się metodę oceny podczas procesu oceny.
Assessment Objective [NISTIR 7298]	Cel oceny [NISTIR 7298]	Zestaw ustaleń, które wyrażają pożądany wynik oceny zabezpieczeń lub zabezpieczeń rozszerzonych.

Terminologia angielska	Terminologia polska	Definicja
Assessment Procedure [NISTIR 7298]	Procedura oceny [NISTIR 7298]	Zestaw *celów* oceny oraz powiązany zestaw *metod* i *obiektów* oceny.
Assessor	Oceniający	Por. *Oceniający środki bezpieczeństwa*.
Assurance [NISTIR 7298]	Wiarygodność [NISTIR 7298]	Fundament zaufania, że zestaw zabezpieczeń zastosowanych w systemie informacyjnym jest skuteczny.
Assurance Case [NISTIR 7298]	Przypadek wiarygodności [NISTIR 7298]	Uporządkowany zestaw argumentów i dowodów wskazujących, że system informacyjny spełnia określone wymogi w zakresie danego wskaźnika jakościowego.
Authentication [FIPS 200]	Uwierzytelnienie [FIPS 200[54]]	Potwierdzenie tożsamości użytkownika, procesu lub urządzenia, często stanowi warunek wstępny zezwolenia na dostęp do zasobów w systemie informacyjnym.
Authenticity [CNSSI 4009]	Autentyczność [CNSSI 4009]	Prawdziwość oraz możliwość weryfikacji i zaufania, zaufanie wobec prawidłowości transmisji, wiadomości lub nadawcy wiadomości. Por. *Uwierzytelnienie*.

[54] Patrz: polskojęzyczna publikacja NSC 200. Przypis odnosi się do całego dokumentu.

Terminologia angielska	Terminologia polska	Definicja
Authorization (to operate) **[CNSSI 4009]**	Upoważnienie do działania [CNSSI 4009]	Oficjalna decyzja wydana przez przedstawicieli organizacji wyższego szczebla, zezwalająca na działanie systemu informacyjnego i jednoznacznie akceptująca ryzyko dla działalności jednostki organizacyjnej (w tym misji, funkcji, wizerunku lub reputacji), zasobów jednostki organizacyjnej, osób, innych organizacji i państwa na podstawie wdrożenia uzgodnionego zestawu środków bezpieczeństwa i prywatności.
Authorization Boundary **[NIST SP 800-37]**	Granica autoryzacji [NIST SP 800-37]	Wszystkie komponenty systemu informacyjnego dopuszczone do eksploatacji przez osobę autoryzującą, nieobejmujące innych autoryzowanych systemów, z którymi połączony jest system informacyjny.
Authorizing Official (AO) **[CNSSI 4009]**	Osoba autoryzująca [CNSSI 4009]	Pracownik wyższego szczebla lub członek kadry kierowniczej, który jest upoważniony do przyjmowania odpowiedzialności za działanie systemu informacyjnego na akceptowalnym poziomie ryzyka dla działalności jednostki organizacyjnej (w tym misji, funkcji, wizerunku lub reputacji), zasobów jednostki organizacyjnej, osób, innych organizacji i państwa.
Availability **[44 U.S.C., Sec. 3542]**	Dostępność [44 U.S.C., Sec. 3542]	Zapewnienie terminowego i niezawodnego dostępu do informacji i wykorzystania tej informacji.
Categorization	Kategoryzacja	Por. *Kategoryzacja zabezpieczeń*.

Terminologia angielska	Terminologia polska	Definicja
Chief Information Officer (CIO) **[PL 104-106, Sec. 5125(b)]**	Chief Information Officer (CIO) [PL 104-106, Sec. 5125(b)]	Przedstawiciel jednostki organizacyjnej odpowiedzialny za: 1. Udzielanie porad i wsparcia kierownikowi jednostki wykonawczej i innemu personelowi kierowniczemu wyższego szczebla jednostki organizacyjnej w celu zapewnienia, że technologia informacyjna jest pozyskiwana, a zasoby informacyjne są zarządzane w sposób zgodny z przepisami prawa, zarządzeniami wykonawczymi, dyrektywami, zasadami, przepisami i priorytetami ustanowionymi przez kierownika jednostki organizacyjnej. 2. Opracowywanie, utrzymywanie i wspieranie wdrażania niezawodnej i zintegrowanej architektury technologii informacyjnej dla jednostki organizacyjnej. 3. Wspieranie skutecznego i sprawnego projektowania oraz obsługi wszystkich głównych procesów zarządzania zasobami informacyjnymi dla jednostki organizacyjnej, w tym usprawnień procesów pracy jednostki organizacyjnej.
Chief Information Security Officer	CISO	Por. *SAISO*.
Common Control **[CNSSI 4009]**	Zabezpieczenie wspólne [CNSSI 4009]	Zabezpieczenie wykorzystywane przez jeden lub więcej systemów informacyjnych organizacji. Por. *Dziedziczenie środków bezpieczeństwa*.

Terminologia angielska	Terminologia polska	Definicja
Common Control Provider [NISTIR 7298]	Dostawca zabezpieczeń wspólnych [NISTIR 7298]	Przedstawiciel organizacji odpowiedzialny za opracowywanie, wdrażanie, ocenę i monitorowanie zabezpieczeń wspólnych (tj. zabezpieczeń obejmujących wiele systemów informacyjnych).
Compensating Security Controls [NISTIR 7298]	Zabezpieczenia kompensacyjne [NISTIR 7298]	Zabezpieczenia techniczne, operacyjne oraz dotyczące zarządzania (środki przeciwdziałania i bezpieczeństwa) stosowane przez organizację zamiast zabezpieczeń zalecanych dla niskich, umiarkowanych lub wysokich poziomów bazowych opisanych w publikacji specjalnej NIST 800-53, które zapewniają równoważną lub porównywalną ochronę systemu informacyjnego.
Comprehensive Testing [NISTIR 7298]	Testy kompleksowe [NISTIR 7298]	Metodologia testowania, która zakłada pełną i istotną wiedzę na temat wewnętrznej struktury i szczegółów wdrożenia obiektu oceny. Określane także mianem testowania białej skrzynki.

Terminologia angielska	Terminologia polska	Definicja
Computer Incident Response Team (CIRT) **[CNSSI 4009]**	Zespół reagowania na incydenty komputerowe (CIRT) [CNSSI 4009]	Grupa pracowników składająca się zwykle z analityków bezpieczeństwa, zorganizowana w celu opracowywania, zalecania i koordynowania natychmiastowych działań łagodzących w celu zatrzymywania incydentów bezpieczeństwa informacyjnego, zwalczania ich oraz przywracania działania systemów. Nazywany również zespołem reagowania na incydenty bezpieczeństwa komputerowego (*ang. Computer Security Incident Response Center - CSIRT*) lub centrum reagowania na incydenty komputerowe (*ang. Computer Security Incident Response Team* - CIRC) lub mianem zdolności do reagowania na incydenty komputerowe.
Confidentiality **[44 U.S.C., Sec. 3542]**	Poufność [44 U.S.C., Sec. 3542]	Zapewnienie stosowania zatwierdzonych ograniczeń w zakresie ujawniania i dostępu do informacji, w tym środków ochrony prywatności i informacji osobistych.
Configuration Control (or Configuration Management) **[CNSSI 4009]**	Zabezpieczenia konfiguracyjne (lub zarządzanie konfiguracją) [CNSSI 4009]	Proces kontrolowania zmian w sprzęcie, oprogramowaniu układowym, oprogramowaniu uruchamianym w środowiskach oraz dokumentacji w celu ochrony systemu informacyjnego przed niewłaściwymi modyfikacjami przed wdrożeniem, a także w trakcie wdrożenia oraz po jego zakończeniu.

Terminologia angielska	Terminologia polska	Definicja
Continuous Monitoring	Ciągłe monitorowanie	Utrzymywanie ciągłej świadomości w celu wspierania decyzji organizacji dotyczących ryzyka. Por. *Ciągłe monitorowanie bezpieczeństwa informacji*, *Monitorowanie ryzyka* oraz *Monitorowanie stanu*.
Controlled Interface [CNSSI 4009]	Interfejs nadzorowany [CNSSI 4009]	Granica z zestawem mechanizmów, które egzekwują zasady bezpieczeństwa i kontrolują przepływ informacji między połączonymi systemami informacyjnymi.
Countermeasures [CNSSI 4009]	Środki przeciwdziałania [CNSSI 4009]	Działania, urządzenia, procedury, techniki lub inne środki, które zmniejszają podatność systemu informacyjnego na zagrożenia. Pojęcie jest synonimem środków bezpieczeństwa oraz zabezpieczeń.
Coverage [NISTIR 7298]	Zasięg [NISTIR 7298]	Atrybut powiązany z metodą oceny, który odnosi się do zakresu obiektów oceny uwzględnionych w ocenie (np. rodzajów obiektów podlegających ocenie i liczby obiektów danego rodzaju podlegających ocenie). Wartości atrybutu zasięgu, uszeregowane hierarchicznie od najmniejszego do największego, obejmują: podstawowy, ukierunkowany i kompleksowy.
Data Loss	Utrata danych	Ujawnienie własnościowych, wrażliwych lub niejawnych informacji poprzez kradzież lub wyciek danych.

Terminologia angielska	Terminologia polska	Definicja
Depth **[NISTIR 7298]**	Głębokość [NISTIR 7298]	Atrybut związany z metodą oceny, który odnosi się do rygoru i poziomu szczegółowości związanego z zastosowaniem metody. Wartości atrybutu głębokości, uszeregowane hierarchicznie od najmniejszego do największego, obejmują: podstawowy, ukierunkowany i kompleksowy.
Domain **[CNSSI 4009]**	Domena [CNSSI 4009]	Środowisko lub kontekst, który obejmuje zestaw zasobów systemowych i zestaw encji systemowych, które mają prawo dostępu do zasobów określonych przez wspólne zasady bezpieczeństwa, model bezpieczeństwa lub architekturę bezpieczeństwa. Por. *Domena zabezpieczeń*.
Environment of Operation **[NISTIR 7298]**	Środowisko eksploatacji [NISTIR 7298]	Fizyczne otoczenie, w którym system informacyjny przetwarza, przechowuje i przesyła informacje.
Examine **[NISTIR 7298]**	Badanie [NISTIR 7298]	Rodzaj metody oceny, która charakteryzuje się procesem sprawdzania, kontroli, przeglądu, obserwacji, testów lub analizy pojedynczego obiektu oceny lub większej liczby obiektów oceny w celu zrozumienia, uzyskania wiedzy lub dowodów wykorzystywanych w celu określania skuteczności zabezpieczeń w czasie.

Terminologia angielska	Terminologia polska	Definicja
Executive Agency [41 U.S.C., Sec. 403]	Jednostka wykonawcza	Jednostki wchodzące w skład władzy wykonawczej, odpowiedzialne za bezpośrednie zarządzanie sprawami państwa lub samorządu, w tym Kancelaria Prezydenta RP oraz Rada Ministrów i podległe jej organy administracji rządowej - centralne i terenowe, władze wykonawcze jednostek samorządu terytorialnego na szczeblach województwa oraz powiatu, jednostki wchodzące w skład Sił Zbrojnych RP, a także spółki państwowe oraz spółki z udziałem Skarbu Państwa.
Expected Output	Oczekiwane wyniki	Wszelkie dane zebrane w wyniku monitorowania i oceny w ramach strategii ciągłego monitorowania bezpieczeństwa informacji.
High-Impact System [FIPS 200]	System o wysokim poziomie wpływu [FIPS 200]	System informacyjny, w którym co najmniej jednemu celowi bezpieczeństwa (poufność, integralność lub dostępność) przypisano wysoką wartość potencjalnego wpływu zgodnie z definicją zawartą w dokumencie FIPS 199[55].
Hybrid Security Control [CNSSI 4009]	Zabezpieczenie hybrydowe [CNSSI 4009]	Zabezpieczenie wdrożone w systemie informacyjnym częściowo jako zabezpieczenie wspólne, a częściowo jako zabezpieczenie specyficzne dla systemu Por. *Zabezpieczenie wspólne oraz Zabezpieczenie specyficzne systemu*.

[55] Patrz: polskojęzyczna publikacja NSC 199. Przypis odnosi się do całego dokumentu.

Terminologia angielska	Terminologia polska	Definicja
Incident **[FIPS 200]**	Incydent [FIPS 200]	Zdarzenie, które stanowi rzeczywiste lub potencjalne zagrożenie poufności, integralności lub dostępności systemu informacyjnego lub informacji przetwarzanych, przechowywanych lub przesyłanych przez system, a także zdarzenie, które stanowi naruszenie lub bezpośrednie zagrożenie naruszenia zasad bezpieczeństwa, procedur bezpieczeństwa lub zasad dopuszczalnego użytkowania.
Individuals **[NISTIR 7298]**	Osoba fizyczna [NISTIR 7298]	Obiekt oceny obejmujący osoby wdrażające specyfikacje, mechanizmy lub działania.
Information Owner **[CNSSI 4009]**	Właściciel informacji [CNSSI 4009]	Przedstawiciel posiadający ustawowe lub operacyjne uprawnienia do określonych informacji i odpowiedzialny za ustanowienie zabezpieczeń dotyczących generowania, gromadzenia, przetwarzania, rozpowszechniania i usuwania informacji.
Information Resources **[44 U.S.C., Sec. 3502]**	Zasoby informacyjne [44 U.S.C., Sec. 3502]	Informacje i powiązane zasoby, takie jak pracownicy, sprzęt, fundusze i technologie informacyjne.
Information Security **[44 U.S.C., Sec. 3542]**	Bezpieczeństwo informacji [44 U.S.C., Sec. 3542]	Ochrona informacji i systemów informacyjnych przed nieuprawnionym dostępem, wykorzystaniem, ujawnieniem, uszkodzeniem, modyfikacją i zniszczeniem, w celu zapewnienia poufności, integralności i dostępności.

Terminologia angielska	Terminologia polska	Definicja
Information Security Architect [NISTIR 7298]	Architekt bezpieczeństwa informacji [NISTIR 7298]	Osoba, grupa lub organizacja odpowiedzialna za zapewnienie, że wymagania dotyczące bezpieczeństwa informacji niezbędne do ochrony podstawowych misji i procesów biznesowych organizacji są odpowiednio uwzględnione we wszystkich aspektach architektury korporacyjnej, w tym w modelach referencyjnych, architekturach segmentów i rozwiązań oraz wynikających z nich systemach informacyjnych wspierających określone misje i procesy biznesowe.
Information Security Continuous Monitoring (ISCM)	Ciągłe monitorowanie bezpieczeństwa informacji (ISCM)	Utrzymywanie ciągłej świadomości bezpieczeństwa informacji, podatności w zabezpieczeniach i zagrożeń w celu podejmowania decyzji dotyczących zarządzania ryzykiem w organizacji. [Uwaga: Terminy „ciągły" oraz „trwający" użyte w tym kontekście oznaczają, że zabezpieczenia i ryzyka organizacyjne są oceniane i analizowane z częstotliwością pozwalającą na wspieranie decyzji dotyczących bezpieczeństwa opartych na ryzyku w celu odpowiedniej ochrony informacji organizacji.]
Information Security Continuous Monitoring (ISCM) Program	Program ciągłego monitorowania bezpieczeństwa informacji (ISCM)	Program ustanowiony w celu gromadzenia informacji zgodnie z wcześniej ustalonymi wskaźnikami, w oparciu o informacje łatwo dostępne w części dzięki wdrożonym środkom bezpieczeństwa.

Terminologia angielska	Terminologia polska	Definicja
Information Security Continuous Monitoring (ISCM) Process	Proces ciągłego monitorowania bezpieczeństwa informacji (ISCM)	Proces obejmujący: • Określenie strategii ciągłego monitorowania bezpieczeństwa informacji. • Ustanowienie programu ciągłego monitorowania bezpieczeństwa informacji. • Wdrożenie programu ciągłego monitorowania bezpieczeństwa informacji. • Analizę danych i opracowywanie sprawozdań z wynikami. • Reagowanie na ustalenia. • Przegląd i aktualizacja strategii i programu ciągłego monitorowania bezpieczeństwa informacji.
Information Security Program Plan [NISTIR 7298]	Plan programu bezpieczeństwa informacji [NISTIR 7298]	Formalny dokument, który zawiera przegląd wymogów w zakresie bezpieczeństwa dla programu bezpieczeństwa informacji obejmującego całą organizację oraz opisuje środki zarządzania programem i zabezpieczenia wspólne stosowane lub planowane w celu spełnienia tych wymagań.
Information Security Risk [NIST SP 800-39]	Ryzyko bezpieczeństwa informacji [NIST SP 800-39]	Ryzyko dla operacji organizacyjnych (w tym misji, funkcji, wizerunku, reputacji), aktywów organizacyjnych, osób, innych organizacji i państwa ze względu na możliwość nieuprawnionego dostępu, wykorzystania, ujawnienia, zakłócenia, modyfikacji lub zniszczenia informacji i/lub systemów. Por. *Ryzyko*.

Terminologia angielska	Terminologia polska	Definicja
Information System **[44 U.S.C., Sec. 3502]**	System informacyjny [44 U.S.C., Sec. 3502]	Zestaw zasobów informacyjnych zorganizowanych w celu gromadzenia, przetwarzania, utrzymywania, wykorzystywania, udostępniania, rozpowszechniania oraz dysponowania informacjami.
Information System Boundary	Granica systemu informatycznego	Por. *Granica autoryzacji*.
Information System Owner (or Program Manager) **[NISTIR 7298]**	Właściciel systemu informacyjnego (lub menedżer programu) [NISTIR 7298]	Osoba odpowiedzialna za zaopatrzenie, rozwój, integrację, modyfikację lub eksploatację i utrzymanie systemu informacyjnego.
Information System Security Engineer **[CNSSI 4009]**	Inżynier bezpieczeństwa systemów informacyjnych [CNSSI 4009]	Osoba odpowiedzialna za prowadzenie działań związanych z inżynierią bezpieczeństwa systemów informacyjnych.
Information System Security Engineering **[CNSSI 4009]**	Inżynieria bezpieczeństwa systemów informacyjnych [CNSSI 4009]	Proces, który umożliwia gromadzenie i doskonalenie wymogów dotyczących bezpieczeństwa informacji oraz zapewnia ich integrację z komponentami technologii informacyjnej i systemami informacyjnymi dzięki projektowaniu lub konfiguracji zabezpieczeń w celu uzyskania określonych rezultatów.

Terminologia angielska	Terminologia polska	Definicja
Information System- related Security Risks	Ryzyka bezpieczeństwa związane z systemem informacyjnym	Ryzyko wynikające z utraty poufności, integralności lub dostępności informacji lub systemów informacyjnych i uwzględniające wpływ na organizację (w tym zasoby, misję, funkcje, wizerunek lub reputację), osoby fizyczne, inne organizacje i naród. Por. *Ryzyko*.
Information System Security Officer (ISSO) [CNSSI 4009]	ISSO [CNSSI 4009]	Osoba odpowiedzialna za utrzymanie odpowiedniego poziomu bezpieczeństwa operacyjnego systemu lub programu informacyjnego.
Information Technology [40 U.S.C., Sec. 1401]	Technologia informacyjna [40 U.S.C., Sec. 1401]	Dowolne urządzenie lub wzajemnie połączone systemy lub podzespoły sprzętowe wykorzystywane do automatycznego pozyskiwania, przechowywania, przetwarzania, zarządzania, przemieszczania, kontrolowania, wyświetlania, przełączania, wymiany, przesyłania lub odbierania danych lub informacji przez jednostkę wykonawczą. W kontekście poprzedniego zdania, sprzęt jest używany przez jednostkę wykonawczą, jeśli jest wykorzystywany bezpośrednio przez jednostkę wykonawczą lub przez wykonawcę na podstawie umowy z jednostką wykonawczą, która: (I) wymaga użycia danego sprzętu; lub (II) wymaga użycia, w znacznym zakresie, takiego sprzętu do wykonania usługi lub dostarczenia produktu. Termin *technologia informacyjna* obejmuje komputery, urządzenia dodatkowe, oprogramowanie, oprogramowanie układowe, a także procedury, usługi (w tym usługi wsparcia) oraz powiązane zasoby.

Terminologia angielska	Terminologia polska	Definicja
Information Type [FIPS 199]	Typ informacji [FIPS 199]	Określona kategoria informacji (np. dane osobowe, medyczne, zastrzeżone, finansowe, dochodzeniowe, wrażliwe, dane dotyczące zarządzania bezpieczeństwem) określone przez organizację lub w niektórych przypadkach przez przepisy prawa, rozporządzenia wykonawcze, dyrektywę, zasady lub rozporządzenia.
Integrity [44 U.S.C., Sec. 3542]	Integralność [44 U.S.C., Sec. 3542]	Zabezpieczenie przed nieprawidłową modyfikacją lub zniszczeniem informacji oraz zapewnienie niezaprzeczalności i autentyczności informacji.
Interview [NISTIR 7298]	Wywiad [NISTIR 7298]	Rodzaj metody oceny, która charakteryzuje się procesem rozmów z osobami fizycznymi lub grupami w ramach organizacji w celu zrozumienia, uzyskania wiedzy lub dowodów, wyjaśnienia wątpliwości lub zgromadzenia informacji pozwalających na zebranie dowodów wykorzystywanych w celu określania skuteczności zabezpieczeń w czasie.
Intrusion Detection and Prevention System (IDPS) [NISTIR 7298]	System wykrywania i zapobiegania włamaniom (IDPS) [NISTIR 7298]	Oprogramowanie, które automatyzuje proces monitorowania zdarzeń zachodzących w systemie komputerowym lub sieci i analizowania ich pod kątem oznak możliwych incydentów oraz podejmowania prób powstrzymania wykrytych możliwych incydentów.
Malware [NISTIR 7298]	Oprogramowanie złośliwe [NISTIR 7298]	Program wprowadzony do systemu, zazwyczaj w sposób niejawny, z zamiarem naruszenia poufności, integralności lub dostępności danych, aplikacji lub systemu operacyjnego ofiary.

Terminologia angielska	Terminologia polska	Definicja
Management Controls **[FIPS 200]**	Zabezpieczenia zarządzania [FIPS 200]	Środki bezpieczeństwa (tj. zabezpieczenia lub środki zaradcze) dotyczące systemu informacyjnego, które koncentrują się na zarządzaniu ryzykiem i zarządzaniu bezpieczeństwem systemu informacyjnego.
Mechanisms **[NISTIR 7298]**	Mechanizm [NISTIR 7298]	Obiekt oceny, który obejmuje określone zagadnienia związane z ochroną (np. sprzęt, oprogramowanie lub oprogramowanie układowe) stosowane w systemie informacyjnym lub na jego granicy.
Metrics **[NISTIR 7298]**	Wskaźniki [NISTIR 7298]	Narzędzia zaprojektowane w celu ułatwienia podejmowania decyzji oraz usprawnienia procesów i rozliczalności dzięki gromadzeniu danych, analizom oraz opracowywaniu sprawozdań związanych z wydajnością.

Terminologia angielska	Terminologia polska	Definicja
National Security System **[44 U.S.C., Sec. 3542]**	Krajowy system bezpieczeństwa [44 U.S.C., Sec. 3542]	Każdy system informacyjny (w tym każdy system telekomunikacyjny) używany lub obsługiwany przez jednostkę organizacyjną lub wykonawcę jednostki organizacyjnej lub inną organizację w imieniu jednostki organizacyjnej:(I) którego funkcja, działanie lub użytkowanie obejmuje działania wywiadowcze; działania kryptologiczne związane z bezpieczeństwem narodowym; dowodzenie i sprawowanie kontroli nad siłami zbrojnymi; urządzenia będące integralną częścią broni lub systemu uzbrojenia; lub który ma krytyczne znaczenie dla realizacji misji wojskowych lub wywiadowczych (z wyłączeniem systemu, który ma być wykorzystywany do rutynowych zastosowań administracyjnych i biznesowych, na przykład kadrowych, finansowych bądź logistycznych; bądź (II) który podlega ciągłej ochronie na podstawie procedur dotyczących informacji, które zostały wskazane w ustawie lub rozporządzeniu wykonawczym jako wymagające zachowania klauzuli tajności w interesie obrony narodowej lub polityki zagranicznej.
Operational Controls **[FIPS 200]**	Zabezpieczenia operacyjne [FIPS 200]	Środki bezpieczeństwa (tj. zabezpieczenia lub środki przeciwdziałania) dotyczące systemu informacyjnego, które są wdrażane i wykonywane przede wszystkim przez osoby fizyczne (w przeciwieństwie do systemów).
Organization **[FIPS 200, Adapted]**	Organizacja [FIPS 200, termin dostosowany]	Podmiot o dowolnej wielkości, złożoności lub pozycji w strukturze organizacyjnej (np. przedsiębiorstwo bądź dowolny z jego wydziałów operacyjnych).

Terminologia angielska	Terminologia polska	Definicja
Organizational Information Security Continuous Monitoring	Ciągłe monitorowanie bezpieczeństwa informacji w organizacji	Bieżące monitorowanie pozwalające na zapewnienie i zagwarantowanie skuteczności zabezpieczeń związanych z systemami, sieciami i cyberprzestrzenią poprzez ocenę wdrożenia zabezpieczeń i stanu bezpieczeństwa w organizacji na podstawie ram tolerancji ryzyka organizacyjnego oraz w ramach struktury sprawozdawczości zaprojektowanej w celu podejmowania w czasie rzeczywistym decyzji dotyczących zarządzania ryzykiem opartych na danych.
Patch Management [CNSSI 4009]	Zarządzanie poprawkami [CNSSI 4009]	Systematyczne powiadamianie, określanie, wdrażanie, instalacja i weryfikacja poprawek kodu systemu operacyjnego i aplikacji. Poprawki te określane są także mianem łatek, dodatków serwisowych, a także patchy oraz hot fixów.
Penetration Testing [NISTIR 7298]	Testowanie penetracyjne [NISTIR 7298]	Metodologia testowania, w której oceniający, korzystając z całej dostępnej dokumentacji (np. projektu systemu, kodu źródłowego, instrukcji i dokumentacji) próbują obejść zabezpieczenia systemu informacyjnego, działając w określonych uprzednio ramach.
Plan of Action & Milestones (POA&M) [OMB Memorandum 02-01]	Plan i etapy działania/ Kamienie milowe [Memorandum OMB 02-01]	Dokument wskazujący zadania do wykonania. Wyszczególnia zasoby wymagane do realizacji elementów planu, kolejne kamienie milowe w realizacji zadań oraz zaplanowane daty realizacji.

Terminologia angielska	Terminologia polska	Definicja
Potential Impact [FIPS 199]	Potencjalny wpływ [FIPS 199]	Utrata poufności, integralności oraz dostępności danych może mieć: (I) *ograniczony* niekorzystny wpływ (niski według dokumentu FIPS 199); (II) *poważny* niekorzystny wpływ (umiarkowany według dokumentu FIPS 199); a także (III) poważny lub *katastrofalny* niekorzystny wpływ (wysoki według dokumentu FIPS 199) na działalność, zasoby lub pracowników organizacji.
Records [CNSSI 4009]	Dokumentacja [CNSSI 4009]	Dokumenty opracowane w sposób automatyczny lub ręczny, stanowiące dowody wykonanych działań lub osiągniętych wyników (np. formularze, sprawozdania, wyniki testów), służące jako podstawa do weryfikacji, czy organizacja i system informacyjny działają zgodnie z przeznaczeniem. Termin jest używany także w odniesieniu do powiązanych pól danych (tj. grup pól danych, do których program może uzyskać dostęp i które zawierają kompletny zestaw informacji o poszczególnych elementach).
Resilience [NIST SP 800-39, Adapted]	Odporność [NIST SP 800-39, termin dostosowany]	Zdolność do: (I) dalszego działania w niekorzystnych warunkach lub stresie, nawet w stanie zdegradowanym lub osłabionym, przy jednoczesnym zachowaniu podstawowych zdolności operacyjnych; oraz (II) odzyskania możliwości działania w czasie zgodnym z potrzebami misji.

Terminologia angielska	Terminologia polska	Definicja
Risk **[FIPS 200, Adapted]**	Ryzyko [FIPS 200, termin dostosowany]	Stopień, w jakim dany podmiot jest zagrożony przez potencjalne wystąpienie danej okoliczności lub danego zdarzenia, zwykle stanowiący wypadkową: (I) niekorzystnych skutków, które zaistniałyby w przypadku wystąpienia danej okoliczności lub danego zdarzenia; oraz (II) prawdopodobieństwa jego wystąpienia. [Uwaga: Ryzyka bezpieczeństwa związane z systemem informacyjnym to ryzyka, które wynikają z utraty poufności, integralności lub dostępności informacji lub systemów informacyjnych i uwzględniające potencjalny niekorzystny wpływ na działalność organizacji (w tym misję, funkcje, wizerunek lub reputację), zasoby organizacji, osoby fizyczne, inne organizacje i państwo. Niekorzystne skutki dla państwa mogą obejmować między innymi naruszenie systemów informacyjnych, które obsługują aplikacje infrastruktury krytycznej lub systemów krytycznych dla ciągłości działania państwa]
Risk Assessment **[CNSSI 4009]**	Szacowanie ryzyka [CNSSI 4009]	Proces identyfikacji, szacowania i ustalania priorytetów ryzyka dla działalności organizacji (w tym misji, funkcji, wizerunku, reputacji), aktywów organizacji, osób fizycznych, innych organizacji i państwa, wynikających z działania systemu informacyjnego. Część zarządzania ryzykiem obejmuje analizy zagrożeń i podatności oraz bierze pod uwagę środki ograniczania ryzyka wynikające z planowanych lub wprowadzonych środków bezpieczeństwa. Termin jest synonimem analizy ryzyka.

Terminologia angielska	Terminologia polska	Definicja
Risk Executive (Function) [CNSSI 4009]	Osoba odpowiedzialna za zarządzanie ryzykiem. [CNSSI 4009]	Osoba lub grupa w organizacji, która zapewnia, że: (I) kwestie związane z ryzykiem bezpieczeństwa dla poszczególnych systemów informacyjnych, w tym decyzje dotyczące autoryzacji, są analizowane z perspektywy całej organizacji w odniesieniu do ogólnych celów strategicznych i celów organizacji w zakresie realizacji jej misji i funkcji biznesowych; oraz (II) zarządzanie ryzykiem bezpieczeństwa związanym z systemami informacyjnymi jest spójne w całej organizacji, jest zgodne z poziomem ryzyka tolerowanego przez organizację i rozważane w połączeniu z ryzykiem organizacyjnym wpływającym na sukces misji lub procesów biznesowych.
Risk Management [FIPS 200, Adapted]	Zarządzanie ryzykiem [FIPS 200, termin dostosowany]	Program i procesy wspierające zarządzanie ryzykiem związanym z bezpieczeństwem informacji dla działalności organizacyjnych (w tym misji, funkcji, wizerunku, reputacji), zasobów organizacji, osób fizycznych, innych organizacji i państwa: (I) ustanowienie kontekstu dla działań związanych z ryzykiem; (II) ocena ryzyka; (III) reagowanie na ryzyko po jego ustaleniu; oraz (IV) monitorowanie ryzyka w czasie.
Risk Monitoring	Monitorowanie ryzyka	Utrzymywanie ciągłej świadomości środowiska ryzyka organizacji, programu zarządzania ryzykiem i powiązanych działań w celu wspierania decyzji dotyczących ryzyka.

Terminologia angielska	Terminologia polska	Definicja
Risk Response [NIST SP 800-39]	Reakcja na ryzyko [NIST SP 800-39]	Akceptacja, uniknięcie, ograniczenie, podział lub przeniesienie ryzyka na działania danej organizacji, w tym misję, wizerunek lub reputację, jej majątek, a także jednostki, organizacje oraz naród.
Risk Tolerance [NISTIR 7298]	Tolerowanie ryzyka [NISTIR 7298]	Poziom ryzyka, jaki jednostka jest skłonna podjąć w celu osiągnięcia pożądanego rezultatu.
Safeguards [CNSSI 4009]	Zabezpieczenia [CNSSI 4009]	Środki bezpieczeństwa, których stosowanie jest zalecane w celu spełnienia wymogów bezpieczeństwa (dotyczących poufności, integralności i dostępności) określonych dla systemu informacyjnego. Zabezpieczenia mogą obejmować funkcje bezpieczeństwa, ograniczenia dotyczące zarządzania, bezpieczeństwo personelu oraz bezpieczeństwo fizyczne, obszarów i urządzeń. Pojęcie jest synonimem zabezpieczeń i środków przeciwdziałania.
Security Authorization	Autoryzacja bezpieczeństwa	Por. *Autoryzacja*.
Security Automation Domain	Domena automatyzacji zabezpieczeń	Obszar bezpieczeństwa informacji obejmujący grupę narzędzi, technologii i danych.
Security Categorization [CNSSI 1253, FIPS 199]	Kategoryzacja bezpieczeństwa [CNSSI 1253, FIPS 199]	Proces określania kategorii bezpieczeństwa informacji lub systemu informacyjnego. Metodologie kategoryzacji bezpieczeństwa są opisane w instrukcji CNSS 1253 dla krajowych systemów bezpieczeństwa oraz w dokumencie FIPS 199 dla systemów innych niż krajowe.

Terminologia angielska	Terminologia polska	Definicja
Security Control Assessment **[CNSSI 4009, Adapted]**	Ocena środków bezpieczeństwa [CNSSI 4009, termin dostosowany]	Testowanie bądź ocena zabezpieczeń w zakresie zarządzania, zabezpieczeń operacyjnych oraz technicznych systemu informacyjnego w celu określenia zakresu, w jakim są one prawidłowo wdrożone, działają zgodnie z przeznaczeniem i przynoszą pożądane rezultaty w odniesieniu do spełnienia wymogów w zakresie bezpieczeństwa systemu.
Security Control Assessor **[NISTIR 7298]**	Oceniający środki bezpieczeństwa [NISTIR 7298]	Osoba, grupa lub organizacja odpowiedzialna za przeprowadzenie oceny zabezpieczeń.
Security Control Baseline **[FIPS 200, Adapted]**	Zestaw minimalnych zabezpieczeń [FIPS 200, termin dostosowany]	Jeden z zestawów minimalnych zabezpieczeń określonych dla systemów informacyjnych w publikacji specjalnej NIST 800-53 i FIPS 199.
Security Control Effectiveness	Skuteczność zabezpieczeń	Miara poprawności wdrożenia (zgodności wdrożenia zabezpieczenia z planem bezpieczeństwa) oraz spełniania przez plan bezpieczeństwa potrzeb organizacji na podstawie bieżącej tolerancji ryzyka.

Terminologia angielska	Terminologia polska	Definicja
Security Control Inheritance [CNSSI 4009]	Dziedziczenie zabezpieczenia [CNSSI 4009]	Sytuacja, w której system informacyjny lub aplikacja są chronione za pomocą zabezpieczeń (lub elementów zabezpieczeń), które są opracowywane, wdrażane, oceniane, autoryzowane i monitorowane przez podmioty inne niż podmioty odpowiedzialne za system lub aplikację, w tym podmioty wewnętrzne lub zewnętrzne w stosunku do organizacji, w której działa dany system lub dana aplikacja. Por. *Zabezpieczenie wspólne*.
Security Controls [FIPS 199]	Zabezpieczenia [FIPS 199]	Metody zarządzania, zabezpieczenia operacyjne i techniczne (zabezpieczenia lub środki przeciwdziałania) przewidziane dla systemu informacyjnego w celu ochrony poufności, integralności i dostępności systemu i przechowywanych danych.
Security Domain [CNSSI 4009]	Domena bezpieczeństwa [CNSSI 4009]	Domena, która wdraża zasady bezpieczeństwa i jest administrowana przez pojedynczą jednostkę.
Security Impact Analysis [NIST SP 800-53]	Analiza wpływu na bezpieczeństwo [NIST SP 800-53]	Analiza przeprowadzona przez przedstawiciela organizacji w celu określenia zakresu, w jakim zmiany w systemie informacyjnym wpłynęły na stan jego bezpieczeństwa.
Security Incident	Incydent bezpieczeństwa	Por. *Incydent*.

Terminologia angielska	Terminologia polska	Definicja
Security Management Dashboard [NIST SP 800-128]	Pulpit zarządzania bezpieczeństwem [NIST SP 800-128]	Narzędzie, które zestawia i przekazuje informacje istotne z punktu widzenia stanu bezpieczeństwa organizacji w czasie zbliżonym do rzeczywistego interesariuszom odpowiedzialnym za zarządzanie bezpieczeństwem.
Security Objective [FIPS 199]	Atrybut bezpieczeństwa [FIPS 199]	Poufność, integralność lub dostępność.
Security Plan [NISTIR 7298]	Plan bezpieczeństwa [NISTIR 7298]	Formalny dokument, który zawiera przegląd wymagań bezpieczeństwa dotyczących danego systemu informacyjnego lub programu bezpieczeństwa informacji oraz opisuje istniejące lub planowane zabezpieczenia pozwalające na spełnienie tych wymogów. Por. *Plan bezpieczeństwa systemu* lub *Plan programu bezpieczeństwa informacji*.
Security Policy [CNSSI 4009]	Polityka bezpieczeństwa [CNSSI 4009]	Zestaw kryteriów świadczenia usług w zakresie bezpieczeństwa.
Security Posture [CNSSI 4009]	Stan bezpieczeństwa [CNSSI 4009]	Stan bezpieczeństwa sieci, informacji i systemów organizacji oparty na zasobach IA (pracownikach, sprzęcie, oprogramowaniu, politykach) oraz możliwości zarządzania obroną organizacji oraz reagowania na zmiany sytuacji.

Terminologia angielska	Terminologia polska	Definicja
Security Requirements [FIPS 200]	Wymagania bezpieczeństwa [FIPS 200]	Wymagania nałożone na system informacyjny, które wynikają z obowiązujących przepisów prawa, rozporządzeń wykonawczych, dyrektyw, zasad, norm, instrukcji, przepisów, procedur lub misji organizacyjnej / potrzeb biznesowych w celu zapewnienia poufności, integralności i dostępności przetwarzanych, przechowywanych lub przesyłanych informacji.
Security Status	Status bezpieczeństwa	Por. *Stan bezpieczeństwa*.
Senior (Agency) Information Security Officer (SISO) [44 U.S.C., Sec. 3544]	S(A)ISO [44 U.S.C., Sec. 3544]	Osoba pełniąca obowiązki CIO zgodnie z przepisami o zarządzaniu bezpieczeństwem informacji, pełniąca rolę głównego łącznika pomiędzy CIO i osobami autoryzującymi jednostki organizacyjnej, właścicielami systemów informacyjnych i ISSO. [Uwaga: Organizacje mogą używać terminu *Senior Information Security Officer* lub *Chief Information Security Officer* na określenie osób zajmujących stanowiska o podobnym zakresie obowiązków do SAISO.
Senior Information Security Officer	SISO	Por. *S(A)ISO*.
Specification [NISTIR 7298]	Specyfikacja [NISTIR 7298]	Obiekt oceny, który obejmuje artefakty oparte na dokumentach (w tym polityki, procedury, plany, wymagania dotyczące bezpieczeństwa systemu, specyfikacje funkcjonalne i projekty architektury) związane z systemem informacyjnym.

Terminologia angielska	Terminologia polska	Definicja
Status Monitoring	Monitorowanie stanu	Monitorowanie wskaźników bezpieczeństwa informacji określonych przez organizację w strategii bezpieczeństwa informacji oraz ciągłego monitorowania bezpieczeństwa informacji.
Subsystem [NISTIR 7298]	Podsystem [NISTIR 7298]	Element systemu informacyjnego składający się z informacji, technologii informacyjnej i pracowników, wykonujący jedną lub więcej określonych funkcji.
System	System	Por. *System informacyjny*.
System Development Life Cycle (SDLC) [CNSSI 4009]	Cykl życia systemu [CNSSI 4009]	Zakres działań związanych z systemem, obejmujący jego projektowanie, opracowanie i pozyskanie, wdrożenie, eksploatację i utrzymanie, a także utylizację.
System Development Life Cycle (SDLC) [CNSSI 4009, Adapted]	Cykl życia systemu [CNSSI 4009, termin dostosowany]	Zakres działań związanych z systemem, obejmujący jego projektowanie, opracowanie i pozyskanie, wdrożenie, eksploatację i utrzymanie, a także utylizację, która powoduje wdrożenie kolejnego systemu.
System Security Plan [FIPS 200]	Plan bezpieczeństwa systemu [FIPS 200]	Formalny dokument, który zawiera przegląd wymogów w zakresie bezpieczeństwa systemu informacyjnego i opisuje istniejące lub planowane zabezpieczeń pozwalające na spełnienie tych wymogów.
System-Specific Security Control [CNSSI 4009]	Zabezpieczenie specyficzne systemu [CNSSI 4009]	Zabezpieczenie systemu informacyjnego, które nie stanowi zabezpieczenia wspólnego lub części zabezpieczenia hybrydowego, wdrożone w systemie informacyjnym.

Terminologia angielska	Terminologia polska	Definicja
Tailoring **[CNSSI 4009]**	Dostosowywanie [CNSSI 4009]	Proces, w którym zestaw minimalnych zabezpieczeń jest modyfikowany na podstawie: (I) zastosowania procedury ustalania zakresu działania systemu; (II) specyfikacji zabezpieczeń kompensacyjnych, jeśli są konieczne; oraz (III) specyfikacji parametrów określonych przez organizację dla zabezpieczeń na podstawie instrukcji przypisania i deklaracji wyboru.
Technical Controls **[FIPS 200]**	Zabezpieczenia techniczne [FIPS 200]	Środki bezpieczeństwa (tj. zabezpieczenia lub środki przeciwdziałania) dotyczące systemu informacyjnego, które są wdrażane i wykonywane przez system informacyjny za pomocą mechanizmów zawartych w sprzęcie, oprogramowaniu lub oprogramowaniu układowym systemu.
Test **[NISTIR 7298]**	Test [NISTIR 7298]	Rodzaj metody oceny, która charakteryzuje się procesem wykonywania jednego lub więcej obiektów oceny w określonych warunkach w celu porównania zachowania rzeczywistego z zachowaniem oczekiwanym; wyniki tego procesu są wykorzystywane do wspierania określania skuteczności zabezpieczeń w czasie.

Terminologia angielska	Terminologia polska	Definicja
Threat [CNSSI 4009, Adapted]	Zagrożenie [CNSSI 4009, termin dostosowany]	Wszelkie okoliczności lub zdarzenia mogące mieć negatywny wpływ na działalność organizacji (w tym misję, funkcję, wizerunek lub reputację), jej zasoby, pracowników, inne organizacje lub państwo w wyniku nieautoryzowanego dostępu do systemu informacyjnego, zniszczenia, ujawnienia, modyfikacji informacji lub odmowy świadczenia usługi.
Threat Information [CNSSI 4009, Adapted]	Informacje o zagrożeniach [CNSSI 4009, termin dostosowany]	Wnioski analityczne dotyczące trendów, technologii lub taktyk stosowanych przez adwersarzy, wpływające na bezpieczeństwo systemów informacyjnych.
Threat Source [FIPS 200]	Źródło zagrożenia [FIPS 200]	Zamiar i metoda ukierunkowane na celowe wykorzystanie podatności lub sytuacja i metoda prowadząca do jej przypadkowego użycia. Pojęcie jest synonimem czynnika zagrożenia.
Vulnerability [CNSSI 4009]	Podatność [CNSSI 4009]	Słabość systemu informacyjnego, procedur bezpieczeństwa systemu, zabezpieczeń wewnętrznych lub wdrożenia, która może zostać wykorzystana lub uruchomiona przez źródło zagrożenia.
Vulnerability Assessment [CNSSI 4009]	Ocena podatności [CNSSI 4009]	Formalny opis i ocena podatności systemu informacyjnego.
White Box Testing	Testowanie białej skrzynki	Por. *Testy kompleksowe*.

ZAŁĄCZNIK C – SKRÓTY I AKRONIMY

POWSZECHNE SKRÓTY I AKRONIMY

Akronim	Terminologia angielska	Terminologia polska
AO	Authorizing Official	Osoba autoryzująca
CAPEC	Common Attack Pattern Enumeration & Classification	Lista i klasyfikacja typowych wzorców ataków
CIO	Chief Information Officer	Kluczowa osoba w jednostce organizacyjnej odpowiedzialna za technologie informacyjne, zwykle członek kierownictwa jednostki organizacyjnej
CIRT	Computer Incident Response Team	Zespół reagowania na incydenty komputerowe
COTS	Commercial Off-The-Shelf	Rozwiązania komercyjne
CVSS	Common Vulnerability Scoring System	Nazwa platformy oceny podatności
CVE	Common Vulnerabilities and Exposures	Typowe podatności i zagrożenia
CWE	Common Weakness Enumeration	Lista typowych podatności
CWSS	Common Weakness Scoring System	Nazwa systemu oceny podatności
DLP	Data Loss Prevention	Zapobieganie utracie danych

Akronim	Terminologia angielska	Terminologia polska
FDCC	Federal Desktop Core Configuration	Konfiguracja podstawowa komputerów federalnych
FISMA	Federal Information Security Management Act of 2002	Ustawa federalna dotycząca zarządzania bezpieczeństwem informacji z 2002 roku
IDPS	Intrusion Detection and Prevention System	System wykrywania i zapobiegania włamaniom
ISCM	Information Security Continuous Monitoring	Ciągłe monitorowanie bezpieczeństwa informacji
ISO	Information System Owner	Właściciel systemu informacyjnego
ISSO	Information System Security Officer	Osoba odpowiedzialna za bezpieczeństwo systemów informacyjnych
IT	Information Technology	Technologia informacyjna
NCP	National Checklist Program	Krajowy program list kontrolnych
NVD	National Vulnerability Database	Krajowa baza danych dotyczących podatności na zagrożenia
OCIL	Open Checklist Interactive Language	Nazwa języka
OMB	Office of Management and Budget	Biuro ds. Zarządzania i Budżetu

Akronim	Terminologia angielska	Terminologia polska
OVAL	Open Vulnerability and Assessment Language	Nazwa języka
PII	Personally Identifiable Information	Dane osobowe
PM	Program Management	Zarządzanie programem
POA&M	Plan Of Action & Milestones	Plan i etapy działania/ Kamienie milowe
RMF	Risk Management Framework	Ramy zarządzania ryzykiem
SAR	Security Assessment Report	Sprawozdanie z oceny bezpieczeństwa
SCAP	Security Content Automation Protocol	Automatyczny protokół zabezpieczeń zawartości
SDLC	System Development Life Cycle	Cykl życia systemu
SIA	Security Impact Analysis	Analiza wpływu na bezpieczeństwo
SIEM	Security Information and Event Management	Bezpieczeństwo informacji i zarządzanie zdarzeniami
SISO	Senior Information Security Officer	Osoba odpowiedzialna za bezpieczeństwo informacji
SP	Special Publication	Publikacja specjalna
SwAAP	Software Assurance Automation Protocol	Nazwa protokołu zapewniania wiarygodności oprogramowania

Akronim	Terminologia angielska	Terminologia polska
USGCB	United States Government Configuration Baseline	------
XCCDF	eXtensible Configuration Checklist Description Format	Nazwa formatu opisu list kontrolnych konfiguracji
XML	Extensible Markup Language	Nazwa języka

ZAŁĄCZNIK D – TECHNOLOGIE WSPIERAJĄCE CIĄGŁE MONITOROWANIE BEZPIECZEŃSTWA INFORMACJI

Organizacje mogą bardziej efektywnie wykorzystywać swoje budżety przeznaczone na bezpieczeństwo poprzez wdrażanie technologii automatyzujących wiele działań związanych z ciągłym monitorowaniem bezpieczeństwa informacji, wspierających wdrażanie zasad i strategii zarządzania ryzykiem, bezpieczeństwo operacyjne, zapewnianie zgodności z przepisami i wewnętrznymi procedurami, a także sprawozdawczość i dokumentację. Organizacje mogą zdecydować się na zastosowanie architektury referencyjnej, takiej jak NIST CAESARS Framework Extension, w celu wdrożenia technologii związanych z ciągłym monitorowaniem bezpieczeństwa informacji[56]. Dostępnych jest wiele narzędzi i technologii, które organizacja może wykorzystać do sprawnego i skutecznego gromadzenia, agregowania, analizowania i raportowania danych, począwszy od ciągłego monitorowania stanu bezpieczeństwa architektury korporacyjnej i środowiska eksploatacji, a skończywszy na komponentach poszczególnych systemów informacyjnych. Te narzędzia i technologie mogą umożliwiać i wspomagać zautomatyzowane monitorowanie wspierające różne procesy organizacyjne, w tym między innymi:

- Bieżącą ocenę skuteczności zabezpieczeń.
- Opracowywanie sprawozdań ze stanu bezpieczeństwa na odpowiednim poziomie szczegółowości na potrzeby przedstawicieli organizacji odpowiedzialnych za bezpieczeństwo.
- Zarządzanie ryzykiem oraz weryfikację i ocenę działań ograniczających ryzyko.
- Zapewnianie zgodności z wymogami wewnętrznymi i zewnętrznymi.
- Analizy wpływu zmian w środowisku eksploatacji na bezpieczeństwo.

[56] Więcej informacji można znaleźć w wersji roboczej dokumentu NISTIR 7756 z późniejszymi zmianami, CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Architecture.

Narzędzia i technologie omówione w niniejszym załączniku opierają się na strategiach, zasadach oraz rolach i obowiązkach całego programu ciągłego monitorowania bezpieczeństwa informacji w organizacji i mogą pomóc organizacjom w ich wysiłkach na rzecz automatyzacji wdrażania, oceny i monitorowania wielu zabezpieczeń opisanych w dokumencie NIST SP 800-53. Choć opisane narzędzia i technologie są przeznaczone przede wszystkim do ciągłego monitorowania zabezpieczeń technicznych, które można zautomatyzować, mogą one dostarczać danych potwierdzających istnienie oraz skuteczność zabezpieczeń nietechnicznych oraz elementów zabezpieczeń technicznych, których nie można łatwo zautomatyzować. Automatyzację osiąga się dzięki różnorodnym komercyjnym i rządowym produktom, wbudowanym funkcjom systemów operacyjnych oraz niestandardowym narzędziom i skryptom, które wykorzystują znormalizowane specyfikacje automatyzacji.

Ważne jest, aby zrozumieć i docenić potrzebę okresowej oceny skuteczności wszystkich zabezpieczeń, w szczególności zabezpieczeń innych niż techniczne. Dane zebrane za pomocą zautomatyzowanych narzędzi mogą nie zawierać informacji na temat istnienia i skuteczności takich zabezpieczeń. W niektórych przypadkach możliwe jest wyciągnięcie pewnych wniosków na temat skuteczności takich zabezpieczeń na podstawie danych zebranych za pomocą zautomatyzowanych narzędzi. Choć użycie zautomatyzowanych narzędzi i technologii do monitorowania przestrzegania zasad i procedur może okazać się niemożliwe, może istnieć możliwość monitorowania powiązanych atrybutów bezpieczeństwa w sposób zautomatyzowany.

Język Open Checklist Interactive Language (OCIL) omówiony w rozdziale D.3.1, może być wykorzystywany do częściowej automatyzacji niektórych zabezpieczeń, które wymagają uwagi ze strony człowieka, a jednocześnie mogą być weryfikowane w formacie pytań i odpowiedzi. Przykładowo, może istnieć możliwość opracowania zautomatyzowanego kwestionariusza w celu zebrania informacji związanych z corocznym szkoleniem w zakresie bezpieczeństwa.

Ważność informacji związanych z bezpieczeństwem gromadzonych w sposób ciągły lub na żądanie za pomocą zautomatyzowanych narzędzi zakłada ciągłą skuteczność podstawowych zabezpieczeń związanych z zarządzaniem oraz zabezpieczeń

operacyjnych. W związku z tym przydatność i użyteczność zautomatyzowanych narzędzi i technologii, w tym rozwiązań, które bezpośrednio gromadzą, agregują i analizują dane, zależy od procesów operacyjnych wspierających ich wykorzystanie. Aby organizacje mogły osiągnąć korzyści w zakresie bezpieczeństwa operacyjnego oraz aby narzędzia i technologie odzwierciedlały dokładny stan bezpieczeństwa organizacji, ich wdrożeniem, utrzymaniem oraz bieżącą obsługą muszą zajmować się odpowiednio przeszkoleni pracownicy. To samo dotyczy także wdrażania podstawowych zabezpieczeń, interpretacji danych uzyskanych w procesie monitorowania oraz doboru i wdrażania stosownych środków zaradczych.

Niniejszy załącznik omawia rolę narzędzi i technologii w automatyzacji wielu działań dotyczących ciągłego monitorowania bezpieczeństwa informacji. Omówiono w nim popularne narzędzia, technologie i otwarte specyfikacje wykorzystywane do gromadzenia, analizowania i przedstawiania danych w celu wspierania ciągłego monitorowania stanu bezpieczeństwa organizacji, w tym zapewniania wglądu w zasoby informacyjne, świadomości zagrożeń i podatności w zakresie bezpieczeństwa oraz stanu skuteczności zabezpieczeń. Uwzględniono przykłady zabezpieczeń, które można zautomatyzować przy użyciu różnych technologii. Podane w treści przykłady nie stanowią wyczerpującej listy. Na rynek nieustannie trafiają nowe produkty i technologie. Zabezpieczenia, które ą powszechnie automatyzowane, a które nie są wymienione jako przykłady związane z technologiami wymienionymi poniżej, obejmują między innymi zabezpieczenia, w których automatyzacja jest osiągana dzięki funkcjom wbudowanym w systemy operacyjne, niestandardowym narzędziom i skryptom lub połączeniom kilku narzędzi i możliwości[57].

[57] Przykłady zabezpieczeń, które można zautomatyzować w pełni bądź częściowo w ramach inżynierii bezpieczeństwa lub wykorzystania oprogramowania dostawców zewnętrznych i narzędzi do zarządzania dziennikami obejmują zarządzanie kontami, dokumentację szkoleń w zakresie bezpieczeństwa, zgłaszanie incydentów i kontrolę dostępu.

D.1 TECHNOLOGIE GROMADZENIA DANYCH

Technologie gromadzenia danych to te, które zapewniają możliwość obserwowania, wykrywania i rejestrowania znanych zagrożeń bezpieczeństwa i podatności dotyczących bezpieczeństwa, a także zapobiegają zagrożeniom oraz umożliwiają podjęcie działań naprawczych lub zarządzanie różnymi aspektami zabezpieczeń wdrożonych w celu przeciwdziałania tym zagrożeniom i podatnościom. Technologie te są wdrażane głównie na poziomie systemów informacyjnych (poziom 3). Można je jednak skonfigurować w taki sposób, aby wspierały bieżące potrzeby organizacji w zakresie monitorowania bezpieczeństwa na poziomie misji i procesów biznesowych dzięki wskaźnikom dotyczącym zarządzania bezpieczeństwem informacji. Wdrożenie tych narzędzi w całej organizacji pozwala na wykorzystywanie tych możliwości przez wszystkie systemy.

Domena automatyzacji zabezpieczeń to obszar bezpieczeństwa informacji, który obejmuje grupowanie narzędzi, technologii i danych. Dane w domenach są gromadzone, zestawiane, analizowane i raportowane w celu przedstawienia stanu bezpieczeństwa organizacji reprezentowanej przez monitorowane domeny. Automatyzacja zagadnień związanych z bezpieczeństwem zapewnia znormalizowane specyfikacje, które umożliwiają interoperacyjność i przepływ danych między tymi domenami. Możliwości monitorowania są osiągane poprzez wykorzystanie różnych narzędzi i technik. Szczegółowość gromadzonych danych jest określana przez organizację, w oparciu o wyznaczone cele monitorowania i możliwości architektury korporacyjnej w zakresie wspierania takich działań.

W tym rozdziale opisano narzędzia i technologie dotyczące jedenastu domen automatyzacji zabezpieczeń, które wspierają ciągłe monitorowanie:

- Zarządzanie podatnościami;
- Zarządzanie poprawkami;
- Zarządzanie zdarzeniami;
- Zarządzanie incydentami;

- Wykrywanie złośliwego oprogramowania;
- Zarządzanie zasobami;
- Zarządzanie konfiguracją;
- Zarządzanie siecią;
- Zarządzanie licencjami;
- Zarządzanie informacjami;
- Wiarygodność oprogramowania.

Domeny zostały przedstawione na rysunku D-1.

Rysunek D-1. Domeny automatyzacji zabezpieczeń

D.1.1. ZARZĄDZANIE PODATNOŚCIAMI I POPRAWKAMI

Podatność to usterka oprogramowania, która powoduje potencjalne zagrożenie bezpieczeństwa. Liczba wykrytych podatności oraz poprawek opracowanych w celu ich wyeliminowania stale rośnie, co sprawia, że ręczne instalowanie poprawek do systemów oraz ich komponentów staje się coraz trudniejszym zadaniem. W miarę możliwości organizacje powinny wykrywać, zgłaszać i usuwać luki w zabezpieczeniach w skoordynowany sposób obejmujący kompleksowo całą organizację przy użyciu zautomatyzowanych narzędzi i technologii zarządzania podatnościami i poprawkami.

Organizacje powszechnie wykorzystują skanery podatności w celu wykrywania znanych podatności hostów oraz sieci, a także powszechnie używanych systemów operacyjnych i aplikacji. Narzędzia te pozwalają na proaktywne wykrywanie podatności i zapewniają szybki i łatwy sposób pomiaru zagrożenia, wykrywają nieaktualne wersje oprogramowania, weryfikują zgodność z politykami bezpieczeństwa obowiązującymi w organizacji oraz generują alarmy i sprawozdania dotyczące wykrytych podatności.

Narzędzia do zarządzania poprawkami skanują systemy i komponenty systemów w poszukiwaniu podatności obsługiwanych przez dane rozwiązanie, dostarczają informacji o potrzebnych poprawkach i innych aktualizacjach oprogramowania oraz umożliwiają administratorowi podjęcie decyzji o instalacji poprawek. Narzędzia i programy do zarządzania poprawkami są oferowane przez wielu dostawców. Każde takie narzędzie wspomaga proces automatycznej identyfikacji, dystrybucji i dokumentacji poprawek oprogramowania. Kluczowe znaczenie ma zrozumienie wpływu poprawek przed ich zastosowaniem i wdrożenie ich w kontekście zasad zarządzania poprawkami, a także zapewnienie, że instalacja poprawek nie spowoduje utraty krytycznej funkcjonalności systemów. W niektórych przypadkach, gdy instalacja poprawki nie jest możliwa, konieczne może być zastosowanie innych zabezpieczeń.

Wdrożenie i efektywne wykorzystanie technologii oceny podatności i zarządzania poprawkami[58] może pomóc organizacjom w automatyzacji wdrażania, oceny i ciągłego monitorowania szeregu zabezpieczeń opisanych w dokumencie NIST SP 800-53,

[58] Więcej informacji można znaleźć w dokumencie NIST SP 800-40 *Creating a Patch and Vulnerability Management Program* z późniejszymi zmianami.

w tym SI-2 – Usuwanie usterek, CA-2 – Ocena zabezpieczeń; CA-7 – Ciągłe monitorowanie, CM-3 – Zabezpieczanie zmian konfiguracji, IR-4 – Obsługa incydentów, IR-5 – Monitorowanie incydentów; MA-2 – Nadzór nad utrzymaniem, RA-5 – Monitorowanie i skanowanie podatności, SA-11– Testowanie i ocena przez dewelopera oraz SI-11 – Obsługa błędów. Technologie oceny podatności i zarządzania poprawkami mogą również dostarczać danych pomocniczych, aby pomóc organizacjom w zaspokajaniu wymogów dotyczących sprawozdawczości w obszarach zarządzania konfiguracją oraz podatnościami.

D.1.2. ZARZĄDZANIE ZDARZENIAMI I INCYDENTAMI

Zarządzanie zdarzeniami obejmuje monitorowanie i reagowanie w razie potrzeby na obserwowalne zdarzenia w sieci lub systemie. Istnieje wiele narzędzi i technologii umożliwiających monitorowanie zdarzeń, takich jak systemy wykrywania włamań i mechanizmy dzienników. Niektóre narzędzia mogą wykrywać zdarzenia w oparciu o znane sygnatury ataków, podczas gdy inne wykrywają anomalie dotyczące zachowania lub wydajności, które mogą wskazywać na atak. Pewne zdarzenia mogą sygnalizować, że doszło do incydentu, który jest naruszeniem lub bezpośrednim zagrożeniem naruszenia zasad bezpieczeństwa komputerowego, zasad dopuszczalnego użytkowania lub standardowych praktyk bezpieczeństwa komputerowego. Narzędzia do zarządzania incydentami mogą pomóc w wykrywaniu takich zdarzeń, a także w ograniczaniu wpływu złośliwego cyberataku na organizację oraz odpowiedniej odpowiedzi.

Dziennik to zapis zdarzeń zachodzących w systemach i sieciach organizacji. Dzienniki składają się z wpisów; każdy wpis zawiera informacje związane z konkretnym zdarzeniem, które wystąpiło w systemie lub jego komponencie. Wiele dzienników w organizacji zawiera zapisy związane z bezpieczeństwem komputerowym. Te dzienniki bezpieczeństwa mogą być generowane przez wiele źródeł, w tym oprogramowanie zabezpieczające, takie jak rozwiązania chroniące przed złośliwym oprogramowaniem, zapory ogniowe oraz systemy wykrywania i zapobiegania włamaniom, systemy operacyjne na serwerach, stacjach roboczych, urządzenia sieciowe i aplikacje[59].

[59] Więcej informacji można znaleźć w dokumencie NIST SP 800-92, *Guide to Computer Security Log Management*.

Liczba, objętość i różnorodność dzienników bezpieczeństwa stale wzrasta, co powoduje naturalną potrzebę opracowania rozwiązań do zarządzania dziennikami bezpieczeństwa systemów informacyjnych – procesem generowania, przesyłania, przechowywania, analizowania i usuwania danych dzienników bezpieczeństwa. Zarządzanie dziennikami ma zasadnicze znaczenie dla zapewnienia, że dokumentacja związana z bezpieczeństwem jest przechowywana przez odpowiedni okres. Dzienniki są niezwykle cenne podczas przeprowadzania kontroli i analiz kryminalistycznych, wspierania wewnętrznych dochodzeń, ustalania poziomów bazowych oraz określania trendów operacyjnych i długoterminowych problemów. Rutynowa analiza dzienników jest ważna z punktu widzenia identyfikacji incydentów bezpieczeństwa, naruszeń zasad, nieuczciwych działań oraz problemów operacyjnych i jako taka wspiera działania w zakresie ciągłego monitorowania bezpieczeństwa informacji.

Wdrożenie i efektywne wykorzystanie narzędzi i technologii związanych z dziennikami oraz zarządzaniem dziennikami może pomóc organizacjom w automatyzacji wdrażania, oceny i ciągłego monitorowania szeregu zabezpieczeń opisanych w dokumencie NIST SP 800-53, w tym AU-2 – Audyt zdarzeń, AU-3 – Zawartość rejestrów audytu; AU-4 – Pojemność pamięci zapisów audytu; AU-5 – Reakcja na błędy procesów audytu; AU-6 – Przegląd audytu, analiza i raportowanie, AU-7 – Redukcja treści zapisów z audytu i generowanie raportów, AU-8 – Znaczniki czasu, AU-12 – Tworzenie zapisów audytu; CA-2 – Oceny zabezpieczeń, CA-7 – Ciągłe monitorowanie, IR-5 – Monitorowanie incydentów, RA-3 – Ocena ryzyka oraz SI-4 – Monitorowanie systemu informacyjnego.

Wykrywanie włamań to proces monitorowania zdarzeń występujących w systemie komputerowym lub sieci i analizowania ich pod kątem oznak możliwych incydentów, które są naruszeniami lub które stanowią bezpośrednie zagrożenie naruszenia zasad bezpieczeństwa komputerowego, zasad dopuszczalnego użytkowania lub standardowych praktyk bezpieczeństwa. *Zapobieganie włamaniom* to proces polegający na wykrywaniu włamań i próbie powstrzymania ewentualnych incydentów

w momencie ich wykrycia. Systemy wykrywania i zapobiegania włamaniom (IDPS)[60] koncentrują się przede wszystkim na wykrywaniu możliwych incydentów, rejestrowaniu informacji o ich wystąpieniu, próbach zapobiegania włamaniom oraz zgłaszaniu ich administratorom bezpieczeństwa w celu dalszej analizy i podjęcia działań.

Systemy wykrywania i zapobiegania włamaniom są zwykle używane do rejestrowania informacji związanych z zaobserwowanymi zdarzeniami, powiadamiania administratorów odpowiedzialnych za bezpieczeństwo o ważnych zaobserwowanych zdarzeniach i automatycznego generowania sprawozdań. Działania naprawcze są wykonywane ręcznie po przejrzeniu sprawozdania przez człowieka. Wiele takich systemów można również skonfigurować tak, aby reagowały na wykryte zagrożenie przy użyciu różnych technik, w tym zmiany konfiguracji zabezpieczeń lub blokowania ataku.

W kontekście programu ciągłego monitorowania bezpieczeństwa informacji, systemy wykrywania i zapobiegania włamaniom mogą być wykorzystywane do gromadzenia dowodów skuteczności zabezpieczeń (np. zasad, procedur i innych wdrożonych zabezpieczeń technicznych), dokumentowania istniejących zagrożeń i powstrzymywania nieautoryzowanego korzystania z systemów informacyjnych. Wdrożenie i efektywne wykorzystanie takich rozwiązań może również pomóc organizacjom w automatyzacji wdrażania, oceny i ciągłego monitorowania szeregu zabezpieczeń opisanych w dokumencie NIST SP 800-53, w tym AC-4 – Egzekwowanie zasad przepływu informacji; AC-17 – Dostęp zdalny; AC-18 – Dostęp bezprzewodowy; AU-2 – Audyt zdarzeń; AU-6 – Przegląd audytu, analiza i raportowanie; AU-12 – Tworzenie zapisów audytu; AU-13 – Monitorowanie ujawniania informacji; CA-2 – Oceny zabezpieczeń; CA-7 – Ciągłe monitorowanie; IR-5 – Monitorowanie incydentów; RA-3 – Ocena ryzyka; SC-7 – Ochrona połączeń brzegowych; SI-3 – Zabezpieczenie przed złośliwym kodem; SI-4 – Monitorowanie systemu oraz SI-7 – Aplikacje, oprogramowanie układowe oraz integralność

[60] Więcej informacji na ten temat znajduje się w dokumencie NIST SP 800-94 *Guide to Intrusion Detection and Prevention Systems (IDPS)* z późniejszymi zmianami.

informacji. Tego rodzaju rozwiązania mogą również dostarczać dane pomocnicze, aby pomóc organizacjom w spełnieniu wymagań CERT/CSIRT w zakresie zgłaszania incydentów oraz wymogów w zakresie raportowania w obszarach inwentaryzacji systemów i połączeń, zarządzania incydentami bezpieczeństwa, ochrony granic i zarządzania konfiguracją.

D.1.3. WYKRYWANIE ZŁOŚLIWEGO OPROGRAMOWANIA

Wykrywanie złośliwego oprogramowania[61] zapewnia możliwość wykrywania i zgłaszania obecności wirusów, koni trojańskich, oprogramowania szpiegującego lub innego złośliwego kodu w systemie docelowym lub w danych przeznaczonych dla danego systemu. Organizacje zwykle stosują mechanizmy wykrywania złośliwego oprogramowania w punktach wejścia i wyjścia systemu informacyjnego, na przykład na zaporach sieciowych, serwerach poczty elektronicznej, serwerach WWW, serwerach proxy, serwerach zdalnego dostępu oraz na urządzeniach końcowych (takich jak stacje robocze, serwery, urządzenia mobilne) w sieci w celu wykrywania i usuwania złośliwego kodu przenoszonego za pośrednictwem poczty elektronicznej, załączników poczty elektronicznej, sieci WWW, nośników wymiennych lub w inny sposób, a także wprowadzanego poprzez wykorzystanie podatności w systemie informacyjnym.

Mechanizmy wykrywania złośliwego oprogramowania można skonfigurować w taki sposób, aby wykonywały okresowe skanowanie systemów informacyjnych, a także skanowanie w czasie rzeczywistym plików ze źródeł zewnętrznych, gdy pliki są pobierane, otwierane lub wykonywane zgodnie z zasadami bezpieczeństwa organizacji. Mechanizmy wykrywania złośliwego oprogramowania mogą często podejmować z góry określone działania w odpowiedzi na wykrycie złośliwego kodu.

Oprócz wykrywania złośliwego oprogramowania istnieje wiele technologii i metod ograniczania lub eliminowania skutków ataków przy pomocy złośliwego kodu. W połączeniu z procedurami zarządzania konfiguracjami oraz zabezpieczeniami,

[61] Więcej informacji można znaleźć w dokumencie NIST SP 800-83, *Guide to Malware Incident Prevention and Handling* z późniejszymi zmianami.

a także mechanizmami zabezpieczającymi integralność oprogramowania, mechanizmy wykrywania złośliwego oprogramowania mogą być jeszcze bardziej skuteczne w przeciwdziałaniu uruchamiania nieautoryzowanego kodu. Dodatkowe środki ograniczające ryzyko, takie jak praktyki bezpiecznego programowania, zaufane procesy zamówień i regularne monitorowanie bezpieczeństwa konfiguracji, mogą pomóc w zapewnieniu, że nieautoryzowane funkcje nie będą wykonywane.

Wdrożenie i skuteczne wykorzystanie technologii wykrywania złośliwego oprogramowania może pomóc organizacjom w automatyzacji wdrażania, oceny i ciągłego monitorowania szeregu zabezpieczeń opisanych w dokumencie NIST SP 800-53, w tym CA-2 – Oceny zabezpieczeń; CA-7 – Ciągłe monitorowanie; IR-5 – Monitorowanie incydentów; RA-3 – Ocena ryzyka; SA-12 – Bezpieczeństwo łańcucha dostaw; SA-13 – Wiarygodność; SI-3 – Zabezpieczenie przed złośliwym kodem; SI-4 – Monitorowanie systemu; SI-7 – Aplikacje, oprogramowanie układowe i integralność informacji oraz SI-8 – Ochrona przed spamem. Technologie wykrywania złośliwego oprogramowania mogą również dostarczać danych pomocniczych, aby pomóc organizacjom w spełnieniu wymagań CERT/CSIRT w zakresie zgłaszania incydentów oraz wymagań jednostki organizacyjnej w zakresie zgłaszania i zarządzania incydentami, zdalnego dostępu oraz ochrony granic sieci.

D.1.4. ZARZĄDZANIE ZASOBAMI

Narzędzia do zarządzania zasobami pomagają w inwentaryzacji oprogramowania i sprzętu w organizacji. Można to osiągnąć za pomocą połączenia narzędzi do zarządzania konfiguracją systemów, sieci i zarządzania licencjami, a także za pomocą specjalnych narzędzi. Oprogramowanie do zarządzania zasobami monitoruje cykl życia zasobów organizacji i zapewnia narzędzia, takie jak zdalne zarządzanie zasobami i różne zautomatyzowane funkcje zarządzania.

Wdrożenie i skuteczne wykorzystanie technologii zarządzania zasobami może pomóc organizacjom w automatyzacji wdrażania, oceny i ciągłego monitorowania szeregu zabezpieczeń opisanych w dokumencie NIST SP 800-53, w tym CA-7 – Ciągłe monitorowanie; CM-2 – Konfiguracja bazowa; CM-3 – Zabezpieczanie zmian konfiguracji; CM-4 – Analizy wpływu; CM-8 – Inwentaryzacja komponentów systemu oraz SA-10 – Zarządzanie konfiguracją dewelopera.

D.1.5. ZARZĄDZANIE KONFIGURACJĄ

Narzędzia do zarządzania konfiguracją umożliwiają administratorom konfigurowanie ustawień, monitorowanie zmian w ustawieniach, gromadzenie informacji na temat stanu ustawień i przywracanie ustawień w razie potrzeby. Zarządzanie licznymi konfiguracjami występującymi w systemach informacyjnych i komponentach sieciowych stało się prawie niemożliwe przy użyciu metod ręcznych. Zautomatyzowane rozwiązania mogą obniżyć koszty zarządzania konfiguracją, jednocześnie zwiększając wydajność i niezawodność.

Narzędzia do skanowania konfiguracji systemu zapewniają możliwość przeprowadzania zautomatyzowanych audytów i ocen systemów w celu określenia zgodności z określoną bezpieczną konfiguracją bazową. Użytkownik może potwierdzić zgodność z listami kontrolnymi odpowiednimi dla odpowiednich systemów operacyjnych bądź aplikacji oraz zidentyfikować odstępstwa od nich.

Jeśli system informacyjny lub komponent systemu nie jest zsynchronizowany z zatwierdzonymi bezpiecznymi konfiguracjami bazowymi organizacji i określonymi w planie bezpieczeństwa systemu, przedstawiciele organizacji i właściciele systemów mogą mieć fałszywe poczucie bezpieczeństwa. Brak świadomości może spowodować utratę możliwości podjęcia działań, które pozwolą na usunięcie podatności i ochronę organizacji przed atakami. Działania monitorujące zapewniają organizacji lepszy wgląd w stan bezpieczeństwa jej systemów informacyjnych, zgodnie z określonymi wskaźnikami bezpieczeństwa.

Narzędzia do zarządzania tożsamością i konfiguracją kont umożliwiają organizacji zarządzanie poświadczeniami identyfikacyjnymi, kontrolą dostępu, autoryzacją

i uprawnieniami. Systemy zarządzania tożsamością mogą również umożliwiać i monitorować kontrolę dostępu fizycznego w oparciu o dane uwierzytelniające. Narzędzia do zarządzania tożsamością i konfiguracją kont często pozwalają na automatyzację zadań takich jak resetowanie hasła do konta i innych czynności związanych z utrzymaniem kont. Systemy te monitorują również i zgłaszają działania takie jak nieudane próby logowania, blokady kont i uzyskiwanie dostępu do zasobów.

Dostępnych jest wiele różnych narzędzi do zarządzania konfiguracją, które wspierają potrzeby organizacji. Wybierając narzędzie do zarządzania konfiguracją, organizacje powinny wziąć pod uwagę narzędzia, które mogą pobierać informacje z różnych źródeł i komponentów. Organizacje powinny wybierać narzędzia, które są oparte na otwartych specyfikacjach, takich jak SCAP; które zapewniają interoperacyjność, ocenę i raportowanie w całej organizacji; możliwość dostosowania i personalizacji danych wyjściowych oraz konsolidację danych w narzędziach SIEM i pulpitach zarządzania.

Wdrożenie i skuteczne wykorzystanie technologii zarządzania konfiguracją może pomóc organizacjom w automatyzacji wdrażania, oceny i ciągłego monitorowania szeregu zabezpieczeń opisanych w dokumencie NIST SP 800-53, w tym AC-2 – Zarządzanie kontami; AC-3 – Egzekwowanie uprawnień dostępu; AC-5 – Rozdział obowiązków; AC-7 – Nieudane próby logowania; AC-9 – Powiadomienie o poprzednim zalogowaniu; AC-10 – Kontrola liczby jednoczesnych sesji; AC-11 – Blokada urządzenia; AC-19 – Kontrola dostępu do urządzeń przenośnych; AC-20 – Wykorzystanie systemów zewnętrznych; AC-22 – Treści publicznie dostępne; CA-2 – Oceny zabezpieczeń; CA-7 – Ciągłe monitorowanie; CM-2 – Konfiguracja bazowa; CM-3 – Zabezpieczenie zmian konfiguracji; CM-5 – Ograniczenia możliwości dokonywania zmian; CM-6 – Ustawienia konfiguracji; CM-7 – Zasada minimalnej funkcjonalności; IA-2 – Identyfikacja i uwierzytelnianie (użytkownicy organizacyjni); IA-3 – Identyfikacja i uwierzytelnianie urządzeń; IA-4 – Zarządzanie identyfikatorem; IA-5 – Zarządzanie metodami uwierzytelniania; IA-8, Identyfikacja i uwierzytelnianie (użytkownicy spoza organizacji); IR-5 – Monitorowanie

incydentów; MA-5 – Personel utrzymaniowy; PE-3 – Kontrola dostępu fizycznego; RA-3 – Ocena ryzyka; SA-7 – Oprogramowanie instalowane przez użytkownika; SA-10 – Zarządzanie konfiguracją dewelopera oraz SI-2 – Usuwanie usterek. Technologie zarządzania konfiguracją bezpieczeństwa oraz inżynierii bezpieczeństwa mogą również dostarczać danych pomocniczych, aby pomóc organizacjom w zaspokajaniu wymogów dotyczących sprawozdawczości w obszarach zarządzania konfiguracją oraz zasobami.

D.1.6. ZARZĄDZANIE SIECIĄ

Narzędzia do zarządzania konfiguracją sieci umożliwiają wykrywanie hostów, inwentaryzację, weryfikację zmian, monitorowanie wydajności i inne funkcje zarządzania urządzeniami sieciowymi. Niektóre narzędzia do zarządzania konfiguracją sieci automatyzują konfigurację urządzeń i sprawdzają ich zgodność ze wstępnie skonfigurowanymi regułami. Narzędzia do zarządzania siecią mogą być w stanie wykryć nieautoryzowany sprzęt i oprogramowanie w sieci, takie jak nieznany bezprzewodowy punkt dostępowy.

Wdrożenie i skuteczne wykorzystanie technologii zarządzania siecią może pomóc organizacjom w automatyzacji wdrażania, oceny i ciągłego monitorowania szeregu zabezpieczeń opisanych w dokumencie NIST SP 800-53, w tym AC-4 – Egzekwowanie zasad przepływu informacji; AC-17 – Dostęp zdalny; AC-18 – Dostęp bezprzewodowy; CA-7 – Ciągłe monitorowanie; CM-2 – Konfiguracja bazowa; CM-3 – Zabezpieczenie zmian konfiguracji; CM-4 – Analizy wpływu; CM-6 – Ustawienia konfiguracji; CM-8 – Inwentaryzacja komponentów systemu; SC-2 – Rozdzielenie funkcjonalności systemu i użytkownika; SC-5 – Ochrona przed blokadą usług; SC-7 – Ochrona połączeń brzegowych; SC-10 – Zakończenie połączenia sieciowego; SC-32 – Dzielenie systemu na partycje oraz SI-4 – Monitorowanie systemu.

D.1.7. ZARZĄDZANIE LICENCJAMI

Podobnie jak systemy i urządzenia sieciowe, oprogramowanie i aplikacje są również istotnym źródłem danych na potrzeby ciągłego monitorowania bezpieczeństwa informacji. Informacje o zasobach oprogramowania i licencjach mogą być centralnie

zarządzane przez narzędzie do zarządzania zasobami oprogramowania w celu śledzenia zgodności licencji, monitorowania statusu użytkowania i zarządzania cyklem życia zasobów oprogramowania. Narzędzia do zarządzania licencjami oferują szereg funkcji automatyzujących inwentaryzację, monitorowanie wykorzystania i ograniczenia, wdrażanie, a także instalację poprawek.

Wdrożenie i skuteczne wykorzystanie technologii zarządzania licencjami może pomóc organizacjom w automatyzacji wdrażania, oceny i ciągłego monitorowania szeregu zabezpieczeń opisanych w dokumencie NIST SP 800-53, w tym CA-7 – Ciągłe monitorowanie; CM-8 – Inwentaryzacja komponentów systemu oraz SA-6 – Ograniczenia w użyciu oprogramowania.

D.1.8. ZARZĄDZANIE INFORMACJAMI

W niezliczonych systemach, urządzeniach sieciowych, bazach danych i innych zasobach w organizacji są przechowywane olbrzymie ilości danych cyfrowych. Zarządzanie lokalizacją i transferem danych ma zasadnicze znaczenie dla ochrony ich poufności, integralności i dostępności.

Utrata danych oznacza zwykle ujawnienie prawnie zastrzeżonych, wrażliwych lub niejawnych informacji w wyniku kradzieży lub wycieku. Kradzież danych ma miejsce, gdy dane są celowo wykradane lub ujawniane, na przykład w przypadkach szpiegostwa przemysłowego lub przez niezadowolonych pracowników. Wyciek danych to niezamierzone ujawnienie danych, takie zdarzenie ma miejsce w przypadku zgubionego lub skradzionego laptopa, przechowywania plików w serwisie chmurowym lub zapisania plików na dysku USB w celu wyniesienia ich z terenu organizacji.

Skuteczna strategia zapobiegania utracie danych (*ang. data loss prevention - DLP*) obejmuje inwentaryzację i klasyfikację danych; gromadzenie wskaźników, opracowywanie zasad tworzenia, wykorzystywania, przechowywania, przesyłania i usuwania danych, a także narzędzia do monitorowania danych w spoczynku, w użyciu i w czasie przesyłania. Dostępnych jest wiele narzędzi tego rodzaju. Typowe narzędzia sieciowe i bezpieczeństwa, takie jak oprogramowanie analizujące sieci, programowe zapory sieciowe oraz systemy wykrywania i zapobiegania włamaniom, mogą być używane do monitorowania danych i ich

zawartości podczas przesyłania. Istnieje również specjalne oprogramowanie do zapobiegania utracie danych wyposażone w funkcje takie jak zabezpieczenia portów i urządzeń końcowych, szyfrowanie dysków i plików oraz monitorowanie transakcji w bazach danych. Narzędzia te mogą być wyspecjalizowanymi monitorami ruchu sieciowego lub agentami oprogramowania zainstalowanymi na komputerach stacjonarnych, laptopach i serwerach. Narzędzia tego rodzaju są wyposażone w mechanizmy wykrywania i łagodzenia skutków naruszeń, takie jak alarmy wysyłane za pośrednictwem poczty elektronicznej, dzienniki działań i blokowanie transmisji.

Wdrożenie i efektywne wykorzystanie technologii DLP może pomóc organizacjom w automatyzacji wdrażania, oceny i ciągłego monitorowania szeregu zabezpieczeń opisanych w dokumencie NIST SP 800-53, w tym AC-4 – Egzekwowanie zasad przepływu informacji; AC-17 – Dostęp zdalny; CA-3 – Wymiana informacji; CA-7 – Ciągłe monitorowanie; CM-7 – Zasada minimalnej funkcjonalności, SC-9 – Poufność transmisji oraz SI-12 – Zarządzanie i retencja danych.

D.1.9. WIARYGODNOŚĆ OPROGRAMOWANIA

Projekt NIST Software Assurance Metrics and Tool Evaluation (SAMATE) definiuje wiarygodność oprogramowania jako „zaplanowany i systematyczny zestaw działań, które pozwalają na zapewnienie, że procesy i produkty oprogramowania są zgodne z wymaganiami, standardami i procedurami zawartymi w przewodniku i standardzie NASA Software Assurance Guidebook and Standard w celu zagwarantowania:

- Wiarygodności – braku podatności na ataki, zarówno złośliwe, jak i niezamierzone.
- Przewidywalności wykonania – uzasadnionej pewności, że oprogramowanie po uruchomieniu działa zgodnie z przeznaczeniem”.

Istnieje kilka specyfikacji automatyzacji, które mogą pomóc w ciągłym monitorowaniu zapewniania jakości oprogramowania, w tym nowy protokół automatyzacji zapewniania wiarygodności oprogramowania – Software Assurance Automation Protocol (SwAAP), który jest opracowywany w celu mierzenia i identyfikacji podatności oprogramowania i przypadków wiarygodności. SwAAP wykorzystuje różne

specyfikacje automatyzacji, takie jak Common Weakness Enumeration (CWE), czyli listę słabych punktów, które mogą prowadzić do powstania podatności (np. CVE[62]) oraz Common Weakness Scoring System (CWSS) do oceny ryzyka związanego ze słabymi punktami. SwAAP opera się również na Common Attack Pattern Enumeration & Classification (CAPEC) – publicznie dostępnym katalogu wzorców ataków z kompleksowym schematem i taksonomią klasyfikacji, zapewniającym opisy typowych metod wykorzystywania podatności oprogramowania, a także Malware Attribute Enumeration & Characterization (MAEC) – znormalizowany język kodowania i przekazywania informacji o złośliwym oprogramowaniu w oparciu o atrybuty takie jak zachowania, artefakty i wzorce ataków.

Istnieje wiele narzędzi i technologii zapewniania wiarygodności oprogramowania, które wykorzystują wymienione specyfikacje automatyzacji w celu zapewnienia bezpieczeństwa oprogramowania w całym cyklu życia. Wdrożenie i skuteczne wykorzystanie technologii zapewniania oprogramowania może pomóc organizacjom w automatyzacji wdrażania, oceny i ciągłego monitorowania szeregu zabezpieczeń opisanych w dokumencie NIST SP 800-53, w tym CA-7 – Ciągłe monitorowanie; SA-4 – Proces nabycia; SA-8 – Zasady inżynierii bezpieczeństwa i ochrony prywatności; SA-11 – Testowanie i ocena przez dewelopera; SA-12 – Bezpieczeństwo łańcucha dostaw; SA-13 – Wiarygodność; SA-14 – Analiza krytyczności oraz SI-13 – Przewidywanie awarii.

[62] Common Vulnerabilities and Exposures – słownik identyfikatorów odpowiadających powszechnie znanym podatnościom oraz zagrożeniom, a także standard ich nazewnictwa.

D.2 TECHNOLOGIE AGREGACJI I ANALIZY DANYCH

Technologie agregacji i analizy pozwalają na gromadzenie surowych danych z jednego lub większej liczby zabezpieczeń bądź innych technologii bezpośredniego gromadzenia danych oraz ich zestawiania, analizowania i przedstawiania w sposób, który zapewnia lepszy wgląd w skuteczność wdrażania zabezpieczeń w części lub całej organizacji niż dane z dowolnej pojedynczej technologii.

W tym rozdziale zostały omówione popularne rodzaje technologii agregacji i analizy danych oraz ich role we wspieraniu zdolności w zakresie ciągłego monitorowania bezpieczeństwa informacji. Obejmują one zarówno narzędzia bezpieczeństwa informacji i zarządzania zdarzeniami (SIEM), jak i pulpity zarządzania.

D.2.1. BEZPIECZEŃSTWO INFORMACJI I ZARZĄDZANIE ZDARZENIAMI (SIEM)

Aby zwiększyć możliwości w zakresie wykrywania niewłaściwych lub nietypowych działań, organizacje mogą połączyć analizę informacji ze skanowania podatności, danych dotyczących wydajności, monitorowania sieci i informacji z dzienników audytu za pomocą narzędzi SIEM. Narzędzia SIEM to rodzaj scentralizowanego oprogramowania rejestrującego, które może ułatwić agregację i konsolidację dzienników z wielu komponentów systemu informacyjnego. Narzędzia SIEM mogą również ułatwiać korelację i analizę dzienników audytu. Korelacja informacji z dzienników audytu z informacjami ze skanowania podatności jest ważna dla stwierdzenia poprawności skanowania podatności i korelacji wykrytych ataków z wynikami skanowania.

Produkty SIEM zazwyczaj oferują obsługę wielu źródeł dzienników audytu, takich jak systemy operacyjne, serwery aplikacji (np. serwery WWW, serwery poczty elektronicznej) i oprogramowanie zabezpieczające, a nawet mogą obejmować obsługę fizycznych urządzeń zabezpieczających, takich jak czytniki identyfikatorów. Serwer SIEM analizuje dane ze wszystkich różnych źródeł dzienników audytu, koreluje zdarzenia, wskazuje i nadaje priorytet istotnym zdarzeniom oraz może być skonfigurowany do inicjowania reakcji na zdarzenia.

W przypadku każdego obsługiwanego źródła dzienników produkty SIEM można zazwyczaj skonfigurować w taki sposób, by zapewniały funkcjonalność kategoryzacji najważniejszych pól dziennika (np. wartość w polu 12 dzienników aplikacji XYZ oznacza źródłowy adres IP), co może znacznie usprawnić normalizację, analizę i korelację danych z dzienników audytu. Oprogramowanie SIEM może również ograniczać liczbę zdarzeń poprzez pomijanie pól danych, które nie są istotne z punktu widzenia bezpieczeństwa systemu informacyjnego, potencjalnie zmniejszając wykorzystanie przepustowości sieci i pamięci masowej.

Wdrożenie i efektywne wykorzystanie technologii SIEM może pomóc organizacjom w automatyzacji wdrażania, oceny i ciągłego monitorowania szeregu zabezpieczeń opisanych w dokumencie NIST SP 800-53, w tym AC-5 – Rozdział obowiązków; AU-2 – Audyt zdarzeń; AU-6 – Przegląd audytu; AU-7 – Redukcja treści zapisów z audytu i generowanie raportów; CA-2 – Ocena zabezpieczeń; CA-7 – Ciągłe monitorowanie; IR-5 – Monitorowanie incydentów; PE-6 – Monitorowanie dostępu fizycznego; RA-3 – Ocena ryzyka; RA-5 – Monitorowanie i skanowanie podatności oraz SI-4 – Monitorowanie systemu.

D.2.2. PULPITY ZARZĄDZANIA

Pulpit zarządzania bezpieczeństwem (lub konsola zarządzania informacjami dotyczącymi bezpieczeństwa) zestawia i przekazuje informacje istotne z punktu widzenia stanu bezpieczeństwa organizacji w czasie zbliżonym do rzeczywistego interesariuszom odpowiedzialnym za zarządzanie bezpieczeństwem. Personel odpowiedzialny za bezpieczeństwo informacji obejmuje zarówno administratorów systemów, przez SISO, aż po osoby odpowiedzialne za zarządzanie ryzykiem. Pulpit zarządzania bezpieczeństwem prezentuje informacje w czytelnym i łatwo zrozumiałym formacie, który można dostosować w celu pozyskiwania informacji odpowiednich dla osób pełniących określone role i obowiązki w organizacji.

Aby zmaksymalizować korzyści płynące z pulpitów zarządzania, ważne jest uzyskanie akceptacji i wsparcia ze strony kierownictwa wyższego szczebla, określenie użytecznych i wymiernych wskaźników specyficznych dla organizacji, które są oparte

na zasadach i procedurach bezpieczeństwa informacji, a także zapewnienie dostępności istotnych danych.

Wdrożenie i skuteczne wykorzystanie pulpitów menedżerskich mogą pomóc organizacjom w automatyzacji wdrażania, oceny i ciągłego monitorowania szeregu zabezpieczeń opisanych w dokumencie NIST SP 800-53, w tym AC-5 – Rozdział obowiązków; CA-6 – Autoryzacja, CA-7 – Ciągłe monitorowanie; PM-6 – Miary skuteczności; PM-9 – Strategia zarządzania ryzykiem; RA-3 – Ocena ryzyka oraz SI-4 – Monitorowanie systemu.

D.3 AUTOMATYZACJA I REFERENCYJNE ŹRÓDŁA DANYCH

Zarządzanie bezpieczeństwem systemów w całej organizacji stanowi wyzwanie z kilku powodów. Większość organizacji wykorzystuje szereg systemów w celu bezpiecznej instalacji poprawek oraz zarządzania konfiguracjami, obejmującymi wiele składników oprogramowania (w tym systemy operacyjne i aplikacje), które wymagają zabezpieczenia w każdym systemie. Organizacje muszą prowadzić ciągłe monitorowanie konfiguracji bezpieczeństwa każdego systemu i być w stanie określić stan bezpieczeństwa systemów i całej organizacji w dowolnie wybranym momencie. Organizacje mogą również stanąć przed koniecznością wykazania zgodności z wymogami bezpieczeństwa uwzględnionymi w przepisach, regulacjach i zasadach. Wszystkie te zadania są niezwykle czasochłonne i podatne na błędy, ponieważ nie istnieje jeden znormalizowany i zautomatyzowany sposób ich wykonywania. Innym problemem dla organizacji jest brak interoperacyjności między narzędziami bezpieczeństwa; na przykład stosowanie niejednolitych nazw podatności lub platform powoduje niespójności w sprawozdaniach dostarczanych przez różne narzędzia, co może powodować opóźnienia w ocenie bezpieczeństwa, podejmowaniu decyzji i usuwaniu podatności. Organizacje potrzebują znormalizowanego, zautomatyzowanego podejścia, by skutecznie stawiać czoła tym wyzwaniom.

Automatyzacja to skuteczny sposób na realizację ciągłego monitorowania bezpieczeństwa informacji w obrębie domen i między nimi w celu gromadzenia, zestawiania, analizowania i raportowania ogólnego stanu bezpieczeństwa organizacji. Specyfikacje automatyzacji i znormalizowane formaty zapewniają interoperacyjność i umożliwiają sprawny przepływ danych między tymi domenami. Prawie każde narzędzie bezpieczeństwa zapewnia pewnego rodzaju możliwości automatyzacji w ramach swojej funkcjonalności, w tym importowanie i eksportowanie danych oraz wykonywanie innych wstępnie skonfigurowanych samodzielnych działań. Niektóre z tych zautomatyzowanych funkcji opierają się na zastrzeżonych metodach i protokołach, z kolei inne wykorzystują standardowe specyfikacje i metody. W przypadku korzystania z narzędzia, które automatycznie konfiguruje urządzenia lub zmienia ustawienia, nowe konfiguracje są najpierw

analizowane i weryfikowane w środowisku testowym. Niektóre przykłady działań związanych z automatyzacją zabezpieczeń obejmują:

- Skanowanie w poszukiwaniu luk w zabezpieczeniach i automatyczne instalowanie stosownych poprawek.
- Automatyczne konfigurowanie zabezpieczeń na podstawie listy kontrolnej ustawień zabezpieczeń.
- Skanowanie pod kątem zgodności z ustaloną listą kontrolną ustawień zabezpieczeń.
- Zbieranie wskaźników bezpieczeństwa z narzędzi i przekazywanie ich do konsoli zarządzania w standardowym formacie.

To tylko kilka z wielu działań związanych z bezpieczeństwem, które mogą zostać zautomatyzowane. Narzędzia i technologie omówione w niniejszej publikacji wykorzystują różnorodne protokoły pomocnicze, specyfikacje i zasoby w celu zapewnienia standaryzacji i interoperacyjności niezbędnej do realizacji ciągłego monitorowania bezpieczeństwa informacji.

Społeczność zapoczątkowała ruch na rzecz utworzenia specyfikacji automatyzacji w celu normalizacji formatu i nomenklatury informacji związanych z bezpieczeństwem i technologiami informacyjnymi. Te standardy wymiany danych tworzą podstawę do automatyzacji działań pomimo zastosowania narzędzi różnych dostawców, a także interoperacyjności między domenami. Najbardziej dojrzałym i szeroko stosowanym zestawem specyfikacji jest Security Content Automation Protocol (SCAP), czyli automatyczny protokół zabezpieczeń zawartości, który służy do normalizacji komunikacji błędów oprogramowania i konfiguracji zabezpieczeń. W tej sekcji omówiono, w jaki sposób SCAP, krajowa baza danych dotyczących podatności na zagrożenia (*ang. National Vulnerability Database - NVD*) i listy kontrolne konfiguracji zabezpieczeń są wykorzystywane do reprezentowania i przekazywania danych w znormalizowanym formacie w celu wykonywania funkcji automatyzacji zabezpieczeń i ich roli we wspieraniu programu ciągłego monitorowania bezpieczeństwa informacji.

D.3.1. AUTOMATYCZNY PROTOKÓŁ ZABEZPIECZEŃ ZAWARTOŚCI (SCAP)

SCAP to zestaw specyfikacji[63], które normalizują format i nomenklaturę wykorzystywaną przez oprogramowanie zabezpieczające w celu przekazywania informacji o błędach bezpieczeństwa i konfiguracji zabezpieczeń. SCAP to wielofunkcyjny protokół, który obsługuje zautomatyzowane skanowanie podatności oraz poprawek, działania związane ze zgodnością zabezpieczeń i pomiary bezpieczeństwa. Cele rozwoju SCAP obejmują normalizację zarządzania bezpieczeństwem systemu, zwiększanie interoperacyjności rozwiązań w zakresie bezpieczeństwa i wspieranie stosowania standardowych wyrażeń w materiałach dotyczących bezpieczeństwa. Protokół SCAP może być używany do utrzymywania bezpieczeństwa systemów organizacyjnych, w tym do automatycznej weryfikacji instalacji poprawek, weryfikacji ustawień konfiguracji bezpieczeństwa systemu i sprawdzania systemów pod kątem oznak naruszeń bezpieczeństwa.

Co można zautomatyzować przy pomocy SCAP?

Istnieje wiele łatwo dostępnych narzędzi, które można wykorzystać do automatyzacji działań ciągłego monitorowania bezpieczeństwa informacji dzięki SCAP. Program walidacji produktów SCAP (SCAP Product Validation Program)[64] ma na celu weryfikację możliwości produktów w zakresie korzystania z funkcji dostępnych za pośrednictwem SCAP i jego standardów składowych.

Program weryfikuje dwa rodzaje skanerów podatności oraz poprawek – uwierzytelnione i nieuwierzytelnione. Uwierzytelnione skanery podatności i poprawek zapewniają możliwość skanowania systemu docelowego przy użyciu danych logowania do systemu docelowego w celu zlokalizowania i zidentyfikowania obecności znanych podatności w zabezpieczeniach oraz oceny stanu poprawek oprogramowania w celu określenia bieżącego stanu bezpieczeństwa systemu

---

[63] Więcej informacji można znaleźć w dokumencie NIST SP 800-126, *The Technical Specification for the Security Content Automation Protocol* (SCAP): SCAP Rev. 3.

[64] Więcej informacji na temat programu SCAP Product Validation Program można znaleźć na stronie http://scap.nist.gov/validation/.

w oparciu o zasady organizacji dotyczące poprawek. Nieuwierzytelnione skanery podatności zapewniają możliwość stwierdzenia występowania znanych luk w zabezpieczeniach poprzez ocenę systemu docelowego przez sieć bez uwierzytelnionego dostępu. Skanery podatności obsługujące protokół SCAP można skonfigurować do skanowania połączonych systemów w regularnych odstępach czasu, zapewniając w ten sposób ilościowy i powtarzalny pomiar i ocenę usterek oprogramowania w różnych systemach. Korzystanie ze skanerów podatności opartych na SCAP umożliwia interoperacyjność między skanerami podatności i narzędziami raportującymi w celu zapewnienia spójnego wykrywania i raportowania błędów oraz wspiera kompleksowe możliwości naprawcze.

Choć łatanie i monitorowanie podatności w zabezpieczeniach oraz ich usuwanie może często wydawać się przytłaczającym zadaniem, konsekwentne ograniczanie luk w zabezpieczeniach oprogramowania systemowego można osiągnąć dzięki sprawdzonemu i zintegrowanemu procesowi instalacji poprawek. Dojrzały program zarządzania poprawkami i podatnościami obejmujący technologie automatyzacji zabezpieczeń pomoże organizacji zachować proaktywność względem utrzymania odpowiedniego poziomu bezpieczeństwa swoich systemów.

Technologie oceny podatności i zarządzania poprawkami koncentrują się przede wszystkim na wykrywaniu znanych podatności w popularnych systemach operacyjnych i aplikacjach. W przypadku niestandardowego oprogramowania oraz nietypowych aplikacji, a także wykrywania nieznanych, niezgłoszonych lub niezamierzonych luk w komercyjnych produktach, ocena i analiza podatności mogą wymagać zastosowania dodatkowych, bardziej wyspecjalizowanych technik i podejść, takich jak skanery aplikacji internetowych, przeglądy kodu źródłowego i analizatory kodu źródłowego. Narzędzia te, w połączeniu z metodologiami oceny zabezpieczeń, takimi jak testy penetracyjne i symulowane ataki, zapewniają dodatkowe możliwości identyfikacji podatności w zabezpieczeniach.

SCAP Validation Program ocenia możliwości skanerów konfiguracji, które mogą analizować i oceniać system docelowy w celu określenia jego zgodności ze zdefiniowaną bezpieczną konfiguracją podstawową. Przykłady bezpiecznych

konfiguracji bazowych obejmują Federal Desktop Core Configuration (FDCC)[65] i profile utworzone w ramach inicjatywy United States Government Configuration Baseline (USGCB)[66].

Jak wdrożyć SCAP?

Aby wdrożyć protokół SCAP na potrzeby ciągłego monitorowania bezpieczeństwa informacji, konieczne jest użycie zatwierdzonych narzędzi SCAP[67] oraz list kontrolnych wykorzystujących protokół SCAP w celu automatyzacji bezpiecznego zarządzania konfiguracją i tworzenia danych z oceny zabezpieczeń opisanych w dokumencie NIST SP 800-53. Listy kontrolne wykorzystujące protokół SCAP można odpowiednio dostosować, aby spełniały wymagania poszczególnych organizacji. Takie listy kontrolne mogą również łączyć poszczególne ustawienia konfiguracji zabezpieczeń systemu z odpowiadającymi im wymogami bezpieczeństwa. Na przykład dostępne są powiązania między bezpiecznymi konfiguracjami podstawowymi systemu Windows XP a zabezpieczeniami opisanymi w dokumencie NIST SP 800-53. Powiązania te mogą pozwolić na udowodnienie, że wdrożone ustawienia zapewniają odpowiednie bezpieczeństwo i są zgodne z wymaganiami. Powiązania te stanowią część list kontrolnych SCAP, które umożliwiają narzędziom SCAP automatyczne generowanie danych z oceny dowodów zgodności. Takie rozwiązanie może przełożyć się na znaczącą oszczędność pracy i kosztów związanych z zarządzaniem konfiguracją. Jeśli narzędzia SCAP nie są dostępne lub nie są obecnie wdrażane w organizacji, należy rozważyć wdrożenie list kontrolnych SCAP dla bezpiecznych konfiguracji bazowych, aby przygotować organizację na dostępność lub wdrożenie takich narzędzi.

Aby zautomatyzować ciągłe monitorowanie znanych podatności oprogramowania można użyć list kontrolnych SCAP i narzędzi SCAP do oceny zainstalowanych zasobów oprogramowania i opracowania strategii łagodzenia skutków znanych

---

[65] Więcej informacji na temat FDCC można znaleźć pod adresem http://fdcc.nist.gov.

[66] Więcej informacji na temat USGCB można znaleźć pod adresem http://usgcb.nist.gov.

[67] Więcej informacji na temat zweryfikowanych produktów SCAP można znaleźć na stronie http://nvd.nist.gov/scapproducts.cfm.

podatności w oparciu o stopień ryzyka. Wykonując regularnie zaplanowane skany architektury korporacyjnej w oparciu o najnowsze dane dotyczące bezpieczeństwa dostępne w formie protokołu SCAP, osoba odpowiedzialna za bezpieczeństwo lub administrator systemu mogą na żądanie uzyskać komplet informacji na temat bezpieczeństwa swoich systemów z punktu widzenia ustawień konfiguracji i znanych podatności w oprogramowaniu.

Częściowo zautomatyzowane zabezpieczenia

Wdrożenie, ocena i monitorowanie niektórych zabezpieczeń mogą nie być możliwe do automatyzacji z wykorzystaniem istniejących narzędzi, jednak często istnieje możliwość ich częściowej automatyzacji przy użyciu języka Open Checklist Interactive Language (OCIL). OCIL określa ramy dla opracowania zestawu pytań, które mają być przedstawione użytkownikowi oraz odpowiednie procedury interpretacji odpowiedzi na pytania. OCIL może być używany w połączeniu z innymi specyfikacjami SCAP, takimi jak eXtensible Configuration Checklist Description Format (XCCDF), aby pomóc w obsłudze przypadków, w których języki niższego poziomu, takie jak Open Vulnerability and Assessment Language (OVAL), nie pozwalają na automatyzację pewnych kontroli. OCIL stanowi znormalizowane podejście do oceny oraz opisu ręcznych kontroli zabezpieczeń. Na przykład użytkownik systemu może usłyszeć pytanie: „Czy posiadasz sejf do przechowywania dokumentów?” Specyfikacja OCIL zapewnia możliwość określania pytań, możliwych odpowiedzi do wyboru, działań, które należy podjąć w wyniku odpowiedzi użytkownika, a także obliczania wyników. Jedną z zalet OCIL jest to, że odpowiedzi mogą być zwracane w znormalizowanym formacie, co pozwala na przeprowadzenie analizy statystycznej i innych zautomatyzowanych obliczeń.

D.3.2. ŹRÓDŁA DANYCH REFERENCYJNYCH

NIST zapewnia dwa repozytoria danych – NVD i listy kontrolne konfiguracji bezpieczeństwa, aby wspierać zarówno zautomatyzowane, jak i ręczne działania w zakresie ciągłego monitorowania bezpieczeństwa informacji.

Krajowa baza danych dotyczących podatności na zagrożenia (NVD)

NVD jest rządowym repozytorium danych dotyczących zarządzania podatnościami opartych na specyfikacji SCAP. Dane te umożliwiają automatyzację zarządzania podatnościami, a także pomiaru bezpieczeństwa i zgodności. NVD zawiera listy kontrolne bezpieczeństwa, informacje o usterkach oprogramowania związanych z bezpieczeństwem, błędy konfiguracji, nazwy produktów i wskaźniki wpływu.

Zawartość NVD jest dynamiczna – informacje o podatnościach są aktualizowane o nowe informacje dotyczące poprawek, listy kontrolne są aktualizowane i uzupełniane na bieżąco. Gdy informacje stają się dostępne w NVD, systemy są skanowane w celu ponownej oceny ryzyka i załatania wszystkich nowych podatności. Aby ułatwić znormalizowaną dystrybucję danych, dane dotyczące podatności na zagrożenia są dostępne w postaci źródeł danych XML i aktualizowane w odstępach dwugodzinnych. Organizacje mogą wykorzystać te znormalizowane dane do automatyzacji ciągłego monitorowania bezpieczeństwa informacji, konfigurując zaplanowane skanowanie systemów i oceny zmian oraz wszelkie związane z nimi zagrożenia bezpieczeństwa.

Listy kontrolne konfiguracji zabezpieczeń

Ustawa o badaniach i rozwoju cyberbezpieczeństwa z 2002 roku[68] wymogła, by NIST „opracował oraz w razie potrzeby zaktualizował listy kontrolne zawierające ustawienia i opcje, które minimalizują ryzyko związane z bezpieczeństwem każdego sprzętu komputerowego lub systemu oprogramowania, który jest lub może być szeroko stosowany w rządzie federalnym". Krajowy program list kontrolnych (NCP)[69] to rządowe repozytorium publicznie dostępnych list kontrolnych bezpieczeństwa. Korzystanie z takich list kontrolnych w kontekście nadrzędnego programu bezpieczeństwa informacji może znacznie zmniejszyć narażenie organizacji na zagrożenia.

[68] Tekst ustawy dotyczącej badań i rozwoju cyberbezpieczeństwa z 2022 roku znajduje się pod adresem http://csrc.nist.gov/drivers/documents/HR3394-final.pdf.

[69] Więcej informacji na temat NCP można znaleźć na stronie http://web.nvd.nist.gov/view/ncp/repository.

Lista kontrolna konfiguracji zabezpieczeń, czasami określana mianem zasad utwardzania systemu lub konfiguracji wzorcowej jest zasadniczo dokumentem zawierającym instrukcje lub procedury konfiguracji systemów informacyjnych w celu uzyskania podstawowego poziomu bezpieczeństwa. Listy kontrolne mogą być opracowywane nie tylko przez dostawców technologii informacyjnych, ale także przez konsorcja, środowiska akademickie i przemysłowe, oraz inne podmioty z sektorów publicznego i prywatnego.

NCP udostępnia listy kontrolne zarówno w formacie tekstowym, jak i w formacie SCAP. Listy kontrolne w formacie SCAP umożliwiają narzędziom SCAP automatyczne przetwarzanie list kontrolnych i skanowanie systemów. Podzbiór list kontrolnych zapewnia również wspólne listy konfiguracji (CCE) powiązane z zabezpieczeniami opisanymi w dokumencie NIST SP 800-53, które umożliwiają wykorzystanie listy kontrolnej w kontekście oceny wymagań zawartych w treści dokumentu NIST SP 800-53. Lista kontrolna może zawierać dowolne z poniższych elementów:

- Pliki konfiguracyjne, które automatycznie konfigurują różne ustawienia zabezpieczeń (np. pliki wykonywalne, szablony zabezpieczeń modyfikujące ustawienia, skrypty).
- Dokumentacja (np. plik tekstowy), która przeprowadza użytkownika listy kontrolnej przez proces ręcznej konfiguracji oprogramowania.
- Dokumenty wyjaśniające zalecane metody bezpiecznej instalacji i konfiguracji urządzenia.
- Zasady, które określają wytyczne dotyczące działań takich jak audyt, uwierzytelnianie (np. hasła) i bezpieczeństwo obwodowe.

Nie wszystkie instrukcje na liście kontrolnej konfiguracji zabezpieczeń dotyczą ustawień zabezpieczeń. Listy kontrolne mogą również obejmować praktyki administracyjne dotyczące danego produktu, które pozwalają na zwiększenie jego bezpieczeństwa. Często udane ataki na systemy są bezpośrednim wynikiem błędnych praktyk administracyjnych, takich jak zignorowanie konieczności zmiany domyślnych haseł lub niezainstalowanie nowych poprawek.

Porównanie list kontrolnych można również przeprowadzić w ramach audytu i ciągłego monitorowania bezpieczeństwa wdrożonych systemów, aby zapewnić zgodność konfiguracji z ustalonym poziomem bazowym. Zwykle nie wystarczy skonfigurować urządzenia i założyć, że ustawienia zostaną zachowane – ustawienia mogą ulegać zmianom wraz z instalacją oprogramowania, a także poprawek i aktualizacji, a także w przypadku podłączania i odłączania komputerów do/od domen. Użytkownicy mogą również samodzielnie zmieniać ustawienia zabezpieczeń, na przykład użytkownik może uznać, że wygaszacz ekranu blokujący ekran jest irytujący i wyłączyć tę funkcję.

D.4 MODEL REFERENCYJNY

Organizacje mogą korzystać z technologii, specyfikacji i referencyjnych źródeł danych omówionych w Załączniku D, aby zaprojektować techniczną implementację ciągłego monitorowania bezpieczeństwa informacji, która maksymalizuje wykorzystanie danych związanych z bezpieczeństwem i sprzyja spójności w planowaniu i wdrażaniu działań ISCM. Tam, gdzie to możliwe, techniczna implementacja ciągłego monitorowania bezpieczeństwa informacji pozwala na automatyzację gromadzenia, zestawiania oraz analizy danych, a także raportowania i ich prezentacji w celu tworzenia wskaźników określonych przez organizację.

Organizacje stoją jednak przed poważnymi wyzwaniami związanymi z integracją tych technologii w celu realizacji działań w zakresie ciągłego monitorowania bezpieczeństwa informacji. Zwykle korzystają one bowiem z zestawu różnorodnych produktów zabezpieczających wielu producentów. Dlatego konieczne jest wyodrębnienie z tych narzędzi informacji związanych z bezpieczeństwem (najlepiej w postaci surowych danych o stanie systemu) i znormalizowanie tych danych, aby były porównywalne (na poziomie 3 oraz na poziomach 2 i 1). Możliwości na poziomie 3 pozwalają na przygotowywanie zapytań oraz opracowywanie sprawozdań z danych zebranych z wielu narzędzi obejmujących wiele domen automatyzacji bezpieczeństwa w związku z działaniami dotyczącymi ciągłego monitorowania bezpieczeństwa informacji. Ze względu na fakt, że w wielu organizacjach istnieje wiele lokalnych repozytoriów poziomu 3 obejmujących różne części dużej organizacji, repozytoria danych związanych z ciągłym monitorowaniem bezpieczeństwa informacji poziomu 3 regularnie przekazują dane do repozytoriów poziomu 2, zgodnie z hierarchiczną architekturą. Repozytoria poziomu 2 z kolei przekazują dane do repozytoriów poziomu 1, które mogą przekazywać dane użytkownikom wyższego poziomu. Ze względu na fakt, że dane są przekazywane na wyższe poziomy hierarchii ciągłego monitorowania bezpieczeństwa informacji, następuje proces ich abstrakcji, ponieważ zwykle nie jest możliwe lub wręcz wskazane replikowanie wszystkich informacji związanych z bezpieczeństwem z niższych poziomów na wszystkich poziomach w hierarchii. Użytkownicy na wyższych poziomach wysyłają zapytania skierowane do

niższych poziomów w celu uzyskania danych. Jednym z kluczowych wyzwań jest potrzeba opracowania technicznego mechanizmu umożliwiającego przekazywanie zapytań wyższego poziomu do instancji ciągłego monitorowania bezpieczeństwa informacji na niższym poziomie w celu ich realizacji. Kolejnym wyzwaniem jest to, że podczas odpowiadania na zapytania instancje ciągłego monitorowania bezpieczeństwa informacji niższego poziomu mogą wymagać przeprowadzenia analizy surowych danych w celu wygenerowania wyników. Wyniki te mogą być ustaleniami (powstającymi na podstawie porównania danych z zasadami) lub punktami (będącymi liczbową oceną rezultatów). W związku z tym potrzebny jest mechanizm, za pomocą którego można przekazać informacje o analizie, która ma zostać przeprowadzona. W idealnym przypadku, jeśli żądane dane nie są dostępne w poziomie 3, wówczas instancja ciągłego monitorowania bezpieczeństwa informacji poziomu 3 zleca różnorodnym narzędziom bezpieczeństwa zebranie żądanych danych.

Wyzwaniom tym można sprostać poprzez zastosowanie modelu referencyjnego, który opisuje rodzaje wymaganych narzędzi, ich relacje i wymagane role w realizacji działań dotyczących ciągłego monitorowania bezpieczeństwa informacji. Model ten wykorzystuje lub zapewnia specyfikacje interfejsów, które umożliwiają integrację tych narzędzi w celu realizacji technicznego wdrożenia systemu ciągłego monitorowania bezpieczeństwa informacji przez organizację. Model zapewnia również specyfikacje dla poszczególnych rodzajów narzędzi, dzięki czemu spełniają one swoje zadania we wdrażaniu ciągłego monitorowania bezpieczeństwa informacji w całej organizacji.

Jednym z przykładów modelu referencyjnego wdrożenia ciągłego monitorowania bezpieczeństwa informacji, który wspiera spójną integrację, jest CAESARS Framework Extension, opisany w raporcie międzyagencyjnym NIST (NISTIR) 7756, *CAESARS Framework Extension*: *An Enterprise Continuous Monitoring Technical Reference Architecture (Draft)*. Dokument NISTIR 7756 stanowi podstawę dla modelu referencyjnego ciągłego monitorowania, który ma na celu umożliwienie organizacjom zestawianie zebranych danych z różnorodnych narzędzi bezpieczeństwa, analizowania tych danych, ocenę, przeszukiwanie danych przez użytkowników i zapewniania ogólnej świadomości sytuacyjnej.

Model opiera się na zestawie wysokopoziomowych procesów, które opisują wymagane przepływy danych w ramach technicznej implementacji procesu ciągłego monitorowania bezpieczeństwa informacji. Procesy te są realizowane poprzez specyfikacje podsystemów modelu (tj. wymagania dotyczące rodzajów narzędzi) i specyfikacje interfejsów do komunikacji z narzędziami. Możliwość wykorzystania modelu zależy częściowo od dostępnej infrastruktury i dojrzałości programu pomiarowego organizacji[70]. Funkcjonalne możliwości architektury wdrożonej w celu obsługi ciągłego monitorowania bezpieczeństwa informacji obejmują gromadzenie danych i ich przechowywanie, wysyłanie zapytań, analizę danych, pobieranie, rozpowszechnianie na wyższych poziomach oraz prezentację wyników.

W modelu gromadzone są dane (dla wstępnie ustalonych wskaźników lub w odpowiedzi na zapytanie użytkownika), w tym dane związane z wdrażaniem i skutecznością zabezpieczeń. Rodzaje źródeł danych obejmują pracowników, procesy, technologie i środowisko komputerowe (w tym wyniki oceny zabezpieczeń). Do gromadzenia danych można wykorzystać różne metody, zarówno zautomatyzowane, jak i ręczne. Organizacje mogą rozważyć wykorzystanie metod opartych na normach w narzędziach do gromadzenia danych w celu zmniejszenia kosztów integracji, umożliwienia interoperacyjności różnych narzędzi i technologii oraz umożliwienia jednorazowego gromadzenia danych i ich wielokrotnego wykorzystywania. Dane generowane przez ludzi mogą być gromadzone za pomocą mechanizmów wykorzystujących automatyzację i znormalizowane metody. Metodologie gromadzenia danych winne być znormalizowane i zautomatyzowane tam, gdzie to możliwe, aby umożliwić wewnątrz- i międzypoziomową wymianę informacji, a także zestawianie i analizy danych.

Zebrane dane są oznaczane metadanymi, gdy są przechowywane w sposób, który maksymalizuje możliwości ponownego wykorzystania zgromadzonych informacji. Dane są normalizowane do celów agregacji, korelacji i spójnego wykorzystania we wskaźnikach.

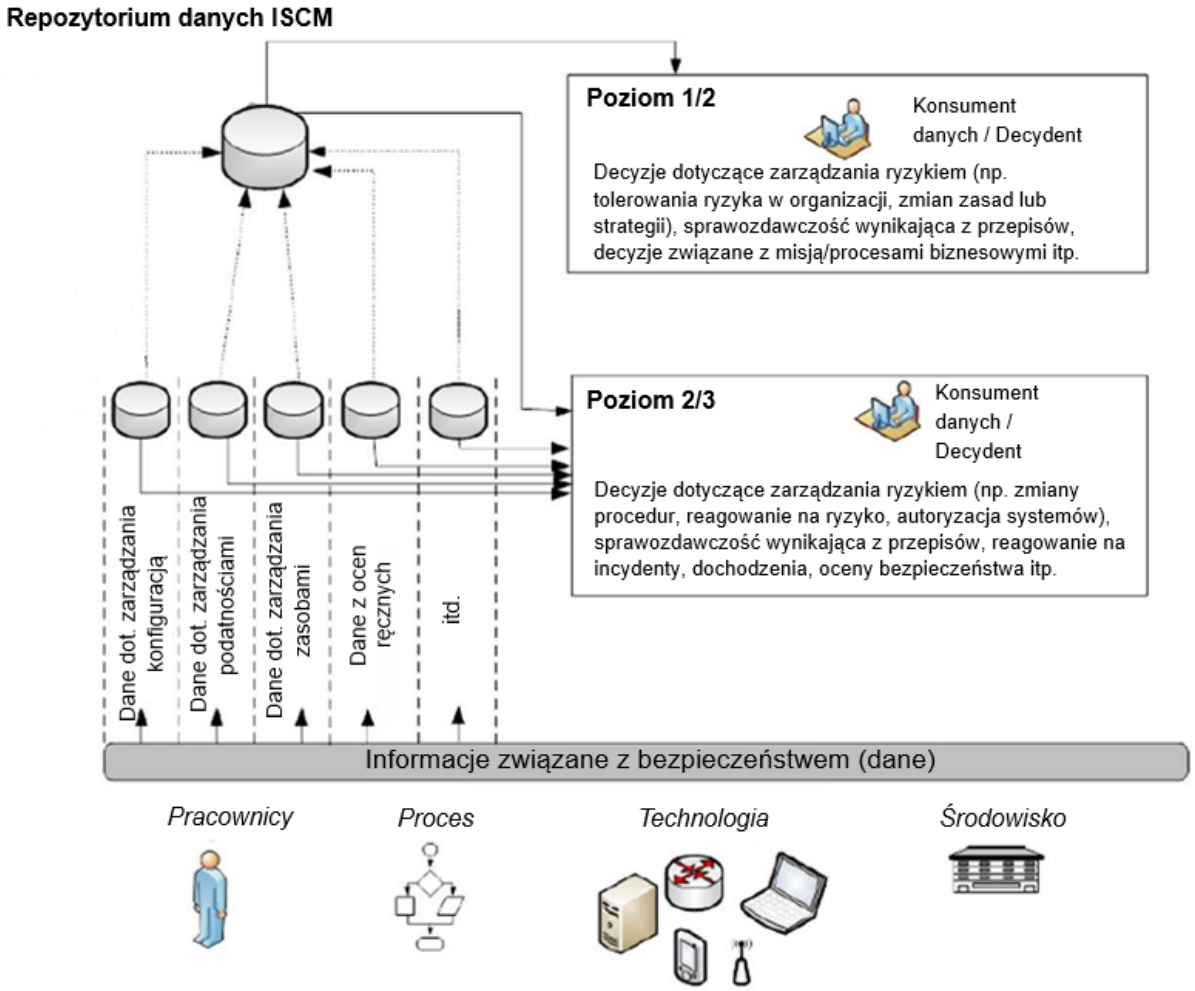
[70] Więcej informacji na temat programów pomiarowych można znaleźć w dokumencie NIST SP 800-55 z późniejszymi zmianami.

Należy zapewnić, by przechowywane były wyłącznie dane, które zostały znormalizowane lub w inny sposób przetworzone z odpowiednimi atrybutami, aby zminimalizować możliwość skażenia wskaźników przez algorytmy czyszczące.

Model ten pozwala na realizację infrastruktury ciągłego monitorowania bezpieczeństwa informacji, która oferuje możliwości wyszukiwania, analizy i prezentacji danych wystarczające do obsługi raportowania i podejmowania decyzji opartych na ryzyku na wszystkich poziomach. Wskaźniki są obliczane zgodnie ze strategią ciągłego monitorowania bezpieczeństwa informacji i ustalonym programem. Wszystkie informacje związane z bezpieczeństwem trafiają do osób pełniących role i realizujących obowiązki związane z ciągłym monitorowaniem bezpieczeństwa informacji, a także innym interesariuszom, w tym konsumentom danych z monitorowania, którzy wykorzystują je w celu zapewniania, by operacje mieściły się w ramach tolerancji ryzyka organizacyjnego zgodnie ze strategią ciągłego monitorowania bezpieczeństwa informacji (np. osobom odpowiedzialnym za zarządzanie poprawkami, ocenę zabezpieczeń, świadomość bezpieczeństwa i szkolenia). Prezentacja danych jest wystarczająco elastyczna, aby zaspokoić różnorodne potrzeby w zakresie dostępu do danych na wszystkich poziomach.

Rysunek D-2 przedstawia wysokopoziomowy widok wdrożenia ciągłego monitorowania bezpieczeństwa informacji zawierający przykładowy przepływ informacji związanych z bezpieczeństwem – od gromadzenia danych źródłowych, poprzez zestawienia i analizy, aż po sprawozdania dostępne dla użytkowników na wszystkich poziomach. Potrzeby użytkowników w zakresie danych dotyczących ciągłego monitorowania bezpieczeństwa informacji różnią się w zależności od poziomu. Administratorzy systemu na poziomie 3 mogą być zainteresowani szczegółami technicznymi w celu realizacji działań na poziomie systemu (np. zmiany konfiguracji), z kolei przedstawiciele zarządu na poziomie 1 mogą być bardziej zainteresowani zestawionymi danymi, które umożliwią im podejmowanie decyzji dotyczących całej organizacji (np. zmian w polityce bezpieczeństwa, zwiększenie przydziału zasobów na programy uświadamiające lub zmiany architektury bezpieczeństwa). Staranne zaprojektowanie ciągłego monitorowania bezpieczeństwa

informacji zapewnia każdemu użytkownikowi *dostęp do danych* w *formacie*, którego potrzebuje i z *częstotliwością* wymaganą do podejmowania skutecznych decyzji. Bardziej szczegółowe informacje na temat modeli referencyjnych ciągłego monitorowania bezpieczeństwa informacji dostępne są w sprawozdaniu NIST Interagency Report 7756.



Rysunek D-2. Przykładowe wdrożenie ISCM