MC

Tłumaczenie standardów i rekomendacji
w zakresie cyberbezpieczeństwa

Przewodnik zarządzania konfiguracją ukierunkowaną na bezpieczeństwo systemów informacyjnych

NIST SP 800-128_wer. 1.0_PL

NIST SP 800-128_wer. 1.0_PL

27 stycznia 2025

Przewodnik zarządzania konfiguracją ukierunkowaną na bezpieczeństwo systemów informacyjnych

Publikacja dostępna pod adresem:

Rekomendacje cyberbezpieczeństwa

NIST Special Publication 800-128

Guide for Security-Focused Configuration Management of Information Systems

Arnold Johnson Kelley Dempsey
Ron Ross Sarbari Gupta Dennis Bailey

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-128

INFORMATION SECURITY

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-128

Guide for Security-Focused Configuration Management of Information Systems

Arnold Johnson Kelley Dempsey
Ron Ross *Computer Security Division Information Technology Laboratory*

Sarbari Gupta Dennis Bailey *Electrosoft Services, Inc.*
Reston, VA

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-128

August 2011
INCLUDES UPDATES AS OF 10-10-2019; SEE PAGE IV

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

O PUBLIKACJI

Niniejsze opracowanie **NIST SP 800-128_wer. 1.0_PL**, ***Przewodnik zarządzania konfiguracją ukierunkowaną na bezpieczeństwo systemów informacyjnych***, stanowi tłumaczenie publikacji NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, i zostało opracowane za zgodą National Institute of Science and Technology.

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 oryginalnej (angielskiej) wersji dokumentu, na podstawie którego powstały niniejsze zalecenia.

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 ***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. Taka identyfikacja nie stanowi rekomendacji, poparcia ani nie ma na celu sugerowania, że dane podmioty, materiały lub urządzenia są bezwzględnie najlepsze z dostępnych dla osiągnięcia danego celu.

[1] Kluczowi uczestnicy zarządzania ryzykiem – patrz: Narodowe Standardy Cyberbezpieczeństwa

RAPORTY DOTYCZĄCE TECHNOLOGII SYSTEMÓW KOMPUTEROWYCH

Laboratorium informatyczne (*Information Technology Laboratory – ITL*) przy Narodowym Instytucie Standaryzacji i Technologii (*National Institute of Standards and Technology – NIST*) działa na rzecz gospodarki krajowej i dobra publicznego poprzez zapewnienie technicznego przywództwa dla infrastruktury pomiarowej i normalizacyjnej kraju. ITL opracowuje badania, metody badań, dane referencyjne, implementacje koncepcji i analizy techniczne, aby przyspieszyć rozwój i produktywne wykorzystanie technologii informacyjnych. Obowiązki ITL obejmują opracowywanie norm i wytycznych w zakresie zarządzania, a także administracyjnych, technicznych i fizycznych związanych z efektywnym kosztowo bezpieczeństwem i prywatnością informacji innych niż związane z bezpieczeństwem narodowym w systemach rządowych. Publikacja specjalna serii 800 zawiera informacje o badaniach, wytycznych i działaniach ITL w zakresie bezpieczeństwa systemów, jak również o współpracy z przemysłem, rządem i organizacjami akademickimi.

STRESZCZENIE

Przewodnik dotyczący zarządzania konfiguracją zorientowaną na bezpieczeństwo systemów informacyjnych zawiera wytyczne dla organizacji odpowiedzialnych za zarządzanie i administrowanie bezpieczeństwem centralnych systemów informacyjnych i powiązanych środowisk operacyjnych. Koncepcje i zasady zarządzania konfiguracją opisane w niniejszej publikacji stanowią informacje pomocnicze do publikacji NSC 800-53[2]. W publikacji NIST SP 800-128_wer. 1.0_PL przyjęto, że bezpieczeństwo informacji jest integralną częścią ogólnego zarządzania konfiguracją w organizacji. Niniejszy dokument koncentruje się na implementacji aspektów bezpieczeństwa systemu informacyjnego w zarządzaniu konfiguracją i jako taki używany jest termin zarządzanie konfiguracją zorientowaną na bezpieczeństwo (*ang. security-focused configuration management - SecCM*), aby podkreślić koncentrację na bezpieczeństwie informacji. Oprócz podstawowych pojęć związanych z SecCM,

[2] Narodowe Standardy Cyberbezpieczeństwa

opisano proces stosowania praktyk SecCM w systemach informacyjnych. Celem działań SecCM jest zarządzanie konfiguracją systemów informacyjnych w celu osiągnięcia odpowiedniego poziomu bezpieczeństwa i monitorowanie go, oraz minimalizacja ryzyka organizacyjnego przy jednoczesnym wsparciu żądanej funkcjonalności i usług biznesowych.

SŁOWA KLUCZOWE

Zarządzanie konfiguracją *(ang. configuration management*); systemy informacyjne (*ang. information systems*); program bezpieczeństwa (*ang. security program*); ramy zarządzania ryzykiem (*ang. risk management framework*); ciągłe monitorowanie zorientowane na bezpieczeństwo (*ang. security-focused continuous monitoring*); zarządzanie konfiguracją zorientowaną na bezpieczeństwo (*ang. security-focused configuration management – SecCM*); zabezpieczenie (*ang. control*); monitorowanie (*ang. monitoring*); automatyczny protokół zabezpieczeń zawartości (*ang. security content automation protocol - SCAP*).

SPIS TREŚCI

Tłumaczenie

SPIS ILUSTRACJI

SPIS TABEL

1. ROZDZIAŁ PIERWSZY

WPROWADZENIE

KONIECZNOŚĆ ZARZĄDZANIA KONFIGURACJĄ W CELU OCHRONY INFORMACJI I SYSTEMÓW

System składa się z wielu komponentów[3], które mogą być połączone w wiele układów, aby spełnić różne potrzeby biznesowe, także związane z misją i bezpieczeństwem informacji. To, jak komponenty systemu są połączone w sieć, skonfigurowane i zarządzane, ma kluczowe znaczenie dla zapewnienia odpowiedniego bezpieczeństwa informacji i obsługi procesu zarządzania ryzykiem w organizacji.

System jest zazwyczaj w trybie ciągłych zmian w odpowiedzi na nowe, rozszerzone, poprawione lub zaktualizowane możliwości sprzętu i oprogramowania, poprawki korygujące błędy oprogramowania i innych istniejących komponentów, nowe zagrożenia bezpieczeństwa, zmieniające się funkcje biznesowe itp. Wdrażanie zmian w systemie prawie zawsze wymaga pewnego dostosowania konfiguracji systemu. Aby wymagane modyfikacje konfiguracji nie wpłynęły negatywnie na bezpieczeństwo systemu lub organizacji, potrzebny jest dobrze zdefiniowany proces zarządzania konfiguracją, który integruje bezpieczeństwo informacji.

Organizacje stosują zarządzanie konfiguracją (CM) do ustalania konfiguracji bazowych oraz do śledzenia i kontrolowania wielu aspektów rozwoju i działania organizacji (np. produktów, usług, procesów produkcji, procesów biznesowych i technologii informacyjnej) i zarządzania nimi. Organizacje mające solidny i skuteczny proces zarządzania konfiguracją, muszą brać pod uwagę implikacje związane z bezpieczeństwem informacji w odniesieniu do rozwoju i działania systemów, w tym sprzętu, oprogramowania, aplikacji i dokumentacji. Skuteczne zarządzanie konfiguracją systemów wymaga integracji zarządzania konfiguracjami bezpieczeństwa z procesem

[3] Składniki systemu obejmują na przykład komputery mainframe, stacje robocze, serwery (w tym serwery baz danych, poczty elektronicznej, uwierzytelniania, WWW, proxy, plików, nazw domen), składniki sieci (w tym zapory, routery, bramy, przełączniki głosu i danych, bezprzewodowe punkty dostępu, urządzenia sieciowe, czujniki), systemy operacyjne, oprogramowanie pośredniczące i aplikacje.

lub procesami zarządzania konfiguracją w organizacji. Dlatego w niniejszym dokumencie zakłada się, że bezpieczeństwo informacji jest integralną częścią ogólnego procesu zarządzania konfiguracją w organizacji. Jednakże skoncentrowano się na implementacji aspektów bezpieczeństwa systemu informacyjnego w zarządzaniu konfiguracją i w takim znaczeniu używany jest termin *zarządzanie konfiguracją zorientowaną na bezpieczeństwo* (SecCM) — aby podkreślić koncentrację na bezpieczeństwie informacji. Zarówno funkcje IT aplikacji biznesowych, jak i praktyki zorientowane na bezpieczeństwo powinny być zintegrowane w jednym procesie, a SecCM w tym kontekście definiuje się jako zarządzanie konfiguracją systemów w celu zapewnienia bezpieczeństwa i ułatwienia zarządzania ryzykiem w zakresie bezpieczeństwa informacji.

1.1 Cel i zastosowanie

Organizacje są odpowiedzialne za „włączenie polityk i procedur, które zapewniają zgodność z minimalnie akceptowalnymi wymaganiami dotyczącymi konfiguracji systemu, określonymi przez organizacje" w ramach ich programu bezpieczeństwa informacji. Zarządzanie konfiguracjami systemów jest również minimalnym wymogiem bezpieczeństwa określonym w dokumentach [NSC 200][4], i [NSC 800-53][5] definiującymi zabezpieczenia wspierające ten wymóg.

Oprócz ogólnych wytycznych dotyczących zapewnienia, aby względy bezpieczeństwa były zintegrowane z procesem zarządzania konfiguracją, niniejsza publikacja zawiera wytyczne dotyczące wdrożenia grupy zabezpieczeń zarządzania konfiguracją zdefiniowane w publikacji [NSC 800-53] (środki bezpieczeństwa od CM-1 do CM-9). Publikacja zawiera również rekomendacje [NSC 800-53] dotyczące środków bezpieczeństwa związane z zarządzaniem konfiguracją architektury systemu i powiązanych komponentów w celu bezpiecznego przetwarzania, przechowywania i przesyłania informacji. Zarządzanie konfiguracją jest ważnym procesem ustanawiania i utrzymywania bezpiecznych konfiguracji systemu oraz stanowi istotne wsparcie dla zarządzania ryzykiem dotyczącym bezpieczeństwa w systemach.

[4] Więcej informacji można znaleźć w publikacji [NSC 200].

[5] Więcej informacji można znaleźć w publikacji [NSC 800-53].

Wytyczne obejmują szeroki zakres zaleceń z perspektywy technicznej, uzupełniających podobne wytyczne dla systemów bezpieczeństwa narodowego, i mogą być stosowane w przypadku takich systemów za zgodą odpowiednich organów sprawujących władzę nad takimi systemami. Zachęca się organizacje sektora prywatnego do rozważenia zastosowania tych wytycznych, w zależności od potrzeb.

Niniejsza publikacja zawiera rekomendacje dla organizacji odpowiedzialnych za zarządzanie i administrowanie bezpieczeństwem systemów i powiązanych środowisk operacyjnych. W przypadku organizacji odpowiedzialnych za bezpieczeństwo informacji przetwarzanych, przechowywanych i przesyłanych przez środowiska zewnętrzne lub zorientowane na usługi (np. dostawcy usług w chmurze), przedstawione tu koncepcje i zasady zarządzania konfiguracją mogą pomóc w ustaleniu wymagań dotyczących zapewnienia bezpieczeństwa dostawcom świadczącym zewnętrzne usługi informatyczne.

1.2 Docelowi odbiorcy

Publikacja przeznaczona jest dla zróżnicowanej grupy odbiorców – specjalistów ds. bezpieczeństwa systemów i informacji. Są to między innymi:

- osoby odpowiedzialne za zarządzanie systemem i bezpieczeństwem informacji oraz nadzór nad nimi (np. kluczowe osoby w jednostce organizacyjnej odpowiedzialne za bezpieczeństwo informacji (SAISO), kluczowe osoby w jednostce organizacyjnej odpowiedzialne za technologie informacyjne (CIO) oraz osoby autoryzujące (AO);
- osoby odpowiedzialne za rozwój systemu (np. menadżerowie programów i projektów, osoby odpowiedzialne za misje /aplikacje projektanci systemów, deweloperzy systemów i aplikacji);
- osoby odpowiedzialne za wdrażanie i funkcjonowanie zasad bezpieczeństwa (np. właściciele systemów informatycznych, właściciele informacji i władający informacją, administratorzy systemów, administratorzy bezpieczeństwa); oraz
- osoby odpowiedzialne za ocenę i monitorowanie bezpieczeństwa systemów i informacji (np. audytorzy, osoby oceniające/zespół oceniający).

Z informacji zawartych w tej publikacji mogą skorzystać również podmioty komercyjne wytwarzające produkty i systemy informatyczne, tworzące technologie związane z bezpieczeństwem informacji oraz świadczące usługi w zakresie bezpieczeństwa informacji.

1.3 Związek z innymi publikacjami dotyczącymi bezpieczeństwa

Koncepcje i zasady zarządzania konfiguracją opisane w niniejszej publikacji stanowią informacje pomocnicze do publikacji [NSC 800-53]. Publikacja dostarcza również ważnych informacji pomocniczych dla etapów wdrażania, oceny i monitorowania ram zarządzania ryzykiem (*ang. Risk Management Framework – RMF*), które są omówione w dokumencie [NSC 800-37]. Szczegółowe zalecenia dotyczące realizacji etapu monitorowania znajdują się w dokumencie [NSC 800-137]. Celem etapu monitorowania w ramach zarządzania ryzykiem jest ciągłe monitorowanie skuteczności wszystkich zabezpieczeń wybranych, wdrożonych i zatwierdzonych do ochrony informacji i systemów organizacji, co obejmuje zabezpieczenia zarządzania konfiguracją zidentyfikowane w dokumencie [NSC 800-53]. Etap monitorowania zidentyfikowany w procesie zarządzania konfiguracją zorientowaną na bezpieczeństwo (SecCM), prezentowany w dalszej części niniejszego dokumentu, wspiera etap monitorowania RMF poprzez zapewnienie konkretnych działań związanych z monitorowaniem architektury strukturalnej systemu oraz konfiguracji oprogramowania i sprzętu, dotyczącej tej architektury systemu.

Wiele z koncepcji i zasad SecCM opisanych w niniejszej publikacji opiera się na podstawowych zasadach ustanowionych w celu zarządzania ryzykiem, znajdujących się w dokumencie [NSC 800-39].

Niniejsza publikacja często odwołuje się do informacji z dokumentów NIST [SP 800-70], *National Checklist Program for IT Products--Guidelines for Checklist Users and Developers*, z późniejszymi zmianami; oraz NIST [SP 800-126], *The Technical Specification for the Security Content Automation Protocol (SCAP)*, wersja 1.3, jako potencjalnych środków automatycznego wsparcia w prowadzeniu wielu działań związanych z zarządzaniem konfiguracją.

Dodatkowo, publikacja odwołuje się do licznych publikacji specjalnych NIST, które zawierają wytyczne dotyczące wykorzystania i konfigurowania konkretnych technologii do zabezpieczania systemów. Wiele z tych publikacji zostało wskazanych w załączniku F – Najlepsze praktyki dotyczące ustanawiania bezpiecznych konfiguracji.

1.4 Struktura publikacji

Pozostała część tej publikacji jest zorganizowana w następujący sposób:

- W **rozdziale drugim** opisano podstawowe pojęcia związane z SecCM, w tym: (I) przegląd ogólnych terminów i koncepcji zarządzania konfiguracją oraz ich związek z ukierunkowanym na bezpieczeństwo zarządzaniem konfiguracją technologii informacyjnych (IT) i systemów; (II) główne etapy SecCM; (III) podstawowe koncepcje istotne dla praktyk związanych z SecCM; oraz (IV) podstawowe role i obowiązki istotne dla SecCM.
- W **rozdziale trzecim** opisano proces stosowania praktyk SecCM do obsługi systemów w organizacji, w tym: (I) planowanie działań SecCM w organizacji; (II) identyfikowanie i wdrażanie bezpiecznych konfiguracji; (III) kontrolowanie zmian konfiguracyjnych w systemach; (IV) monitorowanie konfiguracji systemów w celu zapewnienia, że konfiguracje nie są nieumyślnie zmieniane w stosunku do zatwierdzonych konfiguracji bazowych; oraz (V) stosowanie znormalizowanych protokołów Security Content Automation Protocol (SCAP) do wspierania zautomatyzowanych narzędzi podczas weryfikacji konfiguracji systemów.
- **Pomocnicze załączniki** zawierają bardziej szczegółowe informacje o SecCM, w tym: (A) ogólne odniesienia; (B) słownik terminów i definicji; (C) akronimy; (D) przykładowy zarys planu SecCM; (E) przykładowy szablon wniosku o zmianę konfiguracji; (F) najlepsze praktyki w zakresie ustanawiania bezpiecznych konfiguracji w systemach, (G) schematy przepływu dla różnych procesów i działań SecCM; (H) przykładowa karta zespołu ds. zabezpieczeń konfiguracyjnych (*ang. Configuration Control Board – CCB*) oraz (I) przykładowy szablon analizy wpływu na bezpieczeństwo.

2. ROZDZIAŁ DRUGI

PODSTAWY

PODSTAWOWE POJĘCIA DOTYCZĄCE ZARZĄDZANIA KONFIGURACJĄ BEZPIECZEŃSTWA

W rozdziale przedstawiono podstawy zarządzania konfiguracją zorientowaną na bezpieczeństwo (SecCM), w tym: (I) przegląd podstawowych terminów i koncepcji zarządzania konfiguracją oraz rolę SecCM; (II) podstawowe etapy SecCM; (III) koncepcje SecCM; oraz (IV) role i obowiązki istotne dla SecCM.

2.1 Przegląd

Niniejszy rozdział zawiera przegląd SecCM, w tym jego znaczenie w zarządzaniu ryzykiem organizacyjnym związanym z systemami, podstawowe pojęcia z zakresu zarządzania konfiguracją oraz charakterystykę SecCM w ramach zarządzania konfiguracją.

2.1.1 Podstawowe zarządzanie konfiguracją

Zarządzanie konfiguracją zostało zastosowane do szerokiej gamy produktów i systemów, w takich obszarach tematycznych jak motoryzacja, farmacja i informatyka. Niektóre podstawowe terminy związane z zarządzaniem konfiguracją są krótko wyjaśnione poniżej.

Zarządzanie konfiguracją (*ang. Configuration Management – CM*) obejmuje zestaw działań skoncentrowanych na ustanowieniu i utrzymaniu integralności produktów i systemów przez kontrolę procesów inicjowania, zmiany i monitorowania konfiguracji tych produktów i systemów w całym cyklu życia systemu.

Element konfiguracji (*ang. Configuration Item – CI*) jest możliwą do zidentyfikowania częścią systemu (np. sprzęt, oprogramowanie, oprogramowanie układowe, dokumentacja lub ich kombinacja), która jest odrębnym celem procesów zabezpieczeń konfiguracji (*ang. configuration control processes*).

Konfiguracja bazowa (ang. Baseline Configuration) to zestaw specyfikacji systemu lub elementu konfiguracji w ramach systemu, który został formalnie przejrzany oraz uzgodniony, i który może być zmieniony tylko za pośrednictwem procedury kontroli

zmian. Konfiguracja bazowa jest używana jako podstawa dla przyszłych kompilacji, wersji bądź zmian.

Plan zarządzania konfiguracją (*ang. Configuration Management Plan - Plan CM*) jest kompleksowym opisem ról, odpowiedzialności, polityk i procedur, które mają zastosowanie podczas zarządzania konfiguracją produktów i systemów. Do podstawowych części planu zarządzania konfiguracją należą:

– *Zespół ds. zabezpieczeń konfiguracyjnych* (*Configuration Control Board – CCB*) – grupa wykwalifikowanych osób odpowiedzialnych za proces kontroli i zatwierdzania zmian w całym cyklu rozwojowym i operacyjnym produktów i systemów; może być również określany jako zespół ds. kontroli zmian.

– *Identyfikacja* elementów konfiguracji – metodyka wyboru i nadawania nazw elementom konfiguracji, które muszą być umieszczone w zarządzaniu konfiguracją.

– *Kontrola zmian* konfiguracji – proces zarządzania aktualizacjami konfiguracji bazowej elementów konfiguracji.

– *Monitorowanie* konfiguracji – proces oceny lub testowania poziomu zgodności z ustaloną konfiguracją bazową oraz mechanizmy raportowania o stanie konfiguracji elementów umieszczonych w zarządzaniu konfiguracją.

Niniejsze rekomendacje są związane z zastosowaniem praktyk zarządzania konfiguracją zorientowaną na bezpieczeństwo systemów. Konfiguracja systemu jest reprezentacją jego składników. Określa, jak każdy składnik jest skonfigurowany i jak składniki są połączone lub zorganizowane w celu wdrożenia systemu. Możliwe warunki, w których system lub komponent systemu może być zorganizowany, wpływają na stan bezpieczeństwa systemu. Działania dotyczące zarządzania konfiguracją systemu obejmują opracowanie planu zarządzania konfiguracją, powołanie zespołu ds. zabezpieczeń konfiguracyjnych, opracowanie metodyki identyfikacji elementów konfiguracji, ustalenie konfiguracji bazowej, opracowanie procesu kontroli zmian konfiguracji oraz opracowanie procesu monitorowania konfiguracji i raportowania.

2.1.2 Wyzwania związane z ochroną informacji i zarządzaniem ryzykiem

Wszechobecność technologii informacyjnych zwiększa zależność od systemów, dlatego organizacje stają w obliczu wzrostu liczby i dotkliwości zagrożeń, które mogą mieć negatywny wpływ na operacje, aktywa i osoby. Biorąc pod uwagę potencjalne szkody, które mogą powstać w wyniku zakłóceń środowiskowych, błędów ludzkich, celowych ataków wrogich podmiotów i innych zagrożeń, organizacja musi położyć większy nacisk na zarządzanie ryzykiem związanym z systemami, ponieważ jej celem jest realizacja misji i procesów biznesowych. Podstawą wszelkich działań dotyczących zarządzania ryzykiem organizacyjnym związanym z systemami jest skuteczny program bezpieczeństwa[6].

Na organizacji spoczywa obowiązek wdrożenia zaleceń w sposób zapewniający odpowiednie bezpieczeństwo[7] w zakresie ochrony informacji i systemów. W związku z ciągłym rozwojem zagrożeń w środowisku, w którym organizacje mają ograniczone zasoby służące do ochrony, bezpieczeństwo stało się działaniem opartym na ryzyku, w którym koszty operacyjne i ekonomiczne zapewnienia, że dane zagrożenie nie wykorzysta podatności, są równoważone z potrzebami misji i procesów biznesowych organizacji. W świecie ograniczonych zasobów praktyka zarządzania ryzykiem ma fundamentalne znaczenie dla programu bezpieczeństwa informacji.

W strategiach ochrony misji opartych na ryzyku organizacje wyraźnie identyfikują i reagują na ryzyko związane z wykorzystaniem systemów w realizacji misji i procesów biznesowych. Dokładnie rozważa się, jak szereg różnorodnych zagrożeń może wykorzystać istniejące podatności i wyrządzić szkodę organizacji. W ramach zarządzania ryzykiem organizacje często mają bardzo małą kontrolę nad zagrożeniami. Organizacje nie mają wpływu na występowanie trzęsień ziemi, powodzi, na niezadowolonych pracowników, hakerów i wiele innych zagrożeń; mogą jednak

[6] Bezpieczeństwo informacji jest definiowane jako ochrona informacji i systemów przed nieuprawnionym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem działania, modyfikacją lub zniszczeniem w celu zapewnienia poufności, integralności i dostępności. Na potrzeby niniejszej publikacji pojęcie „bezpieczeństwo” dotyczy „bezpieczeństwa informacji”, a pojęcie „system” – „systemu informacyjnego”.

[7] Odpowiednia ochrona to ochrona współmierna do ryzyka i wielkości szkody wynikającej z utraty, czy niewłaściwego użycia danych lub nieuprawnionego dostępu do nich.

kontrolować podatności oraz redukować zagrożenia przez wdrożenie solidnego procesu SecCM, który jest częścią ogólnego procesu zarządzania ryzykiem. Podatności reprezentują różne rodzaje słabych punktów, które mogą być wykorzystane przez zagrożenie. Analiza podatności systemu ujawnia wiele potencjalnych przyczyn, jednak wiele podatności można przypisać wadom oprogramowania i niewłaściwej konfiguracji komponentów systemu.

Zarządzanie konfiguracjami było tradycyjnie postrzegane jako najlepsza praktyka zarządzania IT[8]. Wykorzystanie SecCM do uzyskania większej kontroli i zapewnienia integralności zasobów IT, ułatwia zarządzanie aktywami, usprawnia reagowanie na incydenty, pracę helpdesku, odzyskiwanie danych po awarii i rozwiązywanie problemów, wspomaga rozwój oprogramowania i zarządzanie wersjami, zwiększa automatyzację procesów oraz zapewnia zgodność z politykami i wspomaga przygotowanie do audytów.

2.1.3 Rola zarządzania konfiguracją zorientowaną na bezpieczeństwo[9]

Konfiguracja systemu i jego komponentów ma bezpośredni wpływ na stan bezpieczeństwa systemu. Sposób tworzenia i utrzymywania konfiguracji wymaga zdyscyplinowanego podejścia w celu zapewnienia odpowiedniego poziomu bezpieczeństwa. Zmiany konfiguracji systemu są często konieczne, aby dotrzymać kroku zmieniającym się funkcjom i usługom biznesowym oraz potrzebom w zakresie bezpieczeństwa informacji. Jednak zmiany mogą mieć negatywny wpływ na wcześniej ustalony stan bezpieczeństwa, dlatego skuteczne zarządzanie konfiguracją jest

[8] Za najlepsze praktyki często uważa się sprawdzone działania lub procesy, które były z powodzeniem stosowane przez wiele organizacji. Najlepsze praktyki zarządzania IT, o których mowa w niniejszej publikacji, są postrzegane z perspektywy całej organizacji jako działania, które najlepiej wspierają misję i funkcje biznesowe lub usługi organizacji.

[9] Istnieje wiele organizacji, które udokumentowały standardy najlepszych praktyk i wytyczne dotyczące zarządzania konfiguracją poprzedzające niniejszą publikację i wpływają na jej kierunek. Są to norma [ISO 10007]; norma [IEEE 828-2012]; Kompleksowy model dojrzałości organizacyjnej (*ang. Capability Maturity Model Integration*)[CMMI], dotyczący przede wszystkim zarządzania konfiguracją w zakresie dokumentów związanych z tworzeniem oprogramowania; biblioteka Information Technology Infrastructure Library [ITIL], mająca wpływ na integrację konfiguracji w ramach zarządzania technologią informacyjną; oraz Międzynarodowa Organizacja Normalizacyjna (*International Organization for Standardization – ISO*), zajmująca się zarządzaniem konfiguracją w ramach systemów zarządzania jakością.

kluczowe dla ustanowienia i utrzymania bezpieczeństwa informacji i systemów. Proces zarządzania konfiguracją zorientowaną na bezpieczeństwo ma kluczowe znaczenie dla utrzymania bezpiecznego stanu w ramach normalnych operacji, operacji odzyskiwania danych w sytuacjach awaryjnych oraz przywracania do działania.

Zarządzanie konfiguracją zorientowaną na bezpieczeństwo (*ang. Security Focused Configuration Management – SecCM*) to zarządzanie bezpiecznymi konfiguracjami systemu w celu zapewnienia bezpieczeństwa i ułatwienia zarządzania ryzykiem oraz ich kontrola. SecCM bazuje na ogólnych koncepcjach, procesach i działaniach związanych z zarządzaniem konfiguracją, z uwzględnieniem wdrożenia i utrzymaniem ustalonych wymagań bezpieczeństwa organizacji i systemów.

Wymagania dotyczące zarządzania konfiguracją bezpieczeństwa informacji są zintegrowane z istniejącymi procesami zarządzania konfiguracją organizacji (np. funkcjami biznesowymi, aplikacjami, produktami) i systemami informacyjnymi (lub je uzupełniają). Działania SecCM obejmują:

- identyfikację i rejestrację konfiguracji, które mają wpływ na stan bezpieczeństwa systemu i organizacji;
- uwzględnienie ryzyka bezpieczeństwa przy zatwierdzaniu wstępnej konfiguracji;
- analizę wpływu zmian konfiguracji systemu na bezpieczeństwo; oraz
- dokumentowanie zatwierdzonych/wprowadzonych zmian.

W przypadkach, gdy w organizacji nie ma procesu CM, praktyki zarządzania konfiguracją zorientowaną na bezpieczeństwo, określone w niniejszym dokumencie, są opracowywane i wdrażane od początku procesu.

Początkowe wdrożenie programu SecCM może wymagać znacznego wysiłku. Jeśli w organizacji nie ma procesu SecCM, należy początkowo zainwestować w opracowanie i wdrożenie programu, który jest wystarczająco wszechstronny, aby objąć wiele technologii, strukturę organizacyjną i rozbieżne procesy, i który może zapewnić spójne wyniki przy jednoczesnym wsparciu misji i procesów biznesowych organizacji. Ponadto należy pozyskać i wdrożyć narzędzia, zinwentaryzować

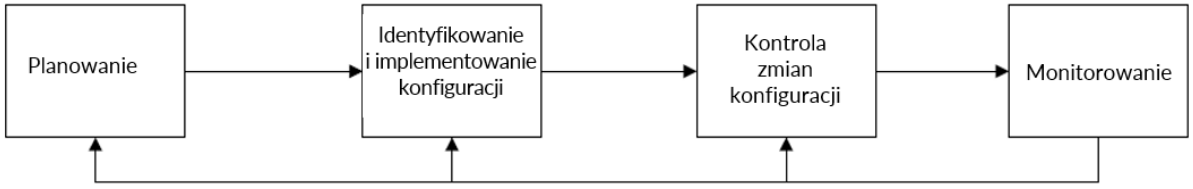
i zarejestrować elementy systemu oraz zmodyfikować procesy, aby uwzględnić nowe sposoby zarządzania technologią w kontekście SecCM.

Raz wprowadzony proces SecCM wymaga ciągłych inwestycji w czas i zasoby. Analiza wpływu poprawek i aktualizacji produktów na bezpieczeństwo wymaga czasu, nawet jeśli zagrożenia i podatności nie są usuwane natychmiast. W miarę wprowadzania zmian w systemach aktualizowana jest konfiguracja bazowa, potwierdzane określone ustawienia konfiguracyjne, a elementy konfiguracji są śledzone, weryfikowane i raportowane. Proces SecCM obejmuje ciągłe działania, które po włączeniu do procesów zarządzania IT dotyczą wszystkich etapów cyklu życia systemu (*ang. System Development Life Cycle -SDLC*). Organizacje, które wdrożą proces SecCM w całym cyklu życia systemu i włączą jego założenia do kultury zarządzania IT, najprawdopodobniej odniosą korzyści w postaci poprawy bezpieczeństwa i funkcjonalności oraz skuteczniejszego zarządzania ryzykiem w organizacji.

2.2 Etapy zarządzania konfiguracją zorientowaną na bezpieczeństwo

Zarządzanie konfiguracją systemów zorientowaną na bezpieczeństwo obejmuje zestaw działań, które można podzielić na cztery główne etapy: Planowanie; Identyfikacja i wdrażanie konfiguracji; Kontrola zmian konfiguracji; Monitorowanie. To właśnie dzięki tym etapom SecCM nie tylko wspiera bezpieczeństwo systemu i jego komponentów, ale także zarządzanie ryzykiem w organizacji. W rozdziale 3 przedstawiono szczegółowe procesy i rozważania dotyczące realizacji niezbędnych działań na każdym z tych etapów.

Na rysunku 2-1 przedstawiono cztery etapy SecCM i opisano je poniżej.



Rysunek 2-1– Etapy zarządzania konfiguracją zorientowaną na bezpieczeństwo

2.2.1 Planowanie

Jak w przypadku wielu działań związanych z bezpieczeństwem, planowanie może w znacznym stopniu wpłynąć na sukces lub porażkę działania. W ramach planowania identyfikowany jest zakres lub możliwość zastosowania procesów SecCM.

Planowanie obejmuje opracowanie polityki i procedur włączenia SecCM do istniejących programów dotyczących technologii informacyjnych i bezpieczeństwa, a następnie rozpowszechnienie tej polityki w całej organizacji. Polityka dotyczy takich obszarów jak wdrażanie planów SecCM, integracja z istniejącymi planami programów bezpieczeństwa, zespołu ds. zabezpieczeń konfiguracyjnych (CCB), procesów kontroli zmian konfiguracji, narzędzi i technologii, wykorzystania typowych bezpiecznych konfiguracji[10] i konfiguracji bazowych, monitorowania oraz metryki zgodności z ustaloną polityką i procedurami SecCM. Zazwyczaj bardziej opłacalne jest opracowanie i wdrożenie planu SecCM, polityk, procedur i powiązanych narzędzi SecCM na poziomie zarządzania ryzykiem organizacji lub misji/procesu biznesowego[11].

2.2.2 Identyfikowanie i wdrażanie konfiguracji

Po zakończeniu planowania i działań przygotowawczych należy opracować, przejrzeć, zatwierdzić i wdrożyć bezpieczną konfigurację bazową systemu. Zatwierdzone konfiguracje bazowe systemu i powiązanych komponentów reprezentują najbardziej bezpieczny stan zgodny z wymaganiami i ograniczeniami operacyjnymi. W przypadku typowego systemu, bezpieczna konfiguracja bazowa może dotyczyć ustawień konfiguracyjnych, obciążeń programowych, poziomów poprawek, sposobu fizycznego lub logicznego rozmieszczenia systemu informacyjnego, wdrożenia różnych zabezpieczeń oraz dokumentacji. Tam, gdzie jest to możliwe, stosuje się automatyzację, aby zapewnić interoperacyjność narzędzi i jednolitość konfiguracji bazowych w całym systemie.

[10] Typowa bezpieczna konfiguracja to uznany, znormalizowany i ustalony wzorzec (np. National Checklist Program, metodyki DISA STIG itp.), który określa konkretne ustawienia bezpiecznej konfiguracji dla danej platformy IT. Patrz https://www.nist.gov/programs-projects/national-checklist-program

[11] Patrz [NSC 800-39], aby uzyskać informacje na temat poziomów zarządzania ryzykiem.

2.2.3 Kontrola zmian konfiguracji

Biorąc pod uwagę stale zmieniający się charakter systemu i misji, którą ten system wspiera, wyzwaniem dla organizacji jest nie tylko ustanowienie początkowej konfiguracji bazowej, która reprezentuje bezpieczny stan (również opłacalny, funkcjonalny i wspierający misję i procesy biznesowe), lecz także utrzymanie bezpiecznej konfiguracji w obliczu znacznych zmian, które dotyczą organizacji.

Na tym etapie procesu SecCM uwzględnia się zarządzanie zmianą w celu utrzymania bezpiecznej, zatwierdzonej konfiguracji bazowej systemu. Dzięki zastosowaniu praktyk SecCM organizacje zapewniają, że zmiany są przed wdrożeniem formalnie identyfikowane, proponowane, przeglądane, analizowane pod kątem wpływu na bezpieczeństwo, testowane i zatwierdzane. W ramach kontroli zmian konfiguracji organizacje mogą stosować różne ograniczenia dostępu do zmian, w tym kontrole dostępu, automatyzację procesów, poziomy abstrakcji, okna serwisowe oraz działania weryfikacyjne i audyty w celu ograniczenia nieautoryzowanych bądź nieudokumentowanych zmian w systemie.

2.2.4 Monitorowanie

Działania monitorujące są wykorzystywane w ramach SecCM do sprawdzenia, czy system jest zgodny z politykami obowiązującymi w organizacji, procedurami oraz zatwierdzonymi bezpiecznymi konfiguracjami bazowymi. Zaplanowanie i wdrożenie bezpiecznych konfiguracji, a następnie kontrola ich zmian zazwyczaj nie wystarcza, aby zapewnić, że zmieniony system będzie nadal bezpieczny. Monitorowanie identyfikuje nieujawnione/nieudokumentowane komponenty systemu, błędne konfiguracje, podatność na zagrożenia i nieautoryzowane zmiany, które, jeśli nie zostaną usunięte, mogą narazić organizacje na zwiększone ryzyko. Wykorzystanie zautomatyzowanych narzędzi pomaga organizacjom skutecznie identyfikować, kiedy system nie jest zgodny z zatwierdzoną konfiguracją bazową i kiedy są konieczne działania naprawcze. Ponadto wykorzystanie zautomatyzowanych narzędzi często ułatwia rozpoznawanie zagrożeń i dokumentowanie odstępstw od konfiguracji bazowej.

Procesy i wymagania w ramach wszystkich czterech etapów SecCM nie są statyczne, dlatego procesy na wszystkich czterech etapach należy przeglądać i korygować w miarę potrzeb, aby wspierać zarządzanie ryzykiem w organizacji. Działania monitorujące SecCM mogą spowodować powrót do któregokolwiek z poprzednich etapów (patrz rys. 2-1) i wprowadzenie zmian.

Monitorowanie SecCM odbywa się za pomocą działań oceniających i sprawozdawczych. Raporty dotyczą bezpiecznego stanu poszczególnych konfiguracji systemu i są wykorzystywane jako dane wejściowe zgodnie z wymogami ram zarządzania ryzykiem w zakresie ciągłego monitorowania bezpieczeństwa informacji[12]. Monitorowanie SecCM może również wspomagać zbieranie informacji dla metryk, które mogą być wykorzystane do zapewnienia ilościowych dowodów na to, że program SecCM spełnia określone cele i może służyć do ogólnej poprawy procesów SecCM.

2.3 Koncepcje zarządzania konfiguracją zorientowaną na bezpieczeństwo

W tym podrozdziale opisano podstawowe pojęcia istotne dla praktyki SecCM w organizacji. Ponieważ organizacje mają bardzo zróżnicowane misje i struktury organizacyjne, mogą istnieć różnice w sposobie wdrażania procesu SecCM i zarządzania nim.

2.3.1 Polityka i procedury zarządzania konfiguracją

Opracowanie udokumentowanej polityki SecCM zapewnia członkom organizacji przekazanie oczekiwań kierownictwa wyższego szczebla wobec SecCM przez konkretne, mierzalne i możliwe do potwierdzenia cele. Jest to podejście „od góry do dołu", które określa, co jest wymagane, a co niedozwolone w odniesieniu do stosowania SecCM do zarządzania i kontroli zasobów informacyjnych.

Polityka określa cele działań, natomiast procedury opisują, w jaki sposób cele polityki są realizowane przez konkretne działania i wyniki. Procedury SecCM są

[12] Więcej informacji na temat ciągłego monitorowania bezpieczeństwa informacji znajduje się w publikacji [NSC 800-137].

opracowywane w celu opisania metodyki i zadań dla każdego działania, wspomagającego realizację polityki SecCM.

Dokumentowanie polityki i procedur zarządzania konfiguracją odbywa się na etapie planowania i wspomaga wdrażanie zabezpieczeń **CM-1 Polityka i procedury**, zawartych w [NSC 800-53].

2.3.2 Plan zarządzania konfiguracją

Plan zarządzania konfiguracją służy do opisu sposobu realizacji polityki SecCM. Plan SecCM może dotyczyć całej organizacji lub może być zlokalizowany i dostosowany do systemu lub grupy systemów wspomagających misję/proces biznesowy w organizacji. Plan SecCM może mieć formę całościowego, samodzielnego dokumentu, w którym opisano wszystkie aspekty SecCM, lub może być zawarty w szerzej zdefiniowanych procedurach CM. Plan SecCM może również przyjąć formę zestawu dokumentów i załączników, które łącznie będą opisywać wszystkie aspekty SecCM. Ponadto, plan SecCM może przyjąć formę zestawu predefiniowanych elementów danych w repozytorium.

Plan SecCM jest tworzony na etapie planowania i wspomaga wdrażanie zabezpieczeń [NSC 800-53] - **CM-1 Polityka i procedury** oraz **CM-9 Plan zarządzania konfiguracją**.

2.3.3 Zespół ds. zabezpieczeń konfiguracyjnych

Zespół ds. zabezpieczeń konfiguracyjnych (*ang. Configuration Control Board – CCB*) jest grupą składającą się zazwyczaj z dwóch lub więcej osób, które ponoszą zbiorową odpowiedzialność i mają uprawnienia do przeglądania i zatwierdzania zmian w systemie informacyjnym. Do oceny i zatwierdzania zmian w systemie jest wybierana grupa, która reprezentuje różne perspektywy w organizacji. CCB pełni funkcję kontrolną i zapewnia równowagę działań związanych ze zmianami konfiguracji, sprawiając, że zmiany są utrzymywane zgodnie z kryteriami określonymi w organizacji (np. zakres, koszt, wpływ na bezpieczeństwo) przed ich wdrożeniem.

CCB może miej charakter mniej formalny dla systemów, które mają ograniczony rozmiar, zakres i poziom krytyczności w kontekście misji organizacji. Organizacja określa wielkość i poziom sformalizowania CCB, odpowiednio dla danego systemu (lub systemów) w organizacji.

Utworzenie CCB jest częścią etapu planowania SecCM i wspomaga realizację zabezpieczeń [NSC 800-53] - **CM-3 Zabezpieczanie zmian konfiguracji.**

2.3.4 Wykaz komponentów

Wykaz komponentów to lista komponentów występujących w organizacji aż do najniższego poziomu systemu. Skonsolidowana reprezentacja komponentów wszystkich systemów w organizacji zapewnia ich większą widoczność i lepszą kontrolę, ułatwiając wdrożenie i działanie programu bezpieczeństwa oraz zarządzanie nim. Organizacja określa poziom szczegółowości danych wymagany do śledzenia komponentów dla SecCM. Na przykład, jedna organizacja może śledzić jako pojedyncze składniki wszystkie komponenty do poziomu stacji roboczej (wraz z urządzeniami peryferyjnymi), podczas gdy inna może dokumentować każde urządzenie peryferyjne jako oddzielny komponent.

Każdy komponent jest związany tylko z jednym systemem, a uprawnienia i odpowiedzialność, które są z nim związane, należą tylko do jednego właściciela systemu (tzn. każda pozycja w wykazie komponentów mieści się w granicach uprawnień jednego systemu).

Utworzenie wykazu komponentów systemu jest częścią etapu planowania SecCM i wspomaga wdrożenie zabezpieczeń [NSC 800-53] - **CM-8 Inwentaryzacja komponentów systemu.**

2.3.5 Elementy konfiguracji

W kontekście SecCM systemów, element konfiguracji (*ang. configuration item - CI*) jest agregatem składników systemu, który jest przeznaczony do zarządzania konfiguracją i traktowany jako pojedyncza jednostka w całym procesie SecCM. Element konfiguracji jest identyfikowany, oznaczany i śledzony podczas swojego cyklu życia – jest celem wielu działań w ramach procesu SecCM, takich jak kontrola zmian konfiguracji i działania monitorujące. Elementem konfiguracji może być konkretny komponent systemu (np. serwer, stacja robocza, router, aplikacja), grupa komponentów systemu (np. grupa serwerów z podobnymi systemami operacyjnymi, grupa komponentów sieciowych, takich jak routery i przełączniki, aplikacja lub zestaw aplikacji), obiekt niebędący komponentem (np. oprogramowanie układowe,

dokumentacja) lub system jako całość. Elementy konfiguracji zapewniają organizacjom sposób na dekomponowanie systemu na części, których konfiguracjami można aktywnie zarządzać.

Celem podziału systemu na elementy konfiguracji jest zapewnienie większej szczegółowości danych i kontroli zarządzania bezpieczną konfiguracją systemu. Poziom szczegółowości danych różni się w zależności od organizacji i systemów i jest równoważony przez koszty zarządzania dla każdego elementu konfiguracji. W jednej organizacji właściwe może być utworzenie pojedynczego elementu konfiguracji do śledzenia wszystkich laptopów w systemie, podczas gdy w innej każdy laptop może stanowić osobny element konfiguracji.

Identyfikacja elementów konfiguracji składających się na system jest częścią etapu planowania SecCM i wspomaga implementację zabezpieczeń [NSC 800-53] - **CM-3 Zabezpieczanie zmian konfiguracji.**

2.3.6 Bezpieczne konfiguracje systemów informacyjnych

Konfiguracje reprezentują możliwe stany, w których może się znajdować system i jego komponenty. Bezpieczne konfiguracje mają na celu zmniejszenie organizacyjnego ryzyka dotyczącego bezpieczeństwa związanego z działaniem systemu i mogą obejmować korzystanie z zaufanych lub zatwierdzonych obciążeń programowych, utrzymywanie aktualnych poziomów poprawek, stosowanie bezpiecznych ustawień konfiguracyjnych używanych produktów IT oraz wdrażanie platform ochrony punktów końcowych. Bezpieczne konfiguracje systemu są najczęściej uzyskiwane przez zastosowanie bezpiecznych ustawień konfiguracyjnych produktów informatycznych (np. systemów operacyjnych, baz danych itp.) wykorzystywanych do budowy systemu. Na przykład bezpieczna konfiguracja dla wybranych produktów informatycznych wykorzystywanych w systemie lub organizacji mogłaby uwzględniać zasadę minimalnej funkcjonalności. Zasada minimalnej funkcjonalności pomaga zminimalizować możliwość wprowadzenia luk w zabezpieczeniach i obejmuje między innymi wyłączenie lub odinstalowanie nieużywanych/niepotrzebnych funkcji systemu operacyjnego (*ang. operating system - OS*), protokołów, portów i usług oraz ograniczenie oprogramowania, które można zainstalować, i funkcjonalności tego oprogramowania.

Zaimplementowanie bezpiecznych konfiguracji jest częścią etapu identyfikacji i wdrażania konfiguracji i wspomaga realizację zabezpieczeń [NSC 800-53] - **CM-6 Ustawienia konfiguracji** oraz **CM-7 - Zasada minimalnej funkcjonalności.**

2.3.7 Konfiguracja bazowa

Konfiguracja bazowa to zestaw specyfikacji dla systemu lub elementu konfiguracji w ramach systemu, który został formalnie przejrzany i uzgodniony oraz który może być zmieniony tylko za pośrednictwem procedur kontroli zmian. Konfiguracja bazowa jest używana jako podstawa dla przyszłych kompilacji, wersji bądź zmian.

Konfiguracja bazowa systemu może się zmieniać w czasie w zależności od etapu cyklu życia systemu (SDLC). Na początku cyklu życia systemu, gdy jest on inicjowany i pozyskiwany, punktem odniesienia może być zbiór wymagań funkcjonalnych. W miarę rozwoju i wdrażania systemu, konfiguracja bazowa może się rozszerzyć o dodatkowe elementy, takie jak: projekt techniczny, obciążenie oprogramowania, architektura oraz konfiguracje systemu i jego poszczególnych komponentów. Konfiguracja bazowa może również reprezentować różne środowiska przetwarzania informacji, takie jak: środowisko deweloperskie, testowe i produkcyjne.

Podczas ustalania nowej konfiguracji bazowej, zatwierdzane są wszystkie zmiany od ostatniej zatwierdzonej konfiguracji. Starsze wersje zatwierdzonych konfiguracji bazowych są utrzymywane i udostępniane do przeglądu lub wycofania w razie potrzeby.

Opracowanie i udokumentowanie konfiguracji bazowej systemu jest częścią etapu identyfikacji i wdrażania konfiguracji i wspomaga wdrożenie zabezpieczeń [NSC 800-53] - **CM-2 Konfiguracja bazowa.**

2.3.8 Kontrola zmian konfiguracji

Kontrola zmian konfiguracji to udokumentowany proces zarządzania zmianami w konfiguracji systemu lub wchodzących w jego skład elementów składowych. Kontrola zmian konfiguracji systemu obejmuje systematyczne proponowanie, uzasadnianie, wdrażanie, testowanie/ocenę, przegląd i usuwanie zmian w systemie, w tym uaktualnień i modyfikacji. Kontrola zmian konfiguracji jest stosowana w celu uwzględnienia zmian w komponentach systemu, zmian ustawień konfiguracyjnych produktów informatycznych, zmian awaryjnych/nieplanowanych

oraz mających na celu usunięcie wad. Zmiany są kontrolowane od momentu ich zaproponowania do wdrożenia i przetestowania. Każdy krok w procesie zmiany jest jasno określony wraz z odpowiedzialnością i uprawnieniami zaangażowanych ról.

Kontrola zmian konfiguracji należy do etapu kontrolowania zmian konfiguracji i wspomaga realizację zabezpieczeń [NSC 800-53] - **CM-3 - Kontrola zmian konfiguracji** oraz **CM-5 - Ograniczenia możliwości dokonywania zmian.**

2.3.9 Analiza wpływu na bezpieczeństwo

Analiza wpływu na bezpieczeństwo to analiza przeprowadzana przez wykwalifikowany personel w organizacji w celu określenia stopnia, w jakim zmiany w systemie wpływają na stan bezpieczeństwa systemu. Ponieważ systemy podlegają zazwyczaj ciągłym zmianom, ważne jest zrozumienie wpływu zmian na funkcjonalność istniejących zabezpieczeń oraz tolerancję ryzyka w organizacji. Analiza wpływu na bezpieczeństwo jest włączona do udokumentowanego procesu kontroli zmian konfiguracji.

Analiza wpływu zmiany na bezpieczeństwo obejmuje analizę i ocenę zmiany pod kątem negatywnego wpływu na bezpieczeństwo, najlepiej przed jej zatwierdzeniem i wdrożeniem, ale także w przypadku zmian awaryjnych/nieplanowanych. Po wdrożeniu i przetestowaniu zmian przeprowadzana jest analiza wpływu na bezpieczeństwo (bądź ocena) w celu zapewnienia, że zmiany zostały wdrożone zgodnie z zatwierdzeniem, oraz sprawdzenia, czy istnieją jakiekolwiek nieprzewidziane skutki zmiany dla istniejących zabezpieczeń.

Analiza wpływu na bezpieczeństwo jest wykonywana w ramach etapu kontroli zmian konfiguracji SecCM i wspomaga wdrożenie zabezpieczeń [NSC 800-53] - **CM-4 Analizy wpływu.**

2.3.10 Monitorowanie konfiguracji

Monitorowanie konfiguracji obejmuje działania mające na celu określenie, czy systemy są skonfigurowane zgodnie z uzgodnionymi przez organizację konfiguracjami bazowymi oraz czy komponenty zidentyfikowane w systemie są zgodne z wykazem komponentów utrzymywanym przez organizację.

Monitorowanie konfiguracji pomaga zapewnić, że środki bezpieczeństwa SecCM działają zgodnie z przeznaczeniem i skutecznie zapewniają bezpieczeństwo, wspierając jednocześnie przestrzeganie polityk i procedur SecCM. Monitorowanie konfiguracji może również pomóc w motywowaniu pracowników do wykonywania czynności SecCM zgodnie z polityką i procedurami. Ponadto monitorowanie konfiguracji wspomaga organizacje w ich wysiłkach na rzecz dostosowania się do ram zarządzania ryzykiem[13]. Informacje zebrane podczas monitorowania konfiguracji mogą być wykorzystane do wsparcia ogólnych działań dotyczących ciągłego monitorowania[14], w tym bieżących ocen konkretnych zabezpieczeń i aktualizacji dokumentacji, takich jak: plany bezpieczeństwa systemu, raporty oceny bezpieczeństwa i raporty o stanie bezpieczeństwa. Możliwości automatyzacji, takie jak te zdefiniowane w protokole SCAP, mogą być wykorzystane do zautomatyzowania działań związanych z oceną.

Monitorowanie konfiguracji jest częścią etapu planowania SecCM i wspomaga wdrożenie zabezpieczeń [NSC 800-53] w grupie zabezpieczeń zarządzania konfiguracją.

2.4 Role i obowiązki SecCM

Zestaw ról (na poziomie organizacji, misji/procesu biznesowego i systemu), które są istotne dla programu SecCM, jest zdefiniowany wraz z zakresem odpowiedzialności. Odpowiedzialność ta dotyczy wyłącznie SecCM, nie obejmuje innych przypisanych do ról obowiązków, które nie są związane z SecCM. Typowe role i obowiązki SecCM obejmują[15]:

Chief Information Officer (CIO)

Chief Information Officer, czyli kluczowa osoba w jednostce organizacyjnej odpowiedzialna za technologie informacyjne, wyznacza kierownika programu SecCM w organizacji oraz zatwierdza plan organizacyjny i politykę SecCM.

[13] Więcej informacji na temat RMF można znaleźć w publikacji NIST SP 800-37.

[14] Więcej informacji na temat ciągłego monitorowania (etap monitorowania w RMF) można znaleźć w publikacji NIST SP 800-137.

[15] Więcej informacji na temat ról związanych z bezpieczeństwem można znaleźć w *NSC 7298, Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa* oraz NSC 800-37.

Senior Agency Information Security Officer (SAISO)

Senior Agency Information Security Officer, czyli kluczowa osoba w jednostce organizacyjnej odpowiedzialna za bezpieczeństwo informacji, może pełnić funkcję kierownika programu SecCM w organizacji. SAISO może również służyć swoją wiedzą specjalistyczną w ramach zespołu ds. zabezpieczeń konfiguracyjnych (CCB) lub przeprowadzając analizy wpływu na bezpieczeństwo. W organizacjach stanowisko to może być również znane pod nazwą Chief Information Security Officer (CISO).

Osoba autoryzująca (AO)

Osoba autoryzująca (*Authorizing Official – AO*) zarządza zespołem ds. zabezpieczeń konfiguracyjnych (CCB) lub uczestniczy w jego pracach w przypadku systemów, które zatwierdza, i może zapewnić personel techniczny do przeprowadzania bądź przeglądu analiz wpływu na bezpieczeństwo. Osoba autoryzująca (AO) koordynuje działania z zakresu zarządzania ryzykiem w kwestiach dotyczących SecCM i podejmuje ostateczną decyzję, czy dana zmiana lub zestaw zmian nadal mieści się w akceptowalnym ryzyku bezpieczeństwa.

Właściciel systemu

Właściciel systemu identyfikuje, definiuje i zapewnia wdrożenie tych aspektów SecCM dla systemu informacyjnego, które nie zostały zdefiniowane przez organizację, której częścią jest ten system. Właściciel systemu zapewnia również realizację wymagań SecCM na poziomie organizacyjnym dla systemu.

Menadżer programu SecCM

Menadżer programu SecCM opracowuje zasady i procedury SecCM, zapewnia kierunek działań i nadzoruje realizację programu SecCM dla organizacji bądź programu SecCM na poziomie systemu. Menadżerem programu SecCM może być kierownik zarządzający ds. bezpieczeństwa informacji (SAISO) (lub osoba wyznaczona przez SAISO lub dyrektora ds. informacji – CIO) na poziomie organizacyjnym, lub właściciel systemu (lub osoba wyznaczona przez właściciela systemu) na poziomie systemu.

System Security Officer (SSO)

Kierownik ds. bezpieczeństwa systemu (SSO) wspomaga właściciela systemu przy wdrażaniu SecCM dla systemu, prowadzi działania związane z monitorowaniem konfiguracji (raportowanie i analiza) oraz może pełnić funkcję członka zespołu ds. zabezpieczeń konfiguracyjnych (CCB).

Administrator systemu (SA)

Administrator systemu (SA) wdraża uzgodnione konfiguracje bazowe, włącza bezpieczne ustawienia konfiguracyjne produktów informatycznych, a w razie potrzeby pomaga analizować wpływu na bezpieczeństwo i monitorować konfigurację. Ponadto administrator systemu (SA) może być włączony w proces określania odpowiedniej konfiguracji bazowej dla każdego elementu konfiguracji i może pełnić funkcję w zespole ds. zabezpieczeń konfiguracyjnych (CCB). Administratorzy systemu są również odpowiedzialni za przestrzeganie polityk SecCM oraz wdrażanie/ przestrzeganie procedur SecCM.

Deweloper systemu/aplikacji

Deweloper zapewnia, że bezpieczne ustawienia konfiguracyjne są wbudowane w aplikacje zgodnie z wymaganiami bezpieczeństwa i pomaga analizować wpływ na bezpieczeństwo oraz, w razie potrzeby, prowadzić działania związane z monitorowaniem konfiguracji. Ponadto programista może być włączony w proces określania odpowiedniej konfiguracji bazowej dla odpowiedniego elementu konfiguracji i może pełnić funkcję w zespole ds. zabezpieczeń konfiguracyjnych (CCB). Programiści są również odpowiedzialni za przestrzeganie polityk SecCM oraz wdrażanie/przestrzeganie procedur SecCM.

Użytkownik systemu (SU)

Użytkownik systemu inicjuje wnioski o zmianę, pomaga w realizacji testów funkcjonalnych i zapewnia zgodność z wymogami SecCM.

3. ROZDZIAŁ TRZECI

PROCES

WDROŻENIE I STOSOWANIE ZARZĄDZANIA KONFIGURACJĄ ZORIENTOWANĄ NA BEZPIECZEŃSTWO

W niniejszym rozdziale opisano proces stosowania zarządzania konfiguracją zorientowaną na bezpieczeństwo do obsługi systemów w organizacji. Celem działań w ramach SecCM jest zarządzanie konfiguracją systemów w celu osiągnięcia odpowiedniego bezpieczeństwa i monitorowanie jej, oraz minimalizacja ryzyka organizacyjnego przy jednoczesnym wsparciu żądanej funkcjonalności i usług biznesowych.

W kolejnych rozdziałach omówiono działania, które występują w każdym z czterech etapów SecCM. Niektóre z tych działań mogą być skuteczniej wykonywane na poziomie organizacji lub misji/procesu biznesowego (tzn. stosowane do więcej niż jednego systemu informacyjnego), natomiast inne działania mogą być skuteczniej wykonywane na poziomie systemu (tzn. stosowane do pojedynczego systemu).
W każdej organizacji określa się, jakie działania są prowadzone na poziomie organizacji lub misji/procesu biznesowego, a jakie na poziomie systemu, zgodnie z wymaganiami zarządzania organizacją. Załącznik G zawiera schematy blokowe opisanych tu działań SecCM. Schematy blokowe mają służyć jako narzędzia, z których organizacje mogą korzystać przy opracowywaniu własnych procesów SecCM.

3.1 Planowanie

Opisano różne działania związane z planowaniem SecCM na poziomie organizacyjnym i systemowym.

3.1.1 Planowanie na poziomie organizacyjnym

W poniższych podrozdziałach opisano działania na etapie planowania, które są zwykle prowadzone na poziomie organizacyjnym (lub poziomie misji/procesu biznesowego). Podrozdziały są wymienione w kolejności, w jakiej zazwyczaj występują działania związane z planowaniem. Jak zawsze, organizacje mają swobodę w określaniu, które działania mają być wykonywane, na jakim poziomie i w jakiej kolejności. Planowanie

na poziomie organizacyjnym obejmuje udokumentowane w programie SecCM polityki i procedury, które wskazują kierunek działań i zapewniają wsparcie zarządzania konfiguracjami poszczególnych systemów w organizacji.

Ustanowienie programu SecCM dla całej organizacji

Praktyka SecCM zapewnienia odpowiedniego bezpieczeństwa i ułatwienia zarządzania ryzykiem jest realizowana najskuteczniej, jeśli jest wdrażana w spójny sposób w całej organizacji. Niektóre działania SecCM są bardziej skuteczne, gdy są wykonywane na poziomie organizacyjnym, z odpowiedzialnością przypisaną do programu SecCM w całej organizacji.

W przypadku organizacji o zróżnicowanej i złożonej architekturze korporacyjnej wdrożenie SecCM w sposób spójny i jednolity wymaga koordynacji zasobów w skali całej organizacji. Menadżer programu na poziomie wyższego szczebla kierowniczego, wyznaczony do prowadzenia i nadzorowania programu SecCM w całej organizacji, może zapewnić ten rodzaj koordynacji. W przypadku wielu dużych organizacji może być potrzebny dedykowany personel. W przypadku mniejszych organizacji lub tych, które mają ograniczone fundusze lub zasoby, program SecCM dla całej organizacji może być wdrażany przez pracowników wyższego szczebla zarządzania, którzy spotykają się jako grupa w celu określenia działań związanych z programem SecCM dla danej organizacji.

Menadżer programu SecCM zapewnia wiedzę i kierunek działań w postaci polityk i procedur, komunikacji, szkoleń, zdefiniowanych ról i obowiązków, wsparcia, nadzoru nad działaniami programu oraz koordynacji z zainteresowanymi stronami. Program SecCM obejmujący całą organizację świadczy również o zaangażowaniu kierownictwa w te działania. To zobowiązanie podejmowane na szczycie organizacji jest przekazywane w całym jej obszarze, aż do poszczególnych właścicieli systemów.

Menadżer programu SecCM ułatwia komunikację dotyczącą polityk SecCM, procedur, problemów itp. w ramach organizacji. Rozważa się wdrożenie konsoli lub „panelu nawigacyjnego” do zarządzania informacjami dotyczącymi bezpieczeństwa w celu przekazywania podstawowych informacji o projekcie i operacjach zainteresowanym

stronom w zrozumiałym dla nich języku. Menadżer programu SecCM rozważa również inne środki komunikacji, takie jak aktualizacje strony internetowej, wiadomości e-mail i biuletyny, aby dzielić się z zainteresowanymi stronami informacjami na temat kamieni milowych, miernikami i innymi aktualnościami związanymi z SecCM.

Główne role: Menadżer programu SecCM.

Role pomocnicze: SAISO (jeśli nie jest menadżerem programu SecCM); Chief Information Officer (CIO), Osoba autoryzująca (AO).

Oczekiwane dane wejściowe: Tolerancja ryzyka w organizacji; wymagania bezpieczeństwa w organizacji; obowiązujące prawa, regulacje, polityki itp. ustalane na wyższych szczeblach zarządzania.

Oczekiwane wyniki: Funkcjonalny program SecCM dla całej organizacji.

Opracowanie polityki SecCM w organizacji

Organizacja jest zazwyczaj odpowiedzialna za zdefiniowanie udokumentowanych polityk dla programu SecCM. Menadżer programu SecCM opracowuje, upowszechnia oraz dokonuje okresowych przeglądów i aktualizacji polityk SecCM dla organizacji. Polityki te są zawarte w ogólnej polityce bezpieczeństwa całej organizacji. Polityka SecCM obejmuje zwykle:

- Cel – cel lub cele ustanowienia polityki SecCM dla całej organizacji.
- Zakres – zakres architektury przedsiębiorstwa, do którego odnosi się polityka.
- Role – role, które są istotne w kontekście polityki.
- Odpowiedzialność – obowiązki dotyczące każdej zdefiniowanej roli.
- Działania – funkcje, które są wykonywane, aby osiągnąć cele polityki.
- Typowe bezpieczne konfiguracje – krajowe bądź ogólnoorganizacyjne znormalizowane wzorce ustawień konfiguracyjnych wraz ze sposobem postępowania w przypadku odstępstw.
- Zapisy – zapisy działań w ramach zarządzania konfiguracją, które mają być zachowane; informacje, które mają znajdować się w każdym rodzaju zapisu; kto

jest odpowiedzialny za utworzenie/przechowywanie zapisów; oraz procedury ochrony, dostępu, audytu i ostatecznie usuwania takich zapisów.

Polityka SecCM może również dotyczyć następujących tematów:

- wymagania dotyczące szkoleń z zakresu SecCM,
- wykorzystanie szablonów SecCM,
- wykorzystanie narzędzi automatycznych,
- zabronione ustawienia konfiguracyjne,
- wymagania dotyczące inwentaryzacji systemów i komponentów.

Polityka SecCM podkreśla zaangażowanie kierownictwa, wyjaśnia wymagany poziom koordynacji pomiędzy jednostkami organizacyjnymi oraz określa podejście do monitorowania konfiguracji.

Główne role: Menadżer programu SecCM.

Role pomocnicze: SAISO (jeśli nie jest menadżerem programu SecCM); Chief Information Officer (CIO); Osoba autoryzująca (AO).

Oczekiwane dane wejściowe: Akceptowane ryzyka w organizacji; wymagania bezpieczeństwa w organizacji; obowiązujące prawa, regulacje, polityki itp. ustalane na wyższych szczeblach zarządzania. Oczekiwane wyniki: Udokumentowane polityki SecCM

Opracowanie organizacyjnych procedur SecCM

Organizacja zazwyczaj ustanawia i utrzymuje wspólne procedury w zakresie działań związanych z zarządzaniem konfiguracją zorientowaną na bezpieczeństwo; jednak niektóre procedury SecCM mogą wymagać opracowania na poziomie systemu. Organizacje mogą również zapewniać procedury hybrydowe. W takim przypadku organizacja ustanawia procedury, które zawierają parametry do zdefiniowania na poziomie systemu. W każdym przypadku procedury są udokumentowane i rozpowszechniane wśród odpowiedniego personelu oraz zgodnie z polityką organizacji. Procedury SecCM dotyczą, w stosownych przypadkach, następujących kwestii:

Szablony – szablony związane z SecCM, które integrują politykę i procedury SecCM w całej organizacji oraz pozwalają poszczególnym właścicielom systemów na wypełnienie informacji specyficznych dla ich systemu. Szablony mogą być opracowane dla planu SecCM, procedur specyficznych dla systemu, wniosków o zmianę, analiz wpływu na bezpieczeństwo, raportów dotyczących SecCM itp. Można również opracować szablony, które będą miały zastosowanie w szczególności do systemów o małym, umiarkowanym lub dużym wpływie na bezpieczeństwo[16]. Przykładowe wzory znajdują się w załącznikach D i E.

Wykaz komponentów – opisuje, w jaki sposób komponenty mają być zarządzane w ramach inwentaryzacji (np. w jaki sposób nowe komponenty są dodawane do wykazu, jakie informacje o każdym komponencie są śledzone oraz w jaki sposób dokonywane są aktualizacje, w tym usuwanie komponentów wycofanych). Jeśli należy zastosować zautomatyzowane narzędzia, trzeba opisać następujące czynniki: jak często będą uruchamiane, kto będzie nimi zarządzał, kto będzie miał dostęp do nich i jak będą kontrolowane.

Konfiguracja bazowa – określa kroki tworzenia konfiguracji bazowej, jej zawartość, zatwierdzenie wstępnej konfiguracji bazowej, utrzymanie konfiguracji bazowej (tj. kiedy powinna być aktualizowana i przez kogo) oraz jej kontrolę. W stosownych przypadkach wymagania pochodzące od organów regulacyjnych są uwzględniane i integrowane podczas definiowania konfiguracji bazowej.

Typowe bezpieczne konfiguracje – określają powszechnie uznane i znormalizowane bezpieczne konfiguracje, które mają zastosowanie do elementów konfiguracji. Typowe konfiguracje bazowe określone w procedurze pochodzą z ustalonych specyfikacji regulacyjnych, organizacyjnych lub branżowych (np. National Checklist Program zawiera odniesienia do typowych konfiguracji bazowych, takich jak: United States Government Configuration Baseline (USGCB), Defense Information System Agency (DISA) Security Technical Implementation Guides (STIGs), Center for Internet

[16] Systemy informacyjne skategoryzowane zgodnie z [NSC 199] oraz poziom wpływu na bezpieczeństwo, wynikający z kategoryzacji zgodnie z [NSC200].

Security (CIS) Benchmarks itp.). Tam, gdzie to możliwe, typowe bezpieczne konfiguracje wykorzystują treści zawarte w SCAP. Uwzględnia się również odstępstwa od typowych bezpiecznych konfiguracji (np. identyfikacja dopuszczalnych metod oceny, zatwierdzania, dokumentowania i uzasadniania odstępstw od typowych bezpiecznych konfiguracji wraz z identyfikacją kontroli wdrożonych w celu zmniejszenia ryzyka związanego z odstępstwami), w przypadku gdy konfiguracja danego systemu musi odbiegać od zdefiniowanej ze względu na wymagania misji lub inne ograniczenia.

Zarządzanie poprawkami – określa sposób, w jaki proces zarządzania poprawkami w organizacji jest zintegrowany z SecCM, jak poprawki są priorytetyzowane i zatwierdzane przez proces kontroli zmian konfiguracji oraz testowane pod kątem ich wpływu na istniejące bezpieczne konfiguracje. Ponadto określa sposób, w jaki poprawki są integrowane z aktualizacjami zatwierdzonych konfiguracji bazowych oraz jak jest kontrolowane wdrażanie poprawek (kontrole dostępu itp.).

Kontrola zmian konfiguracji – określa kroki, które należy podjąć w celu przeniesienia zmiany w konfiguracji z początkowego etapu do ostatecznej wersji w środowisku produkcyjnym. Zakres procedur obejmuje między innymi:

- Procedury żądania i zatwierdzania zmian.
- Kryteria określające rodzaje zmian, które są wstępnie zatwierdzone lub zwolnione z kontroli konfiguracji, takie jak poprawki bezpieczeństwa dostarczone przez dostawcę, zaktualizowane sygnatury antywirusowe, tworzenie lub usuwanie użytkowników, wymiana uszkodzonych urządzeń peryferyjnych, płyty głównej lub dysków twardych itp.[17].
- Procedury analizy wpływu na bezpieczeństwo, w tym poziom dokładności, z jakim mają być dokumentowane wyniki analizy, oraz wymagania dotyczące przeglądu powdrożeniowego w celu potwierdzenia, że zmiana została wdrożona zgodnie z zatwierdzeniem i że nie spowodowała dodatkowego wpływu na bezpieczeństwo.

[17] Wstępnie zatwierdzone zmiany są nadal testowane i dokumentowane przed wdrożeniem.

- Kryteria pozwalające określić, czy zmiana jest na tyle istotna, aby spowodować rozważenie działań związanych z ponowną autoryzacją systemu.
- Przegląd pod kątem spójności z organizacyjną architekturą korporacyjną.
- Utworzenie grupy, która zatwierdza zmiany (np. zespołu ds. zabezpieczeń konfiguracyjnych).
- Wymagania dotyczące testowania zmian w celu przedłożenia ich zespołowi ds. zabezpieczeń konfiguracyjnych (tj. format i rodzaje informacji, które należy przedstawić, takie jak plan testów, harmonogram i wyniki testów).
- Jeżeli dopuszczalne jest zatwierdzanie zmian na poziomie systemu, to należy podać kryteria, na podstawie których wniosek o zmianę może zostać przeniesiony z poziomu systemu na poziom organizacji (np. zmiana będzie miała wpływ na inne systemy organizacji, będzie wymagała przestoju systemu, który może mieć negatywny wpływ na misję itp.).
- Wymagania dotyczące testowania zmian przed dopuszczeniem do środowiska operacyjnego.
- Wymagania dotyczące ograniczeń dostępu do zmian (tj. kto i w jakich okolicznościach może dokonywać zmian w systemie informacyjnym).
- Wymagania dotyczące wycofania zmian w przypadku wystąpienia problemów.
- Wymagania dotyczące zarządzania nieplanowanymi zmianami (np. zmianami koniecznymi do usunięcia błędów krytycznych), które są dostosowane do obsługi przyspieszonych przeglądów i zatwierdzeń.
- Wymagania dotyczące wstecznej analizy, testowania i zatwierdzania zmian, które są wdrażane poza procesem kontroli zmian.

Procedury helpdesk – opisują, w jaki sposób wnioski o zmianę przechodzące przez helpdesk są rejestrowane, zgłaszane, śledzone i włączane do procesu kontroli zmian konfiguracji.

Procedury związane z cyklem życia systemu (SDLC) – opisują, w jaki sposób SecCM jest wykorzystywany do zarządzania i kontroli konfiguracji i zmian w systemie w ramach procesu SDLC zdefiniowanego w organizacji i w całym cyklu życia systemu.

Monitorowanie – opisuje, w jaki sposób działania monitorujące i związane z nimi raporty są stosowane do oceny bezpiecznego stanu systemu oraz jak identyfikować stan, kiedy rzeczywista konfiguracja różni się od zatwierdzonej konfiguracji bazowej (czy wystąpiła nieautoryzowana zmiana) w ramach systemu przez analizę działań monitorujących i raportujących.
Procedury biblioteki nośników – opisują zarządzanie biblioteką nośników, w tym konwencje nazewnictwa dla nośników, procedury etykietowania (nazwa/wersja, data utworzenia, okres przechowywania, właściciel, data zniszczenia, poziom wpływu lub klasyfikacji), śledzenie nośników, kontrole dostępu, zabezpieczenia integralności (np. sumy kontrolne), kontrole zapasów, planowanie pojemności i archiwizację.

Główne role: Menadżer programu SecCM; Właściciele systemów (SO). Uwaga: Menadżerowie programu SecCM i właściciele systemów są odpowiedzialni za określenie, które procedury są wymagane na ich poziomach odpowiedzialności oraz sposobu ich udokumentowania (np. w formie kilku oddzielnych procedur, pojedynczej procedury lub części planu SecCM).

Role pomocnicze: SAISO (jeśli nie jest menadżerem programu SecCM); System Security Officer (SSO); Administrator systemu (SA); Użytkownik systemu (SU).

Oczekiwane dane wejściowe: Tolerancja ryzyka w organizacji w ramach polityki organizacji; organizacyjne wymagania bezpieczeństwa; obowiązujące prawa, regulacje, polityki itp. ustalone na wyższych szczeblach zarządzania. Oczekiwane wyniki: Udokumentowane procedury SecCM.

Opracowanie strategii monitorowania SecCM

Monitorowanie SecCM weryfikuje, czy proces SecCM jest skuteczny w zakresie utrzymania stanu bezpieczeństwa organizacji oraz konfiguracji bazowych i polityki SecCM. Strategia monitorowania SecCM jest oparta na tolerancji ryzyka i wymaganiach bezpieczeństwa dla organizacji. Strategia monitorowania SecCM jest spójna z ogólną strategią ciągłego monitorowania organizacji i stanowi jej część. Organizacja zazwyczaj opracowuje strategię monitorowania SecCM; jednak ma swobodę w opracowywaniu części lub całości strategii monitorowania SecCM na poziomie misji/procesu biznesowego lub systemu.

W ramach strategii ustala się harmonogram monitorowania SecCM i związanej z tym sprawozdawczości. W strategii uwzględniono oceny zaplanowane i doraźne. Harmonogram monitorowania może być zgodny z planowanymi wersjami, dzięki czemu oceny są przeprowadzane przed i po wdrożeniu. Można również przeprowadzać oceny doraźne, aby nie występowały zaniedbania pomiędzy planowanymi ocenami. Dodatkowo harmonogram zawiera postanowienia dotyczące przeglądu i rewizji strategii monitorowania SecCM w celu zapewnienia, że strategia ta nadal spełnia wymagania bezpieczeństwa w organizacji.

Więcej informacji na temat monitorowania SecCM można znaleźć w podrozdziale 3.4.

Główne role: Menadżer programu SecCM.

Role pomocnicze: SAISO lub osoba na zbliżonym stanowisku (jeśli nie jest menadżerem programu SecCM); Właściciel systemu (SO); System Security Officer (SSO).

Oczekiwane dane wejściowe: Polityka i procedury SecCM, ogólna polityka i procedury ciągłego monitorowania organizacji; tolerancja ryzyka w organizacji; wymagania bezpieczeństwa organizacji.

Oczekiwane wyniki: Strategia i harmonogram monitorowania i raportowania dotyczącego konfiguracji.

Określenie typów zmian, które nie wymagają kontroli zmian konfiguracji

W ramach zarządzania zasobami organizacja może chcieć wyznaczyć typy zmian, które są wstępnie zatwierdzone (tj. zmiany, które nie są wysyłane do zespołu CCB w celu zatwierdzenia)[15] oraz zmiany, które zazwyczaj nie są objęte kontrolą konfiguracji (tj. zmiany, które są całkowicie wyłączone z SecCM). Dostarczone przez dostawcę poprawki bezpieczeństwa, zaktualizowane sygnatury antywirusowe oraz wymiana uszkodzonych urządzeń peryferyjnych lub sprzętu wewnętrznego to przykłady zmian, które mogą być wstępnie zatwierdzone. Aktualizacje zawartości bazy danych, tworzenie/ usuwanie/ aktualizacja kont oraz tworzenie lub usuwanie plików użytkowników to przykłady zmian, które są zazwyczaj wyłączone z kontroli zmian konfiguracji.

Główne role: Menadżer programu SecCM; Właściciel systemu (SO).

Role pomocnicze: SAISO (jeśli nie jest menadżerem programu SecCM); osoba autoryzująca (AO); System Security Officer (SSO); administrator systemu (SA); deweloperzy systemu/aplikacji.

Oczekiwane dane wejściowe: Zasady i procedury SecCM; rodzaje zmian, które zazwyczaj występują w organizacji bądź systemie.

Oczekiwane wyniki: Zapis rodzajów zmian, które są wyłączone z kontroli konfiguracji; zapis rodzajów zmian, które podlegają kontroli konfiguracji.

Opracowanie strategii szkoleń SecCM

SecCM jest fundamentalną częścią programu bezpieczeństwa organizacji, ale często wymaga zmiany kultury organizacyjnej. Szkolenie personelu zapewni przekazanie wiedzy na temat zasad i procedur SecCM. Na szkoleniu kierownictwo może również przedstawić argumenty zapewniające, że SecCM jest ważny. Opracowane materiały szkoleniowe SecCM obejmują polityki organizacji, procedury, narzędzia, artefakty i wymagania dotyczące monitorowania. Szkolenie może być obowiązkowe lub opcjonalne, w zależności od potrzeb i jest skierowane do odpowiedniego personelu (np. administratorów systemu, programistów systemu/oprogramowania, menadżerów ds. bezpieczeństwa systemu, właścicieli systemu itp.) w celu zapewnienia, że personel ma umiejętności zarządzania konfiguracjami bazowymi zgodnie z polityką organizacyjną.

Główne role: Menadżer programu SecCM; Właściciel systemu (SO)

Role pomocnicze: SAISO (jeśli nie jest menadżerem programu SecCM); Chief Information Officer (CIO), Osoba autoryzująca (AO), System Security Officer (SSO)

Oczekiwane dane wejściowe: Zasady i procedury SecCM.

Oczekiwane wyniki: Materiały szkoleniowe bądź kursy zaplanowane w razie potrzeby.

Identyfikacja zatwierdzonych produktów IT

Wiele organizacji tworzy listę zatwierdzonego sprzętu i oprogramowania (np. białą listę oprogramowania) do użytku w całej organizacji. Właściciele systemu wybierają produkty z zatwierdzonej listy i używają ich bez konieczności wyraźnego

zatwierdzenia. W zależności od polityki organizacji, dodatkowe produkty wymagane do danego systemu mogą wymagać zatwierdzenia przez zespół CCB dla tego systemu; używany produkt może również wymagać dodania do listy kontrolowanych i zatwierdzonych produktów IT obowiązującej w organizacji. Niektóre organizacje mogą również zapewniać usługę zakupów lub podobny mechanizm zakupów/ kontraktowania, zgodnie z którymi mogą być kupowane wstępnie zatwierdzone lub wymagane do zakupienia produkty.

Główne role: Menadżer programu SecCM bądź zespół ds. zabezpieczeń konfiguracyjnych; właściciel systemu.

Role pomocnicze: SAISO (jeśli nie jest menadżerem programu SecCM); Osoba autoryzująca (AO); System Security Officer (SSO).

Oczekiwane dane wejściowe: Zasady i procedury SecCM; organizacyjne wymogi bezpieczeństwa; informacje o usłudze nabycia/zakupu.

Oczekiwane wyniki: Lista produktów IT zatwierdzonych dla organizacji.

Narzędzia do identyfikacji

Zarządzanie niezliczonymi konfiguracjami znajdującymi się w komponentach systemu stało się niemal niemożliwym zadaniem przy użyciu ręcznych metod, takich jak arkusze kalkulacyjne. Jeśli to możliwe, organizacje szukają zautomatyzowanych rozwiązań, które w dłuższej perspektywie mogą obniżyć koszty oraz zwiększyć wydajność i niezawodność działań SecCM.

W większości przypadków narzędzia wspomagające działania na drugim, trzecim i czwartym etapie SecCM są wybierane do użycia w całej organizacji przez kierownictwo programu SecCM, a właściciele systemów są odpowiedzialni za zastosowanie narzędzi do działań SecCM wykonywanych w każdym systemie. Podobnie organizacja może dostarczyć właścicielom systemów narzędzia i mechanizmy do raportowania i zarządzania zasobami. Zgodnie z polityką organizacji, jeśli są używane narzędzia zautomatyzowane, muszą być zatwierdzone przez automatyczny protokół zabezpieczeń zawartości (*Security Content Automation Protocol – SCAP*) w zakresie, w jakim są dostępne. Protokół SCAP został szczegółowo opisany w podrozdziale 3.5.

Jeśli nie są dostarczane przez organizację, identyfikuje się i wdraża narzędzia wspierające program SecCM na poziomie systemu. Jeśli to możliwe, istniejące narzędzia SecCM pochodzące z organizacji są wykorzystywane do wspomagania spójnych praktyk SecCM w całej organizacji, scentralizowanego raportowania i efektywności kosztowej. Wykorzystanie istniejących narzędzi może wymagać ich zainstalowania i skonfigurowania do działania w poszczególnych systemach. Instalacja i konfiguracja narzędzia wymagają zwykle założenia kont, zidentyfikowania administratorów, określenia harmonogramów, ustawienia odpowiednich konfiguracji bazowych i ewentualnie instalacji klienta na każdym komponencie, który ma być kontrolowany w ramach konfiguracji. Jeśli narzędzie zostało już wdrożone w organizacji, instrukcje dotyczące instalacji, konfiguracji i wdrożenia są dostępne lub w razie potrzeby łatwe do opracowania.

Istnieje wiele różnych narzędzi do zarządzania konfiguracją, dostępnych w celu wspomagania programu SecCM w organizacji. Jako niezbędne minimum, organizacja uwzględnia narzędzia, które mogą automatycznie ocenić ustawienia konfiguracji komponentów systemu. W najszerszym możliwym zakresie należy wybrać zautomatyzowane narzędzia, które mogą skanować różne komponenty systemu (np. serwer WWW, serwer bazy danych, urządzenia sieciowe itp.), pracujące w różnych systemach operacyjnych, identyfikować bieżące ustawienia konfiguracyjne i wskazywać miejsca, w których bieżące ustawienia są niezgodne z polityką. Zautomatyzowane narzędzia do zarządzania konfiguracją importują ustawienia z jednej lub wielu typowych bezpiecznych konfiguracji, a następnie umożliwiają dostosowanie konfiguracji do wymagań organizacji w zakresie bezpieczeństwa i misji/funkcjonalności.

Narzędzia, które wdrażają bądź oceniają ustawienia konfiguracyjne, są oceniane w celu określenia, czy spełniają następujące wymagania:

- umiejętność uzyskiwania informacji z różnych źródeł (różne typy komponentów, różne systemy operacyjne, różne platformy itp.);
- wykorzystanie znormalizowanych specyfikacji, takich jak Extensible Markup Language (XML) i SCAP;

- integracja z innymi produktami, takimi jak stanowiska pomocy, rozwiązania do zarządzania inwentaryzacją i reagowania na incydenty;
- wsparcie zapewnione przez dostawcę (poprawki, uaktualnione sygnatury podatności na zagrożenia itp.);
- zgodność z obowiązującymi przepisami rozporządzeniami wykonawczymi, dyrektywami, rekomendacjami, politykami, normami i wytycznymi oraz powiązanie podatności na zagrożenia z zabezpieczeniami [NSC 800-53];
- znormalizowane możliwości raportowania (np. SCAP, XML), w tym możliwość dostosowywania danych wyjściowych i wykonywania analiz;
- konsolidacja danych w narzędziach do zarządzania informacjami i zdarzeniami bezpieczeństwa (*ang. Security Information and Event Management - SIEM*) oraz produktach typu dashboard.

Organizacje mogą rozważyć wdrożenie rozwiązania typu „wszystko w jednym" do zarządzania konfiguracją. Na przykład różne funkcje zarządzania konfiguracją są zawarte w produktach do zarządzania serwerami, stacjami roboczymi, pulpitami i usługami świadczonymi przez aplikacje. Produkty mogą zawierać takie funkcje jak:

- inwentaryzacja/wykrywanie komponentów systemu;
- dystrybucja oprogramowania;
- zarządzanie poprawkami;
- wdrożenie systemu operacyjnego;
- zarządzanie politykami;
- migracja do nowej konfiguracji bazowej;
- kopia zapasowa / odzyskiwanie danych.

Główne role: Menadżer programu SecCM bądź zespół ds. zabezpieczeń konfiguracyjnych, właściciel systemu (SO).

Role pomocnicze: SAISO (jeśli nie jest menadżerem programu SecCM); CIO; Osoba autoryzująca (AO), System Security Officer (SSO); Administrator systemu (SA).

Oczekiwane dane wejściowe: polityka i procedury SecCM; organizacyjne i systemowe wymogi bezpieczeństwa; informacje o usłudze nabycia/zakupu.

Oczekiwane wyniki: Narzędzia do wdrożenia w celu wsparcia programu SecCM.

Ustanowienie środowiska i programu do testowania konfiguracji

Niektóre organizacje mogą chcieć utworzyć i utrzymywać środowisko testowania konfiguracji oraz program testowania produktów informatycznych, narzędzi oraz proponowanych zmian w centralnie zarządzanym środowisku odizolowanym od środowiska produkcyjnego. Środowisko testowe jest wykorzystywane do różnego rodzaju testów, które obejmują:

- produkty informatyczne proponowane do zatwierdzenia i wykorzystania w organizacji;
- ustawienia konfiguracyjne dla zatwierdzonych produktów informatycznych;
- wydawane przez dostawców poprawki przed ich wprowadzeniem do organizacji;
- walidacja narzędzi, które wykrywają niezatwierdzone ustawienia konfiguracyjne;
- weryfikacja procesów testowania w celu sprawdzenia poprawności zatwierdzonych ustawień konfiguracyjnych;
- analizy wpływu na bezpieczeństwo;
- inne zmiany związane z konfiguracją.

Publikacja NIST [SP 800-115], *Technical Guide to Information Security Testing and Assessment*, zawiera wytyczne dotyczące tego, jak ustanowić i przeprowadzić skuteczny program testów funkcjonalnych bezpieczeństwa informacji. Zawiera szczegółowe wytyczne dotyczące przeglądu konfiguracji systemu i skanowania podatności, które mogą być bezpośrednio zastosowane do programu testowania konfiguracji[18].

[18] Podano jako przykład.

Główne role: Menadżer programu SecCM; Właściciel systemu (SO)

Role pomocnicze: SAISO (jeśli nie jest menadżerem programu SecCM); CIO; Osoba autoryzująca (AO); System Security Officer (SSO); Administrator systemu (SA)

Oczekiwane dane wejściowe: Zasady i procedury SecCM

Oczekiwane wyniki: Odizolowane środowisko testowe i program wspierający SecCM

3.1.2 Planowanie na poziomie systemu

W poniższych podrozdziałach opisano działania na etapie *planowania*, które są zwykle prowadzone na poziomie systemu. Podrozdziały są wymienione w kolejności, w jakiej zwykle realizowane są działania związane z planowaniem. Organizacje mają pełną swobodę w określaniu, które działania mają być wykonywane na poziomie organizacji, a które na poziomie systemu, a także ich kolejności. Etap planowania na poziomie systemu skutkuje kompletnym planem SecCM, powołaniem zespołu ds. zabezpieczeń konfiguracyjnych, dokładnym wykazem komponentów systemu oraz zdefiniowanymi elementami konfiguracji systemu.

Opracowanie planu SecCM dla systemu informacyjnego

Podstawowym celem planu SecCM jest udokumentowanie lub dostarczenie odniesień do specyficznych dla systemu informacji związanych z SecCM. Organizacja może zdefiniować główny plan SecCM i dostarczyć szablony, które wymagają udokumentowania podzbioru planu SecCM dla każdego systemu, lub właściciel systemu może być zobowiązany do zdefiniowania planu SecCM dla systemu jako całości. Niezależnie od formatu, plan SecCM jest uzupełniany na poziomie systemu i zazwyczaj obejmuje następujące kwestie:

- krótki opis systemu;
- wykaz komponentów systemu;
- elementy konfiguracji systemu;
- zasady, które należy zastosować do zarządzania zmianami w elementach konfiguracji (np. w oparciu o poziom wpływu na system[19]);

[19] Systemy sklasyfikowane zgodnie z [NSC 199] i [NSC 200].

- określenie ról i obowiązków;
- określenie i utworzenie grupy lub wskazanie osoby (osób), które rozpatrują wnioski o zmiany;
- procedury kontroli zmian konfiguracji, które mają być przestrzegane (w tym odniesienia do procedur obowiązujących w całej organizacji);
- określenie lokalizacji (np. biblioteki nośników), w której utrzymywane są artefakty SecCM (wnioski o zmianę, zatwierdzenia itp.);
- kontrole dostępu stosowane do kontroli zmian konfiguracji;
- kontrole dostępu w celu ochrony artefaktów SecCM, zapisów, raportów itp. (np. współmiernie do poziomu wpływu na system);
- wykorzystywane narzędzia SecCM;
- identyfikacja typowych bezpiecznych konfiguracji (np. USGCB, DISA STIGs, National Checklist Program itp.), które mają być wykorzystane jako podstawa do ustanowienia zatwierdzonych konfiguracji bazowych dla systemu;
- odstępstwa od typowych bezpiecznych konfiguracji dla elementów konfiguracji wraz z uzasadnieniem;
- kryteria zatwierdzania konfiguracji bazowych dla systemu;
- obsługa wyjątków od planu SecCM (np. lokalizacja artefaktów SecCM, procedury kontroli zmian konfiguracji itp.).

Plan SecCM może mieć różne reprezentacje; może to być rzeczywisty dokument, zbiór danych przechowywanych w ramach narzędzia SecCM lub dowolna inna forma. Procedury SecCM mogą być ujęte oddzielnie lub zawarte w planie SecCM. Plan SecCM można utworzyć również na poziomie systemu, korzystając z szablonów organizacyjnych. Poziom szczegółowości planu SecCM zależy od poziomu wpływu na systemu.

Etap SDLC: Rozpoczęcie na etapie inicjowania, doprecyzowanie na etapie opracowania /pozyskania, zakończenie na etapie wdrożenia/oceny.

Główne role: Właściciel systemu (SO).

Role pomocnicze: System Security Officer (SSO); Administrator systemu (SA); Deweloper systemu/aplikacji; użytkownik systemu (SU).

Oczekiwane dane wejściowe: Polityki, procedury i szablony SecCM na poziomie organizacji.

Oczekiwane wyniki: Plan SecCM, w tym procedury na poziomie systemu.

Tworzenie lub aktualizacja wykazu komponentów systemu

Komponent systemu to odrębny, możliwy do zidentyfikowania składnik aktywów informatycznych, będący elementem składowym systemu. Dokładna inwentaryzacja komponentów jest niezbędna, aby zarejestrować komponenty, które składają się na system. Wykaz komponentów pomaga zwiększyć bezpieczeństwo systemu przez zapewnienie kompleksowego obrazu komponentów, które muszą być zarządzane i zabezpieczone. Wszystkie komponenty systemu są śledzone od momentu nabycia do wycofania z użytkowania w ramach procesu SDLC organizacji.

Wykaz komponentów systemu można przedstawić jako:

Wykaz komponentów systemu = {SC[20]1, SC2, ... SCn},

gdzie: *n* jest większe lub równe jeden, a SC reprezentuje komponent systemu w organizacji.

Każdy komponent w organizacji jest objęty uprawnieniami tylko jednego systemu oraz jest śledzony i udokumentowany w wykazie, który odzwierciedla powiązanie z systemem, w ramach którego jest zarządzany (tj. komponent powiązany z systemem jest uwzględniony w wykazie komponentów tego systemu). Komponent może obsługiwać systemy z różnych zakresów uprawnień (takie jak serwer obsługujący kilka aplikacji internetowych lub maszyn wirtualnych); jednak właściciele wspieranych systemów nie mają ani uprawnień, ani nie ponoszą odpowiedzialności za taki komponent, a zatem nie jest on uwzględniony w wykazach komponentów obsługiwanych systemów.

Wykaz komponentów jest uzupełniany podczas procesu wykrywania. Wykrywanie, które może być ręczne lub zautomatyzowane, to proces pozyskiwania informacji

[20] Komponent systemu (*ang. System Component – SC*).

o komponentach, które tworzą systemy w organizacji. Organizacja zazwyczaj określa rodzaje i szczegółowość komponentów (urządzenia peryferyjne oraz stacje robocze, routery itp.), które mają być identyfikowane w ramach inwentaryzacji. W większości organizacji ręczne zbieranie tych informacji w celu włączenia ich do inwentaryzacji lub analizy w stosunku do autoryzowanej inwentaryzacji jest niepraktyczne. Stosowanie zautomatyzowanych narzędzi do wyszukiwania, analizy i zarządzania wykazami komponentów jest na ogół bardziej efektywnym i skutecznym sposobem prowadzenia takich wykazów. Należy jednak zauważyć, że nawet przy zastosowaniu zautomatyzowanych narzędzi do zarządzania inwentaryzacją, nadal może być konieczne ręczne wprowadzanie do niej niektórych elementów danych. Przykłady takich danych to m.in. identyfikatory unikalne w organizacji, powiązanie z systemem (w zależności od konfiguracji sieci – czy instalacja narzędzia do zarządzania inwentaryzacją odbywa się na poziomie organizacyjnym czy systemowym itp.), właściciela, administratora lub użytkownika systemu/komponentu, powiązanie z elementem konfiguracji lub typem komponentu. Narzędzia wspomagające zarządzanie inwentaryzacją to zazwyczaj aplikacje oparte na bazie danych, służące do śledzenia komponentów systemu w danym środowisku i zarządzania nimi. Po utworzeniu wykazu często stosuje się zautomatyzowane narzędzia do wykrywania, usuwania lub dodawania komponentów. Niektóre narzędzia do zarządzania inwentaryzacją umożliwiają rozszerzone monitorowanie komponentów przez wykorzystanie wbudowanego podprogramu, który przechwytuje pewne wywołanie w systemie operacyjnym i przekierowuje je do innej ścieżki programu; instalację agentów na każdym komponencie; lub zastosowanie API. Dzięki tej funkcjonalności system zarządzania inwentaryzacją może monitorować zmiany w konfiguracji komponentu i raportować wyniki określonym pracownikom.

Narzędzia do zarządzania inwentaryzacją są walidowane przez SCAP w zakresie, w jakim są dostępne. Przy zakupie aplikacji – standardowej (COTS) lub niestandardowej – do zarządzania inwentaryzacją, organizacje powinny uwzględnić wymagania SCAP w zapytaniach ofertowych, umowach zakupu, kontraktach itp. Określenie komponentów za pomocą powszechnie rozpoznawanego identyfikatora,

takiego jak Common Platform Enumeration (CPE), może ułatwić wymianę danych pomiędzy narzędziami zgodnymi ze SCAP[21]. Stosowanie powszechnie uznawanych identyfikatorów od początku procesu nabywania zapewnia wspólne nazewnictwo w wykazie komponentów w celu ich śledzenia w całym SDLC (tj. od nabycia do wycofania z eksploatacji).

Wykaz komponentów systemu dodaje rzeczywistą wartość do SecCM, gdy każda pozycja na wykazie jest związana z informacjami, które mogą być wykorzystane do określenia zatwierdzonych konfiguracji bazowych, kontroli zmian konfiguracji, analizy wpływu na bezpieczeństwo oraz monitorowania i raportowania. Niektóre elementy danych[22], zwykle przechowywane dla każdego komponentu w wykazie komponentów systemu, obejmują:

- unikalny identyfikator bądź numer seryjny;
- system, którego częścią jest dany komponent[23];
- typ komponentu (np. serwer, komputer stacjonarny, aplikacja);
- informacje o producencie/modelu;
- typ i wersja systemu operacyjnego/ Service Pack Level (najlepiej przy użyciu odpowiedniej nazwy w schemacie Common Platform Enumeration);
- obecność maszyn wirtualnych[24];

[21] Więcej informacji na temat automatycznego protokołu zabezpieczeń zawartości (SCAP) można znaleźć w podrozdziale 3.5.

[22] Patrz [NISTIR 7693], aby uzyskać informacje na temat specyfikacji elementów danych.

[23] Pojedynczy element systemu może obsługiwać dodatkowe systemy informacyjne. Na przykład, serwer w farmie serwerów może hostować kilka maszyn wirtualnych, a każda maszyna wirtualna z kolei może obsługiwać aplikację internetową. Gdy dla takiego serwera nastąpi przerwanie świadczenia usług lub naruszenie bezpieczeństwa, informacje przechowywane w wykazie komponentów, dotyczące zastosowań tego serwera, mogą pomóc w szybkiej identyfikacji aplikacji dotkniętych tym problemem i podjęciu odpowiednich działań. Dodatkowo maszyny wirtualne są uwzględniane jako osobne pozycje w wykazach komponentów systemu i podlegają kontroli konfiguracji. Identyfikacja maszyn wirtualnych i włączenie ich do procesu zarządzania konfiguracją jest ważne w ogólnym zarządzaniu ryzykiem organizacyjnym i bezpieczeństwem na poziomie systemu.

[24] Tamże.

- wersja aplikacji/ informacje o licencji (najlepiej przy użyciu odpowiedniej nazwy w schemacie Common Platform Enumeration);
- fizyczna lokalizacja (np. numer budynku/pokoju);
- logiczna lokalizacja (np. adres IP);
- adres MAC;
- właściciel;
- status operacyjny;
- administratorzy główni i pomocniczy;
- użytkownik główny (jeśli dotyczy).

Niektóre dodatkowe elementy danych mogą być również rejestrowane w celu ułatwienia działań w ramach SecCM:

- status komponentu (np. sprawny, zapasowy, usunięty itp.);
- powiązania z innymi elementami systemu w wykazie[25]
- powiązania z innymi systemami/ zależności od nich[26];
- inne systemy obsługiwane przez ten komponent[27];
- identyfikacja wszelkich umów o poziomie usług (SLA), które dotyczą danego komponentu;
- najczęściej stosowane bezpieczne konfiguracje;
- element konfiguracji (CI), którego komponent jest częścią;
- punkty kontrolne obsługiwane przez ten komponent;
- identyfikacja wszelkich dzienników zdarzeń, które dotyczą danego komponentu.

[25] Tamże.

[26] Tamże.

[27] Tamże.

Etap SDLC: Rozpoczęcie na etapie opracowania/pozyskania, zakończenie na etapie wdrożenia/oceny, bieżące aktualizacje na etapie eksploatacji i konserwacji

Główne role: Właściciel systemu (SO)

Role pomocnicze: System Security Officer (SSO); Administrator systemu (SA), Użytkownik systemu (SU).

Oczekiwane dane wejściowe: Narzędzia na poziomie organizacji bądź systemu, polityka i procedury na poziomie organizacji bądź systemu

Oczekiwane wyniki: Dokładny spis elementów systemu

Określanie elementów konfiguracji

Podczas wdrażania zarządzania konfiguracją właściciel systemu określa, jak najlepiej zdekomponować system na jeden lub więcej elementów konfiguracji (*ang. configuration item - CI*). Elementy konfiguracji mogą być pojedynczym komponentem, dokumentem, schematem sieciowym, skryptem, niestandardowym kodem źródłowym lub innym elementem systemu, który wymaga zarządzania konfiguracją, lub grupą takich komponentów.

System może być reprezentowany jako zbiór jednego lub większej liczby elementów konfiguracji (CI)w następujący sposób:

System = {CI1, CI2, .CIn}, gdzie n jest większe lub równe 1.

Pomiędzy systemami a elementem konfiguracji istnieje relacja jeden do wielu. Każdy system składa się z jednego lub większej liczby elementów konfiguracji, a każdy element konfiguracji jest częścią tylko jednego systemu. W przypadkach, gdy organizacja ustanawia i utrzymuje typowe konfiguracje bazowe dla danej platformy (np. Windows wersja X, Linux wersja Y) lub typu komponentu (np. stacja robocza, serwer, router), każdy indywidualny system dziedziczy wspólną konfigurację bazową jako element konfiguracji lub jego części dla tego systemu. Element konfiguracji (CI) jest zarządzany w celu wykorzystania w tym systemie w celu uwzględnienia wszelkich uzasadnionych i zarejestrowanych odstępstw (patrz podrozdział 3.2.2.III). Element konfiguracji jest własnością tylko jednego systemu i jest zarządzany jako jego część, niezależnie od wspólnego źródła konfiguracji bazowej.

Element konfiguracji może składać się z jednego lub większej liczby komponentów systemu (*ang. system component - SC*), np. serwer, stacja robocza, router, aplikacja; jednego lub większej liczby obiektów systemowych niebędących komponentami (*ang. non-component - NC*), np. dokumentacja, schematy, oprogramowanie układowe; lub ich kombinacji, jak wskazano w poniższych wzorach:

I $CI_A = \{SC_1, SC_2, \ldots SC_n\};$

II $CI_B = \{NC_1, NC_2, \ldots NC_n\};$ ***bądź***

III $CI_C = \{SC_1, SC_2, \ldots SC_n + NC_1, NC_2, \ldots NC_n\},$

gdzie *n* jest większe lub równe jeden.

Na przykład system z wieloma serwerami wykorzystującymi podobną technologię może być traktowany łącznie jako jeden element konfiguracji (jak we wzorze I). Aplikacje systemowe mogą być reprezentowane jako jeden lub większa liczba elementów konfiguracji CI (również jak we wzorze I). Cała dokumentacja dla systemu może być zawarta w jednym elemencie konfiguracji CI lub każdy dokument może być traktowany jako osobny element konfiguracji CI (jak we wzorze II). Z drugiej strony, właściciel systemu może uznać, że bardziej celowe jest włączenie serwerów, aplikacji działających na serwerach oraz dokumentacji pomocniczej do jednego elementu konfiguracji CI (jak we wzorze III). Przy stosowaniu wzoru I lub II należy pamiętać, że wymóg przeglądu i zatwierdzania propozycji zmian dla jednego elementu konfiguracji CI (np. składającego się z serwerów) może być wyższy niż wymóg stosowany dla innego elementu konfiguracji CI (np. składającego się z dokumentacji). Ponadto elementy konfiguracji CI w ramach tego samego systemu można śledzić przy użyciu różnych narzędzi.

Każda pozycja w wykazie komponentów systemu (SC) jest związana tylko z jednym elementem konfiguracji (CI), a zatem jest objęta zakresem uprawnień dla pojedynczego systemu.

Każdemu elementowi konfiguracji (CI) przypisuje się jednoznaczny identyfikator, aby można było się do niego odnieść w ramach procesów SecCM. Każdy element konfiguracji (CI) może mieć serię zatwierdzonych konfiguracji bazowych w trakcie

swojego cyklu życia i jest obiektem kontroli zmian konfiguracji. Podczas cyklu życia elementu konfiguracji (CI) organizacja zarządza jego numerami wersji.

Dla każdego elementu konfiguracji (CI) utrzymywany jest zestaw elementów danych, które służą do zdefiniowania i opisania elementu konfiguracji (CI), aby umożliwić jego przebudowę od podstaw. Rodzaje informacji, które są związane z elementem konfiguracji (CI), mogą obejmować:

- system, którego częścią jest dany element CI;
- logiczne bądź fizyczne umiejscowienie w systemie;
- informacje dotyczące własności i zarządzania;
- spis komponentów systemu (SC), który składa się na element konfiguracji (CI);
- wykaz dokumentów, które składają się na element konfiguracji (CI);
- numery wersji komponentów (SC) i obiektów niebędących komponentami (NC);
- powiązania z innymi elementami konfiguracji (CI) w ramach systemu lub zależność od nich;
- informacje związane z niestandardowym oprogramowaniem (*ang. custom software*) wykorzystywanym w ramach elementu konfiguracji (CI);
- produkty lub składniki IT typowych bezpiecznych konfiguracji;
- wszelkie inne informacje potrzebne do odbudowy lub odtworzenia elementu konfiguracji (CI).

Dekompozycja systemu na szereg elementów konfiguracji (CI) może ułatwić zarządzanie zmianami w systemie, jednak należy pamiętać, że gdy jeden element konfiguracji (CI) w systemie ulegnie zmianie, może to mieć wpływ na inne elementy konfiguracji (CI) w systemie. Ponadto zatwierdzone zmiany elementu konfiguracji (CI) mogą powodować aktualizacje wykazu komponentów systemu.

Innym potencjalnym typem elementu konfiguracji (CI) do rozważenia, szczególnie w odniesieniu do ustanowienia i utrzymania programu testowania konfiguracji, jest element konfiguracji (CI) dla narzędzi SecCM i procesów testowania. Narzędzia i procesy testowania

wykorzystywane do walidacji odstępstw od zatwierdzonych konfiguracji bazowych systemu są objęte kontrolą konfiguracji w celu zmniejszenia możliwości zwracania przez takie testy wyników fałszywie dodatnich lub fałszywie ujemnych (tj. odpowiednie narzędzia i procesy są w stanie wykryć nieautoryzowane ustawienia konfiguracyjne i z powodzeniem rozpoznać zatwierdzone ustawienia konfiguracyjne).

Etap SDLC: Rozpoczęcie na etapie opracowania/pozyskania, zakończenie na etapie wdrożenia/oceny

Główne role: Właściciel systemu (SO)

Role pomocnicze: System Security Officer (SSO); Administrator systemu (SA).

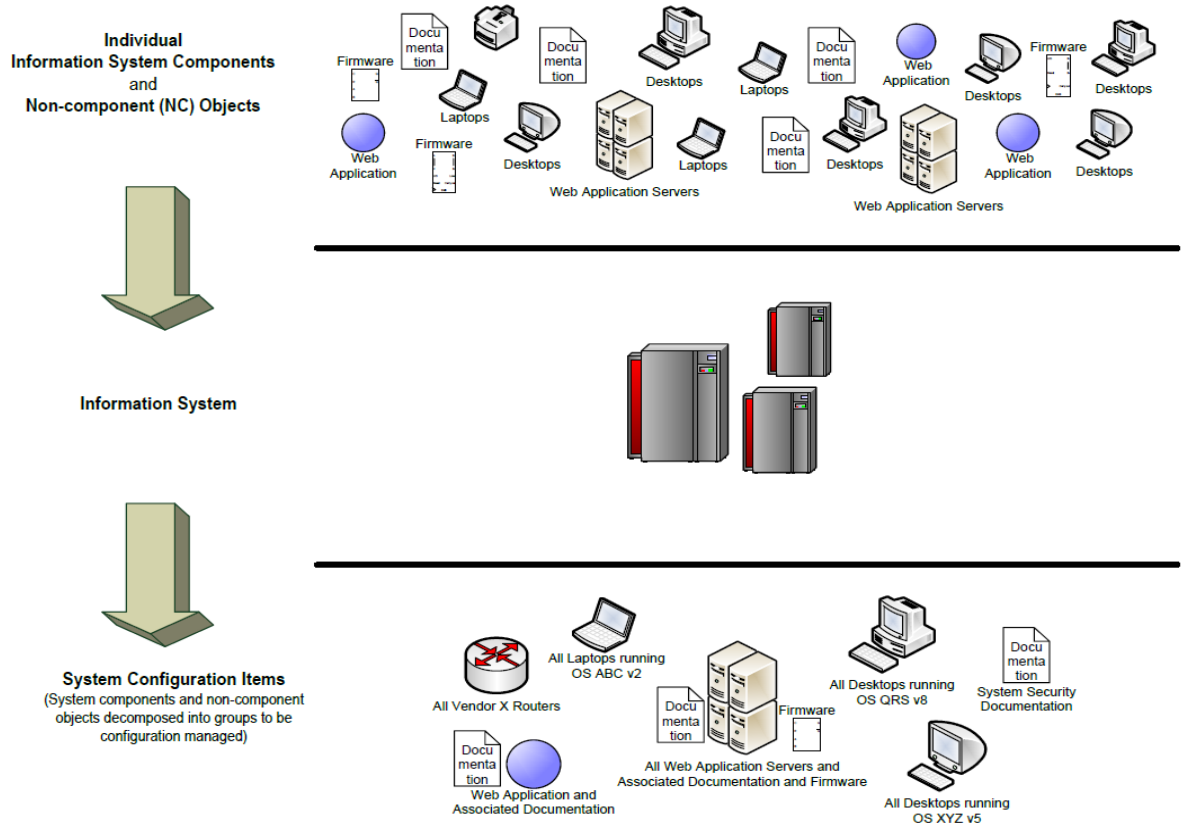
Oczekiwane dane wejściowe: Polityka i procedury na poziomie organizacji bądź systemu; wykaz komponentów systemu; dokumenty systemowe; diagramy systemowe; skrypty systemowe; kod własny systemu; wszelkie inne komponenty systemu wymagające zarządzania konfiguracją

Oczekiwane wyniki: Komponenty systemu i obiekty niebędące komponentami zgrupowane w elemencie konfiguracji (CI)

Związek między systemem informacyjnym a jego elementami konfiguracji i komponentami systemu informacyjnego

Na rysunku 3-1 przedstawiono relacje między systemem jako całością, poszczególnymi komponentami systemu i obiektami niebędącymi komponentami oraz elementami konfiguracji systemu (CI). System składa się z wielu pojedynczych komponentów i obiektów niebędących komponentami, jak opisano powyżej. Komponenty systemu i obiekty niebędące komponentami, które wymagają zarządzania konfiguracją, są grupowane w elementy konfiguracji, których konfiguracje są zarządzane jako całość. Na przykład na rysunku 3-1 na poziomie komponentu widzimy liczne pojedyncze komputery stacjonarne. Na poziomie elementu konfiguracji widzimy, że wszystkie komputery stacjonarne z systemem OS QRS w wersji 8 zostały zgrupowane w jednym elemencie konfiguracji, a komputery z systemem OS XYZ w wersji 5 – w innym. W ten sposób komponenty systemu

i obiekty niebędące komponentami, które mają powiązane/podobne/identyczne wymagania konfiguracyjne, są zarządzane z ukierunkowaniem na konfigurację jako grupa, a nie jako pojedyncze komponenty.



Rysunek 3-1 – Przykład relacji pomiędzy systemem a jego komponentami i elementami konfiguracji

Legenda do rysunku 3-1	
Terminologia angielska	**Terminologia polska**
Individual Information System Components and Non-component (NC) Objects	Komponenty i obiekty inne niż komponenty (NC) pojedynczego systemu informacyjnego
Information System	System informacyjny
System Configuration Items (System components and non-component objects decomposed into groups to be configuration managed)	Elementy konfiguracji systemu (Komponenty systemu i obiekty niebędące komponentami podzielone na grupy w celu zarządzania konfiguracją)
Firmware	Oprogramowanie układowe

Legenda do rysunku 3-1	
Terminologia angielska	**Terminologia polska**
Documentation	Dokumentacja
Web Applications	Aplikacje internetowe
Laptops	Laptopy
Desktops	Komputery stacjonarne
Web Applications Services	Usługi aplikacji internetowych
All Vendor X Routers	Wszystkie routery dostawcy X
All Laptops running OS ABC v2	Wszystkie laptopy z systemem operacyjnym ABC v2
All Web Application Servers and Associated Documentation and Firmware	Serwery wszystkich aplikacji internetowych oraz powiązana z nimi dokumentacja i oprogramowanie układowe
Web Applications and Associated Documentation	Aplikacje internetowe i powiązana z nimi dokumentacja
System Security Documentation	Dokumentacja bezpieczeństwa systemu
AJI Desktops running OS QRS v8	Wszystkie komputery biurkowe z systemem operacyjnym QRS v8

Utworzenie zespołu ds. zabezpieczeń konfiguracyjnych (CCB)systemu

Zespół CCB lub równoważna grupa zajmuje się przeglądem i zatwierdzaniem zmian w konfiguracji systemu. Zespół CCB jest tworzony przez nadanie mu statutu, który określa uprawnienia i zakres działania grupy oraz sposób jej funkcjonowania. Statut może określać członkostwo w zespole CCB, role i obowiązki jego członków oraz to, czy podlega on organowi nadzorczemu, takiemu jak zarząd czy organ zarządzający ryzykiem (funkcja). W statucie opisuje się również proces, w ramach którego działa zespół CCB, w tym sposób postępowania ze zmianami oraz zakres dyspozycji (zatwierdzone, niezatwierdzone, w zawieszeniu itp.), kryteria oceny oraz kworum wymagane do podejmowania decyzji związanych z kontrolą zmian konfiguracji.

Zespół CCB odgrywa ważną rolę podmiotu decydującego o tym, które zmiany mogą zostać uwzględnione i wprowadzone do systemu. Świadomie rozważa potencjalny

wpływ proponowanej zmiany na funkcjonalność i bezpieczeństwo systemu oraz ryzyko dla misji w przypadku wdrożenia zmiany w kontekście tolerancji ryzyka ustalonej przez organizację. Dokonując przeglądu każdej proponowanej i wdrażanej modyfikacji, zespół CCB zapewnia, że istnieje rygorystyczne, systematyczne i bezpieczne podejście do wprowadzania zmian. Jasno zdefiniowany proces lub ramy oceny i zatwierdzania wniosków o zmianę, w tym predefiniowanych kryteriów oceny, pomagają zapewnić, że każda proponowana i wdrażana zmiana jest oceniana w spójny i powtarzalny sposób, równoważący punkty widzenia w kwestiach bezpieczeństwa, biznesowych i technicznych.

Polityka organizacyjna może dopuszczać elastyczność w zakresie wielkości i stopnia sformalizowania zespołu CCB. Systemy o niskim poziomie wpływu bądź małe, nieskomplikowane rozwiązania mogą wymagać mniej formalności, w związku z czym zespół CCB może się składać z zaledwie dwóch członków (zazwyczaj właściciel systemu i SSO). W przypadku systemów o wysokim poziomie wpływu i złożonych systemów o umiarkowanym poziomie wpływu, organizacja może wymagać zespołu CCB, składającego się z minimum trzech osób, z których co najmniej jedna jest właścicielem systemu lub SSO). Dodatkowo, organizacja może określić, że konieczne jest formalne przedłożenie proponowanych zmian zespołowi CCB i przejście przez sformalizowane przeglądy i analizę wpływu na bezpieczeństwo przed akceptacją i zatwierdzeniem.

Niezależnie od wielkości i stopnia sformalizowania zespołu CCB, najlepsze praktyki kontroli zmian konfiguracji wymagają, aby zmiany w systemie były weryfikowane przez co najmniej jedną upoważnioną osobę, która jest niezależna od wnioskodawcy. W celu utrzymania odpowiedniego podziału obowiązków, administratorzy systemu, programiści itp. nie mają uprawnień do jednostronnego proponowania i zatwierdzania zmian w konfiguracji systemu (z wyłączeniem zmian określonych w procedurach jako zwolnione z SecCM). Działania kontrolne są zapisywane w artefakcie, który można zarchiwizować (np. protokoły CCB, działania, które należy podjąć, przydzielona odpowiedzialność za działania wygenerowane sprawozdania, zatwierdzenia/odrzucenia i uzasadnienia itp.).

Wybierając członków zespołu CCB, organizacja bierze pod uwagę role, które reprezentują różnych interesariuszy. Przy włączaniu członków do zespołu CCB są brane pod uwagę punkty widzenia i wiedza fachowa osób reprezentujących misję organizacji bądź systemu, bezpieczeństwo informacji (SSO, architekci bezpieczeństwa itp.), technologię informacyjną (np. administratorzy systemu, inżynierowie sieci, osoby odpowiedzialne za architekturę korporacyjną itp.), użytkowników końcowych, klientów, sprzedawców itp. Nie jest konieczne, aby wszyscy członkowie mieli prawo głosu w zespole CCB, ale ich wkład może pomóc w usprawnieniu procesu podejmowania decyzji. Przykładowo, udział dostawcy może być cenny ze względu na wgląd w specyficzne dla danego produktu funkcje, cechy lub konfiguracje, ale dostawca nie ma prawa głosu w sprawie zatwierdzenia zmiany.

Etap SDLC: Rozpoczęcie na etapie opracowania/pozyskania, zakończenie na etapie wdrożenia/oceny

Główne role: Menadżer programu SecCM (jeśli jest ustanowiony na poziomie organizacyjnym); właściciel systemu (jeśli jest ustanowiony na poziomie systemu). Uwaga: Jeśli pojedynczy zespół CCB obsługuje wiele systemów, ale nie jest na poziomie organizacyjnym, za wdrożenie CCB odpowiada grupa właścicieli wszystkich systemów objętych kontrolą.

Role pomocnicze: SAISO (jeśli nie jest menadżerem programu SecCM); SSO

Oczekiwane dane wejściowe: Polityki i procedury na poziomie organizacji bądź systemu

Oczekiwane wyniki: Utworzony zespół ds. zabezpieczeń konfiguracyjnych i jego statut

3.2 Określanie i wdrażanie konfiguracji

W kolejnych podrozdziałach opisano działania na etapie *określania i wdrażania konfiguracji*. Na tym etapie działania są zwykle kończone na poziomie systemu, zgodnie z obowiązującą organizacyjną bądź systemową polityką i procedurami SecCM. Podrozdziały są wymienione w ogólnym porządku chronologicznym, w jakim występują działania konfiguracyjne. Jak zawsze, organizacje mają swobodę w określaniu, które działania mają być wykonywane, na jakim poziomie i w jakiej kolejności. Ukończenie etapu identyfikowania i wdrażania konfiguracji skutkuje wdrożeniem bezpiecznej konfiguracji bazowej dla każdego systemu i składających się

na niego elementów konfiguracji, (tzn. każdy utworzony element konfiguracji jest obiektem udokumentowanej i zatwierdzonej bezpiecznej konfiguracji).

3.2.1 Ustanawianie bezpiecznych konfiguracji

Podczas opracowywania i wdrażania systemu ustanawia się bezpieczne konfiguracje dla systemu i składających się na niego elementów konfiguracji (CI). Bezpieczne konfiguracje mogą obejmować:

- Ustawianie bezpiecznych wartości (tj. parametrów, które opisują, jak zachowują się poszczególne zautomatyzowane funkcje produktów informatycznych), w tym m.in.:
  - ✓ funkcje systemu operacyjnego i aplikacji (włączenie lub wyłączenie w zależności od konkretnej funkcji, ustawienie konkretnych parametrów itp.);
  - ✓ usługi (np. automatyczne aktualizacje) i porty (np. DNS przez port 53);
  - ✓ protokoły sieciowe (np. NetBIOS, IPv6) i interfejsy sieciowe (np. Bluetooth, IEEE 802.11, podczerwień);
  - ✓ metody zdalnego dostępu (np. SSL, VPN, SSH, IPSEC);
  - ✓ kontrole dostępu (np. kontrola uprawnień do plików, katalogów, kluczy rejestru oraz ograniczanie działań użytkownika, takich jak modyfikowanie dzienników systemowych czy instalowanie aplikacji);
  - ✓ zarządzanie identyfikatorami/kontami (np. zmiana domyślnych nazw kont, określanie długości czasu do wyłączenia nieaktywnych kont, stosowanie unikalnych nazw użytkowników, tworzenie grup użytkowników);
  - ✓ kontrole uwierzytelniania (np. długość hasła, stosowanie znaków specjalnych, minimalna ważność hasła, uwierzytelnianie wieloskładnikowe/używanie tokenów);
  - ✓ ustawienia audytu (np. przechwytywanie kluczowych zdarzeń, takich jak awarie, logowania, zmiany uprawnień, nieudany dostęp do plików, tworzenie użytkowników i obiektów, usuwanie i modyfikowanie plików systemowych, zmiany kluczy rejestru i jądra);

- ✓ ustawienia systemowe (np. limit czasu sesji, liczba połączeń zdalnych, blokada sesji);
- ✓ kryptografia (np. stosowanie zatwierdzonych protokołów i algorytmów kryptograficznych zgodnych z [FIPS 140-3] - w celu ochrony danych podczas przesyłania i przechowywania).

- Stosowanie poprawek wydanych przez producenta w odpowiedzi na zidentyfikowane podatności, w tym aktualizacje oprogramowania.
- Używanie zatwierdzonego, certyfikowanego oprogramowania, jeśli jest wspierane.
- Wdrożenie zabezpieczeń chroniących urządzenia użytkowników końcowych przed atakiem (np. programy antywirusowe, antyszpiegowskie, programy do usuwania reklam, osobiste zapory sieciowe, systemy wykrywania włamań oparte na hostach HIPS).
- Stosowanie zabezpieczeń sieciowych (np. TLS, IPSEC).
- Ustalenie miejsca, w którym fizycznie i logicznie znajduje się dany komponent (np. za zaporą sieciową, w strefie DMZ, w określonej podsieci itp.).
- Utrzymanie i aktualizacja specyfikacji technicznej i dokumentacji projektowej, dokumentacji bezpieczeństwa systemu, procedur systemowych itp.

W wielu przypadkach polityka organizacyjna, zgodnie z przepisami, normami, dyrektywami i zaleceniami, ustanawia ogólnie przyjęte wspólne bezpieczne konfiguracje (np. National Checklist Program, DISA STIG, CIS Benchmarks). Konfiguracje zidentyfikowane w repozytorium National Checklist Program[28], jak również listy kontrolne zawarte w SCAP są źródłem ustanowienia typowych bezpiecznych konfiguracji. Twórcy produktów komercyjnych są również potencjalnym źródłem typowych bezpiecznych konfiguracji. Odstępstwa od powszechnie

[28] NIST [SP 800-70] zawiera informacje o National Checklist Program and Repository. Patrz również https://www.nist.gov/programs-projects/national-checklist-program, gdzie znajdują się listy kontrolne z wielu wiarygodnych źródeł, w tym DISA STIG, CIS Benchmarks i dostawców komercyjnych; a także https://nvd.nist.gov/ncp/repository, aby uzyskać więcej informacji na temat repozytorium.

stosowanych bezpiecznych konfiguracji muszą być uzasadniane i rejestrowane (patrz podrozdział 3.2.2.III).

Podczas tworzenia i utrzymywania bezpiecznych konfiguracji organizacje biorą pod uwagę potencjalne konflikty interoperacyjności we wzajemnie połączonych systemach. Koordynacja bezpiecznych konfiguracji bazowych między osobami zajmującymi się obsługą systemu bądź właściwymi zespołami CCB pomaga zapewnić synchronizację bezpiecznych konfiguracji między połączonymi systemami w celu spełnienia żądanych wymagań dotyczących funkcji bezpieczeństwa i operacyjnych.

Jeśli nie zostało to określone w politykach i procedurach organizacyjnych, właściciel systemu, w koordynacji z SSO, jest odpowiedzialny za ustanowienie bezpiecznych konfiguracji systemu (opartych na odpowiednich, typowych bezpiecznych konfiguracjach, jeśli są dostępne) i składających się na niego elementów konfiguracji. Niezależnie od podmiotu odpowiedzialnego, bezpieczne konfiguracje spełniają wszystkie obowiązujące wymogi centralne i są zatwierdzane zgodnie z polityką organizacyjną.

Etap SDLC: Rozpoczęcie na etapie opracowania/pozyskania, zakończenie na etapie wdrożenia/oceny

Główne role: Właściciel systemu (SO); System Security Officer (SSO)

Role pomocnicze: Administrator systemu (SA); deweloper systemu/aplikacji.

Oczekiwane dane wejściowe: Polityki i procedury na poziomie organizacji bądź systemu, w tym obowiązkowe lub sugerowane typowe bezpieczne konfiguracje; plan bezpieczeństwa systemu/ wymagania dotyczące bezpieczeństwa systemu; dokumentacja techniczna systemu/komponentu.

Oczekiwane wyniki: Wstępne bezpieczne konfiguracje bazowe systemu i jego elementów konfiguracji (CI).

3.2.2 Wdrażanie bezpiecznych konfiguracji

Wdrażanie bezpiecznych konfiguracji produktów informatycznych nie jest prostym zadaniem. Istnieje wiele produktów informatycznych, a każdy z nich ma niezliczoną liczbę możliwych parametrów, które można skonfigurować. Ponadto organizacje mają

potrzeby związane z misją i procesami biznesowymi, które mogą wymagać skonfigurowania produktów informatycznych w określony sposób. W przypadku niektórych produktów może istnieć konieczność modyfikacji ustawień konfiguracyjnych platformy bazowej, aby zapewnić funkcjonalność wymaganą do realizacji misji, co powoduje, że odbiegają one od zatwierdzonych typowych bezpiecznych konfiguracji.

Wykorzystując ustanowioną wcześniej bezpieczną konfigurację (patrz podrozdział 3.2.1) jako punkt wyjścia, zaleca się następujące uporządkowane podejście podczas jej wdrażania:

I Nadawanie priorytetu konfiguracjom

W idealnym środowisku wszystkie produkty informatyczne w organizacji byłyby skonfigurowane do najbardziej bezpiecznego stanu, który nadal zapewniałby funkcjonalność wymaganą przez organizację. Jednak, z powodu limitowanych zasobów i innych ograniczeń, wiele organizacji może uznać za konieczne ustalenie priorytetów wskazujących, które systemy, produkty informatyczne lub elementy konfiguracji powinny być skonfigurowane podczas wdrażania SecCM w pierwszej kolejności.

Przy określaniu priorytetów wdrażania bezpiecznych konfiguracji w systemach, produktach informatycznych lub elementach konfiguracji, organizacje biorą pod uwagę następujące kryteria:

- Poziom wpływu na system – wdrażanie bezpiecznych konfiguracji w systemach o wysokim lub umiarkowanym poziomie wpływu na bezpieczeństwo może mieć pierwszeństwo przed systemami o niskim poziomie wpływu na bezpieczeństwo.
- Szacowanie ryzyka – oszacowanie ryzyka może być wykorzystane do określenia systemów, produktów informatycznych lub elementów konfiguracji mających największy wpływ na bezpieczeństwo i ryzyko organizacyjne.
- Skanowanie podatności – skany podatności mogą być wykorzystane do namierzania systemów, produktów informatycznych lub elementów konfiguracji, które są najbardziej podatne na ataki. Na przykład, Common Vulnerability Scoring

System (CVSS) jest specyfikacją w ramach SCAP, która zapewnia otwarte środowisko do przekazywania informacji na temat właściwości luk w oprogramowaniu i obliczania ich względnej szkodliwości. Wyniki CVSS mogą być użyte do ustalenia priorytetów konfiguracji i wdrażania poprawek.

- Stopień penetracji – stopień penetracji reprezentuje zakres, w jakim dany produkt jest wdrażany w środowisku informatycznym. Na przykład, jeśli organizacja używa określonego systemu operacyjnego na 95% swoich stacji roboczych, może uzyskać najbardziej bezpośrednią wartość przez planowanie i wdrażanie bezpiecznych konfiguracji dla tego systemu operacyjnego. W dalszej kolejności można zająć się innymi produktami informatycznymi lub elementami konfiguracji.

II Testowanie konfiguracji

Organizacje przeprowadzają pełne testy bezpiecznych konfiguracji przed wdrożeniem w środowisku produkcyjnym. Podczas wdrażania konfiguracji można napotkać wiele różnych problemów, takich jak kompatybilność oprogramowania i niezgodność sterowników urządzeń. Na przykład mogą istnieć starsze aplikacje o specjalnych wymaganiach operacyjnych, które nie działają prawidłowo po zastosowaniu typowej bezpiecznej konfiguracji. Ponadto mogą wystąpić błędy konfiguracji, jeśli system operacyjny (OS) i konfiguracje wielu aplikacji zostaną zastosowane do tego samego komponentu. Na przykład ustawienie parametru konfiguracji aplikacji może być niezgodne z podobnym ustawieniem parametru konfiguracji systemu operacyjnego.

Do testowania bezpiecznych konfiguracji są zalecane środowiska wirtualne, ponieważ pozwalają organizacjom zbadać funkcjonalny wpływ na aplikacje bez konieczności konfigurowania rzeczywistych maszyn.

III Rozwiązywanie problemów i dokumentowanie odstępstw

Testowanie bezpiecznych wdrożeń konfiguracji może wprowadzić problemy funkcjonalne w ramach systemu lub aplikacji. Na przykład nowa bezpieczna konfiguracja może zamknąć port lub zatrzymać usługę, która jest potrzebna do

działania systemu operacyjnego lub aplikacji. Problemy te są badane indywidualnie i albo są rozwiązywane, albo dokumentowane jako odstępstwo lub wyjątek od ustalonych typowych bezpiecznych konfiguracji.

W niektórych przypadkach zmiana jednego ustawienia konfiguracyjnego może wymagać zmiany innego ustawienia, innego elementu konfiguracji lub innego systemu. Na przykład typowa bezpieczna konfiguracja może wprowadzić bardziej rygorystyczne wymagania dotyczące hasła, które z kolei mogą wymagać zmiany istniejących aplikacji używających „zredukowanego" logowania SSO (*ang. single sign-on - SSO*). Może też istnieć wymóg, aby zapora sieciowa wbudowana w system operacyjny była domyślnie włączona. W celu zapewnienia, że aplikacje działają zgodnie z oczekiwaniami, może być konieczna zmiana polityki dotyczącej zapory sieciowej, aby zezwolić na używanie określonych portów, usług, adresów IP itp. Gdy nie można rozwiązać konfliktów między aplikacjami a bezpiecznymi konfiguracjami, odstępstwa należy dokumentować i zatwierdzać w ramach procesu kontroli zmian konfiguracji, stosownie do sytuacji.

IV Rejestrowanie i zatwierdzanie konfiguracji bazowej

Ustalona i przetestowana bezpieczna konfiguracja, wraz z wszelkimi niezbędnymi odstępstwami, stanowi przewidywaną konfigurację bazową. Jest ona rejestrowana w celu wspomagania kontroli zmian konfiguracji/analizy wpływu na bezpieczeństwo, rozwiązywania incydentów, rozwiązywania problemów i prowadzenia działań monitorujących. Po zapisaniu, przewidywana konfiguracja bazowa jest zatwierdzana zgodnie z polityką zdefiniowaną w organizacji. Po zatwierdzeniu, przewidywana konfiguracja bazowa staje się wstępna (inicjalną) konfiguracją bazową systemu i składających się na niego elementów konfiguracji.

Konfiguracja bazowa systemu obejmuje wszystkie bezpieczne konfiguracje i składające się na nie elementy konfiguracji. Stanowi ono konfigurację specyficzną dla systemu, względem której kontrolowane są wszystkie zmiany.

Konfiguracja bazowa może obejmować, w stosownych przypadkach, informacje dotyczące architektury systemu, wzajemnych połączeń komponentów sprzętowych,

bezpiecznych ustawień konfiguracyjnych komponentów programowych, obciążenia oprogramowania, dokumentacji pomocniczej oraz elementów w wydanej aktualizacji do oprogramowania. Dla każdego etapu cyklu życia systemu (takiego jak rozwój, testowanie, przemieszczanie, produkcja) może istnieć inna konfiguracja bazowa.

Gdy jest to możliwe, organizacje stosują zautomatyzowane narzędzia wspomagające zarządzanie konfiguracjami bazowymi oraz utrzymujące informacje o konfiguracji w stanie jak najbardziej aktualnym i zbliżonym do rzeczywistego. Istnieje wiele rozwiązań, które utrzymują konfiguracje bazowe dla szerokiej gamy produktów sprzętowych i programowych. Niektóre kompleksowe rozwiązania SecCM integrują utrzymanie konfiguracji bazowych z narzędziami do inwentaryzacji i monitorowania komponentów.

V Wdrażanie konfiguracji bazowej

Zachęca się organizacje do wdrażania konfiguracji bazowych w sposób scentralizowany i zautomatyzowany przy użyciu narzędzi do zarządzania konfiguracją, automatycznych skryptów, mechanizmów dostarczonych przez dostawcę itp.

Biblioteki nośników danych mogą być używane do przechowywania, ochrony i kontroli kopii wzorcowych zatwierdzonych wersji konfiguracji bazowych. Nośnikiem może być środek do przechowywania informacji (papier, taśmy, płyty CD/DVD, napędy USB itp.) lub sama informacja (np. pliki, kod programu). Biblioteka nośników może również zawierać licencjonowane komercyjne oprogramowanie, oprogramowanie tworzone na zamówienie oraz inne artefakty i dokumenty generowane w trakcie SDLC.

Etap SDLC: Etap wdrażania/oceny

Główne role: Właściciel systemu (SO); System Security Officer (SSO)

Role pomocnicze: Administrator systemu (SA); Deweloper systemu/oprogramowania

Oczekiwane dane wejściowe: Polityki i procedury na poziomie organizacji bądź systemu, w tym obowiązkowe lub sugerowane typowe bezpieczne konfiguracje; plan bezpieczeństwa systemu/ wymogi bezpieczeństwa systemu; dokumentacja techniczna systemu/komponentu

Oczekiwane wyniki: Zatwierdzone, zarejestrowane i wdrożone konfiguracje bazowe

elementów konfiguracji systemu, w tym zarejestrowane odstępstwa od typowych bezpiecznych konfiguracji

3.3 Kontrola zmian konfiguracji

Jeśli organizacje mają utrzymać bezpieczne konfiguracje systemów w środowisku, w którym technologia nieustannie się rozwija, a liczba i istotność zagrożeń wzrasta, zmiany konfiguracji systemów muszą być zarządzane i kontrolowane.

W kolejnych podrozdziałach opisano działania na etapie *kontrolowania zmian konfiguracji*. Na tym etapie działania są zwykle realizowane na poziomie systemu zgodnie z polityką i procedurami. Podrozdziały są wymienione w kolejności, w jakiej zazwyczaj występują działania związane z konfigurowaniem. Jak zawsze, organizacje mają swobodę w określaniu, które działania mają być wykonywane, na jakim poziomie i w jakiej kolejności. Ukończenie etapu kontroli zmian konfiguracji skutkuje wdrożeniem ograniczeń dostępu do zmian oraz udokumentowaniem procesów kontroli zmian konfiguracji i procesów analizy wpływu na bezpieczeństwo.

3.3.1 Wdrożenie ograniczeń dostępu do zmian

Ograniczenia dostępu do zmian reprezentują stronę wykonawczą SecCM. Kontrola zmian konfiguracji jest procesem polegającym na obsłudze zmian systemu w ramach zarządzanego procesu, przy czym bez wprowadzenia ograniczeń dostępu dowolna osoba mogłaby wprowadzić zmiany poza procesem. Ograniczenia dostępu są mechanizmem egzekwowania procesów kontroli konfiguracji przez kontrolę dostępu do systemu bądź składających się na niego elementów konfiguracji w celu dokonywania zmian. Ograniczenia dostępu do zmiany mogą obejmować również kontrolę dostępu do dodatkowych informacji związanych ze zmianą, takich jak wnioski o zmianę, zapisy, korespondencja, plany i wyniki testów zmiany itp.

Wdrożenie ograniczeń dostępu dla zmian:

- określenie możliwych rodzajów zmian konfiguracji, które można wprowadzić w systemie z uwzględnieniem warstwy sieciowej, systemu operacyjnego i aplikacji;

II ustalenie, które osoby mają uprzywilejowany dostęp i które z tych uprzywilejowanych osób są upoważnione do dokonywania danych typów zmian;

III wdrożenie mechanizmów technicznych (np. dostęp oparty na rolach, uprawnienia do plików/grup itp.) w celu zapewnienia, że tylko uprawnione osoby mogą wprowadzać odpowiednie zmiany.

Etap SDLC: Etap wdrażania/oceny

Główne role: Właściciel systemu (SO); System Security Officer (SSO)

Role pomocnicze: Administrator systemu (SA)

Oczekiwane dane wejściowe: Plan bezpieczeństwa systemu/ wymagania dotyczące bezpieczeństwa systemu; polityka i procedury na poziomie organizacji bądź systemu

Oczekiwane wyniki: Odpowiednie ograniczenia dostępu dla zmian wprowadzonych w systemie

3.3.2 Wdrożenie procesu kontroli zmian konfiguracji

Dobrze zdefiniowany proces kontroli zmian konfiguracji jest podstawą każdego programu SecCM. Kontrola zmian konfiguracji to proces zapewniający, że zmiany konfiguracji systemu są przed wdrożeniem formalnie wnioskowane, oceniane pod kątem ich wpływu na bezpieczeństwo, testowane pod kątem skuteczności i zatwierdzane. Proces ten może mieć różne etapy i poziomy wymagań w zależności od tolerancji ryzyka organizacyjnego bądź poziomu wpływu na system, jednak kontrola zmian konfiguracji składa się zwykle z następujących kroków:

I **Żądanie** zmiany. Wniosek o zmianę może pochodzić z dowolnej liczby źródeł, w tym od użytkownika końcowego systemu, z działu pomocy technicznej lub od kierownictwa. Proponowane zmiany mogą również pochodzić z poprawek dostarczanych przez producenta, aktualizacji aplikacji, alarmów bezpieczeństwa, skanowania systemu itp. Przykładowy szablon wniosku o zmianę – patrz Załącznik E.

II **Rejestracja** wniosku o wprowadzenie proponowanej zmiany. Wniosek o zmianę jest formalnie wprowadzany do procesu kontroli zmian

konfiguracji, gdy jest rejestrowany zgodnie z procedurami organizacyjnymi. Organizacje mogą wykorzystywać wnioski w formie papierowej, przesłane w wiadomości e-mail, przez system helpdesku bądź zautomatyzowanego narzędzia do śledzenia wniosków o zmianę kierowanych w oparciu o procesy przepływu pracy i pozwalających na elektroniczne potwierdzenia/zatwierdzenia.

III **Określenie**, czy proponowana zmiana wymaga kontroli konfiguracji. Niektóre rodzaje zmian mogą być wyłączone z kontroli zmian konfiguracji lub wstępnie zatwierdzone, jak określono w planie bądź procedurach SecCM. Jeżeli zmiana jest wyłączona z kontroli lub wstępnie zatwierdzona, należy odnotować to we wniosku o zmianę i pozwolić na wprowadzenie zmiany bez dalszej analizy lub zatwierdzenia; jednak dokumentacja systemowa może nadal wymagać aktualizacji (np. plan bezpieczeństwa systemu, konfiguracja bazowa, wykaz komponentów systemu itp.)

IV **Analiza** proponowanej zmiany pod kątem jej wpływu na bezpieczeństwo systemu (patrz podrozdział 3.3.3).

V **Testowanie** proponowanej zmiany pod kątem wpływu na bezpieczeństwo i funkcjonalność. Testowanie potwierdza wpływ zidentyfikowany podczas analizy bądź ujawnia dodatkowy wpływ. Skutki zmiany są przedstawiane zespołowi CCB i osobie autoryzującej (AO).

VI **Zatwierdzenie** zmiany. Ten krok jest zwykle wykonywany przez zespół CCB. Zespół CCB może wymagać wdrożenia dodatkowych środków bezpieczeństwa, jeżeli zmiana jest niezbędna do realizacji misji, ale ma negatywny wpływ na bezpieczeństwo systemu i organizacji. Wdrożenie dodatkowych środków bezpieczeństwa jest koordynowane z osobą autoryzującą (AO) i właścicielem systemu.

VII **Wdrożenie** zatwierdzonej zmiany. Po zatwierdzeniu zmiany, upoważnione osoby dokonują stosownej zmiany. W zależności od zakresu zmiany, pomocne może być opracowanie planu wdrożenia. Wdrożenie zmiany

obejmuje zmiany stosownych/powiązanych parametrów konfiguracyjnych, jak również aktualizację dokumentacji systemu w celu odzwierciedlenia zmiany (zmian). Zainteresowane strony (np. użytkownicy, kierownictwo, helpdesk itp.) są powiadamiane o zmianie, zwłaszcza jeśli wdrożenie zmiany wymaga przerwania świadczenia usług lub zmienia funkcjonalność systemu. W przypadku tej ostatniej sytuacji może być wymagane szkolenie użytkowników i pracowników helpdesk.

VIII **Sprawdzenie**, czy zmiana została wdrożona prawidłowo (np. skanowanie podatności, analiza bezpieczeństwa i funkcjonalności po wdrożeniu, ponowna ocena środków bezpieczeństwa, których to dotyczy, itp.). Kontrola zmian konfiguracji nie jest kompletna, a wniosek o zmianę nie jest zamknięty, dopóki nie zostanie potwierdzone, że zmiana została wdrożona prawidłowo. Może się zdarzyć, że chociaż początkowa analiza wpływu na bezpieczeństwo i testy mogły nie wykazać żadnego wpływu zmiany, to jednak niewłaściwie wdrożona zmiana może spowodować problemy z bezpieczeństwem.

IX **Zamknięcie** wniosku o zmianę. Wraz z zakończeniem powyższych czynności wniosek o zmianę jest zamykany zgodnie z procedurami obowiązującymi w organizacji.

Zmiany są również oceniane pod kątem spójności z organizacyjną architekturą korporacyjną. Jeśli procedury kontroli zmian konfiguracji zostały zdefiniowane przez organizację, właściciel systemu interpretuje je w kontekście systemu docelowego i udoskonala proces, aby można go było wykonać. Zmiany w procesie mogą wymagać zatwierdzenia przez zespół CCB na poziomie organizacji, zgodnie z polityką SecCM.

Ważne jest, aby personel IT ds. operacji i utrzymania, który obsługuje system, był aktywnym uczestnikiem procesu kontroli zmian konfiguracji i był odpowiedzialny za zgodność z tym procesem. Jeśli konieczne jest znaczne przeprojektowanie procesów biznesowych, na przykład aktualizacja działań helpdesku lub procesu zarządzania poprawkami, może być wymagane szkolenie.

Nieplanowane lub nieautoryzowane zmiany

Często się zdarza, że działania takie jak wdrażanie lub usuwanie sprzętu, wprowadzanie zmian w konfiguracji oraz instalowanie poprawek odbywają się poza procesem kontroli zmian konfiguracji, mimo że mogą mieć znaczny wpływ na bezpieczeństwo systemu. Dodatkowo mogą pojawić się sytuacje wymagające nieplanowanej (awaryjnej) zmiany. Obowiązkiem właścicieli systemu jest identyfikacja wszystkich źródeł zmian, aby upewnić się, że zmiany wymagające kontroli konfiguracji przechodzą proces kontroli, nawet jeśli jest wykonywany po fakcie.

Jeśli pojawi się konieczność wprowadzenia nieplanowanych zmian, a czas nie pozwala na przeprowadzenie ustalonego procesu kontroli zmian konfiguracji, nieplanowane zmiany są nadal zarządzane i kontrolowane. Organizacje zapewniają instrukcje dotyczące obsługi nieplanowanych zmian w ramach kontroli zmian konfiguracji, jak również instrukcje dotyczące obsługi nieautoryzowanych zmian, które są następnie wykrywane. Procedury kontroli zmian konfiguracji dotyczą również usuwania usterek, aby przyspieszyć zmianę, ale w sposób kontrolowany, w celu usunięcia błędów oprogramowania. Nieplanowane zmiany są analizowane/rozwiązywane przez zespół CCB tak szybko, jak to możliwe po wprowadzeniu nieplanowanych zmian.

Etap SDLC: Etap wdrożenia/oceny, trwający podczas etapu eksploatacji i utrzymania

Główne role: Właściciel systemu (SO); CCB, System Security Officer (SSO)

Role pomocnicze: Administrator systemu (SA), użytkownik systemu (SU)

Oczekiwane dane wejściowe: Polityki i procedury SecCM na poziomie organizacji bądź systemu; plan bezpieczeństwa systemu/ wymagania dotyczące bezpieczeństwa systemu

Oczekiwane wyniki: Udokumentowany i wdrożony proces kontroli zmian konfiguracji

3.3.3 Przeprowadzenie analizy wpływu na bezpieczeństwo

Analiza wpływu na bezpieczeństwo jest jednym z najbardziej krytycznych kroków w procesie kontroli zmian konfiguracji w odniesieniu do SecCM. Organizacje przeznaczają znaczne środki na rozwój i utrzymanie bezpiecznego stanu systemów; brak właściwej analizy zmiany pod kątem wpływu na bezpieczeństwo może zniweczyć wysiłek włożony w zapewnienie bezpieczeństwa systemu i narazić organizację na atak. Działanie związane z analizą wpływu

na bezpieczeństwo zapewnia połączenie między kontrolą zmiany konfiguracji a poprawą stanu bezpieczeństwa. Zarządzanie zmianami przez ustrukturyzowany proces ma swoje korzyści – na przykład zwiększenie efektywności. Jednak tylko wtedy, gdy zmiany są oceniane pod kątem ich wpływu na bezpieczeństwo, proces kontroli zmian konfiguracji przynosi korzyści dotyczące stanu bezpieczeństwa systemu.

Bardzo duże organizacje lub właściciele dużych i złożonych systemów mogą uznać za pomocne utworzenie komisji ds. weryfikacji konfiguracji, który będzie zarządzać i przeprowadzać analizy wpływu na bezpieczeństwo oraz przekazywać wyniki do odpowiedniego zespołu CCB.

Zmiany są badane pod kątem wpływu na bezpieczeństwo oraz pod kątem zabezpieczeń, które mogą być wdrażane w celu ograniczenia wynikających ze zmiany wykrytych podatności. Analizy wpływu na bezpieczeństwo są prowadzone przez osoby lub zespoły mające techniczną wiedzę o systemie w całym SDLC, tak aby wpływ zmian na bezpieczeństwo był rozważany na każdym etapie:

- **Etap inicjowania (przed wprowadzeniem zmiany)**

  Analiza wpływu na bezpieczeństwo przed wdrożeniem zmiany ma kluczowe znaczenie dla ustalenia, czy zmiana będzie miała wpływ na bezpieczny stan systemu. Wstępna analiza wpływu na bezpieczeństwo jest przeprowadzana przed zatwierdzeniem zmiany przez zespół CCB. Jeśli istnieją obawy dotyczące bezpieczeństwa związane ze zmianą, można się nimi zająć/złagodzić je, zanim przystąpi się do utworzenia, przetestowania bądź wdrożenia zmiany.

- **Etapy opracowania/pozyskania i wdrożenia/oceny**

  Analiza wpływu na bezpieczeństwo nie jest jednorazowym zdarzeniem na etapie inicjowania w celu wsparcia decyzji zespołu CCB przy zatwierdzaniu zmian. Kiedy zmiana jest wstępnie proponowana i przeglądana, sposób, w jaki zostanie utworzona i wdrożona, może nie być znany, co może w znacznym stopniu rzutować na jej wpływ na bezpieczeństwo. Przykładowo, w przypadku komponentu tworzonego na zamówienie w fazie projektowania przeprowadza się analizę wpływu na bezpieczeństwo w odniesieniu do technicznych

dokumentów projektowych, aby się upewnić, że projekt uwzględnia najlepsze praktyki w zakresie bezpieczeństwa, wdraża odpowiednie zabezpieczenia i nie będzie wymagać ponownego opracowania w późniejszym czasie z powodu wprowadzonych podatności. Programiści zapewniają, że podczas tworzenia komponentu, jego bezpieczeństwo jest brane pod uwagę, a projekt jest testowany podczas wdrażania, aby potwierdzić, że oczekiwane środki bezpieczeństwa zostały wdrożone i że nie wprowadzono nowych lub nieoczekiwanych podatności.

- **Etap eksploatacji i utrzymania (po wdrożeniu zmiany)**

  Analiza wpływu na bezpieczeństwo w fazie operacji i utrzymania potwierdza, że pierwotna analiza wpływu na bezpieczeństwo była prawidłowa oraz że nieoczekiwane podatności lub wpływ na środki bezpieczeństwa niezidentyfikowane w środowisku testowym nie zostały wprowadzone do środowiska operacyjnego. Dodatkowo na etapie eksploatacji i utrzymania analizowany jest wpływ na bezpieczeństwo nieplanowanych i nieautoryzowanych zmian.

Proces analizy wpływu na bezpieczeństwo składa się z następujących kroków:

I **Zrozumienie zmiany** – jeśli zmiana jest proponowana, należy opracować ogólny przegląd architektury, który pokaże, jak zmiana zostanie wdrożona. Jeśli zmiana już nastąpiła (nieplanowana/nieautoryzowana), należy uwzględnić dokumentację/informacje uzupełniające i dokonać jej przeglądu lub wykorzystać wszelkie dostępne informacje (np. zapisy z audytu, wywiad z pracownikami, którzy dokonali zmiany itp.).

II Identyfikowanie podatności na zagrożenia – jeśli zmiana dotyczy sprzętu lub oprogramowania COTS, identyfikacja podatności może obejmować między innymi przeszukanie np. bazy danych dotyczących podatności na zagrożenia (*ang. National Vulnerability Database – NVD*)[29], która zawiera listę podatności,

[29] https://nvd.nist.gov/

doświadczenia użytkowników itp. Organizacje mogą wykorzystywać informacje z bazy NVD do rozwiązywania znanych problemów i ich usuwania lub łagodzenia, zanim staną się zagrożeniem. Można również przeszukać inne publiczne bazy danych podatności, słabych punktów i zagrożeń (np. CERT). Za pomocą niektórych zautomatyzowanych narzędzi do skanowania podatności (w miarę możliwości zwalidowanych przez SCAP) można przeszukiwać różne publiczne bazy podatności, które odnoszą się do produktów informatycznych/ nazw CPE produktów informatycznych. Jeśli zmiana wiąże się z rozwiązaniem niestandardowym, przeprowadzana jest bardziej dogłębna analiza wpływu na bezpieczeństwo. Bezpieczeństwo aplikacji wykracza poza zakres tej publikacji, jednak istnieje wiele najlepszych praktyk i użytecznych źródeł informacji na temat tego, jak zapewnić bezpieczeństwo kodu źródłowego oprogramowania.

III **Ocena ryzyka** – po zidentyfikowaniu podatności należy przeprowadzić ocenę ryzyka, aby określić prawdopodobieństwo wystąpienia zagrożenia wykorzystującego podatność oraz wpływ takiego zdarzenia. Podatności mogą zostać zidentyfikowane w zmianach w miarę ich proponowania, tworzenia i testowania, jednak oszacowane ryzyko może być na tyle niskie, że można je zaakceptować bez podejmowania działań naprawczych (tj. akceptacja ryzyka). W innych przypadkach ryzyko może być na tyle wysokie, że zmiana nie jest zatwierdzana (unikanie ryzyka) lub wdrażane są zabezpieczenia i środki zaradcze w celu zmniejszenia ryzyka (łagodzenie ryzyka)[30].

IV **Ocena wpływu na istniejące zabezpieczenia** – oprócz oceny ryzyka związanego ze zmianą, organizacje analizują, czy i jak zmiana wpłynie na istniejące zabezpieczenia. Na przykład, zmiana może obejmować instalację oprogramowania, które zmienia istniejącą konfigurację bazową, albo sama zmiana może powodować lub wymagać zmiany w istniejącej konfiguracji bazowej. Zmiana może mieć również wpływ na inne systemy lub ich komponenty, które zależą od zmienianej funkcji lub komponentu, tymczasowo lub trwale. Na przykład, jeśli baza danych, która jest używana

[30] Więcej informacji na temat oceny ryzyka można znaleźć w publikacji [NSC 800-30].

do działania zabezpieczeń związanych z audytowaniem, zostanie zaktualizowana do najnowszej wersji, funkcjonalność audytu w systemie może zostać wstrzymana na czas wdrażania aktualizacji.

V **Planowanie zabezpieczeń i środków zaradczych** – w przypadkach, gdy ryzyko zostało zidentyfikowane i jest nieakceptowalne, organizacje wykorzystują analizę wpływu na bezpieczeństwo do zmiany lub zaplanowania zabezpieczeń i środków zaradczych w celu zmniejszenia ryzyka. Na przykład, jeśli analiza wpływu na bezpieczeństwo ujawnia, że proponowana zmiana powoduje modyfikację typowego bezpiecznego ustawienia konfiguracyjnego, inicjowane są plany przeprojektowania zmiany tak, aby funkcjonowała w ramach istniejącego ustawienia. Jeśli zmiana wiąże się z nowymi zwiększonymi uprawnieniami dla użytkowników, należy opracować plany ograniczenia dodatkowego ryzyka (np. złożenie wniosków o wyższe poziomy uprawnień dla tych użytkowników lub wdrożenie silniejszej kontroli dostępu).

Przykładowy szablon analizy wpływu na bezpieczeństwo znajduje się w Załączniku I.

Etap SDLC: Etap eksploatacji i utrzymania

Główne role: SSO

Role pomocnicze: Osoba autoryzująca (AO); właściciel systemu (SO); Administrator systemu (SA); deweloper systemu/aplikacji

Oczekiwane dane wejściowe: Żądanie zmiany bądź wszelka dokumentacja uzupełniająca; plan bezpieczeństwa systemu, w tym bieżące zatwierdzone konfiguracje bazowe; zapisy z audytu systemu; odpowiednie informacje o podatnościach COTS

Oczekiwane wyniki: Zidentyfikowane podatności; ocena ryzyka zidentyfikowanych podatności, w tym wszelkie potencjalne środki zaradcze; analiza wpływu zmiany na bezpieczeństwo

3.3.4 Rejestrowanie i archiwizowanie

Gdy zmiana została przeanalizowana, zatwierdzona, przetestowana, wdrożona i zweryfikowana, organizacja aktualizuje dokumentację związaną ze zmianą, taką jak dokumentacja techniczna czy konfiguracja bazowa, a także dokumentację związaną

z bezpieczeństwem, taką jak plany bezpieczeństwa systemu, ocena ryzyka, raporty z oceny oraz plany działania i kamienie milowe. W przypadkach, gdy istnieje wysokie ryzyko lub gdy dokonano znacznych zmian, może być wymagana ponowna autoryzacja systemu.

W miarę wprowadzania zmian w konfiguracji bazowej, nowa konfiguracja bazowa staje się bieżącą wersją, a poprzednia traci ważność, ale jest zachowywana do celów historycznych. Jeśli wystąpią problemy z wersją produkcyjną, zachowanie poprzednich wersji pozwala na wycofanie zmian lub przywrócenie do poprzedniej bezpiecznej i funkcjonalnej wersji konfiguracji bazowej. Dodatkowo, archiwizacja poprzednich konfiguracji bazowych jest przydatna do reagowania na incydenty i wspierania identyfikowalności[31] podczas formalnych audytów[32].

Etap SDLC: Etap eksploatacji i utrzymania

Główne role: System Security Officer (SSO)

Role pomocnicze: Właściciel systemu (SO); Administrator systemu (SA); deweloper systemu/aplikacji.

Oczekiwane dane wejściowe: Zidentyfikowane podatności; ocena ryzyka zidentyfikowanych podatności, w tym wszelkie potencjalne środki zaradcze; analiza wpływu zmiany na bezpieczeństwo.

Oczekiwane wyniki: Zaktualizowana dokumentacja techniczna i dokumentacja związana z bezpieczeństwem systemu; decyzja, czy wymagana jest ponowna autoryzacja w systemie nowa konfiguracja bazowa.

3.4 Monitorowanie SecCM

Jeżeli system jest niespójny z zatwierdzonymi konfiguracjami określonymi przez konfiguracje bazowe elementów konfiguracji systemu, plan bezpieczeństwa systemu itp. lub jeśli wykaz komponentów organizacji jest niedokładny, organizacja może być nieświadoma potencjalnych podatności i nie podjąć działań, które w przeciwnym razie ograniczyłyby te podatności i ochroniłyby ją przed atakami (tj. zmniejszyłyby

[31] Identyfikowalność to zdolność do prześledzenia historii, zastosowania lub lokalizacji przedmiotu rozpatrywania w całym jego cyklu życia.

[32] Zarchiwizowane konfiguracje bazowe są chronione zgodnie z poziomem wpływu na system.

ryzyko). Działania monitorujące zapewniają organizacji lepszy wgląd w rzeczywisty stan bezpieczeństwa jej systemów, a także wspierają przestrzeganie polityk i procedur SecCM. Monitorowanie SecCM zapewnia również wkład do ogólnej strategii ciągłego monitorowania organizacji[33].

Organizacje wdrażają strategię monitorowania konfiguracji opracowaną na etapie planowania SecCM. Działania monitorujące SecCM potwierdzają, że istniejąca konfiguracja jest identyczna z bieżącą zatwierdzoną konfiguracją bazową, że wszystkie pozycje w wykazie komponentów mogą być zidentyfikowane i są powiązane z odpowiednim systemem oraz, jeśli to możliwe, sprawdzane jest, czy istnieją jakiekolwiek niezatwierdzone komponenty (tj. nie odnotowane w wykazie komponentów). Niezatwierdzone komponenty często stwarzają poważne zagrożenie dla bezpieczeństwa; rzadko mają zaktualizowane poprawki i nie są skonfigurowane przy użyciu zatwierdzonych konfiguracji bazowych, a także nie są oceniane ani uwzględniane w procesie upoważniania do działania. Na przykład, jeśli technik używa routera do testów, a następnie zapomina go usunąć, lub jeśli pracownik ustawia punkt dostępu bezprzewodowego w „zdalnym biurze" bez zgody kierownictwa, organizacja może stać się podatna na zagrożenia bez świadomości tego faktu.

3.4.1 Ocena i raportowanie

Monitorowanie SecCM odbywa się za pomocą działań oceniających oraz sprawozdawczych. W przypadku organizacji o dużej liczbie komponentów, jedynym praktycznym i skutecznym rozwiązaniem w zakresie działań monitorujących SecCM jest zastosowanie rozwiązań automatycznych, wykorzystujących standardowe metody raportowania, takie jak SCAP. System może mieć wiele komponentów i wiele konfiguracji bazowych. Ręczne zbieranie informacji o konfiguracji wszystkich komponentów i ich ocena względem polityki i zatwierdzonych konfiguracji bazowych jest w większości przypadków niepraktyczne, a nawet niemożliwe. Zautomatyzowane narzędzia mogą również ułatwić raportowanie do systemów typu SIEM, które mogą być dostępne dla kierownictwa bądź sformatowane w postaci innych raportów

[33] Patrz [NSC 800-37] i [NSC 800-137].

dotyczących stanu konfiguracji bazowej w celu wspomagania ogólnego ciągłego monitorowania. Podczas zbierania i analizowania wyników wygenerowanych przez automatyczne narzędzia należy zachować ostrożność, aby uwzględnić wszelkie wyniki fałszywie dodatnie (*ang. false-positive – FP*).

Monitorowanie SecCM może być wspierane na różne sposoby, w tym między innymi poprzez:

- Skanowanie w celu wykrycia komponentów nie ujętych w wykazie. Na przykład gdy po przetestowaniu nowej zapory sieciowej technik zapomniał usunąć ją z sieci. Jeśli jest nieprawidłowo skonfigurowana, może umożliwić dostęp do sieci intruzom. Skanowanie zidentyfikowałoby to urządzenie sieciowe jako nieujęte w wykazie, umożliwiając organizacji podjęcie stosownych działań.
- Skanowanie w celu identyfikacji rozbieżności pomiędzy zatwierdzoną konfiguracją bazową a rzeczywistą konfiguracją systemu. Na przykład technik wprowadził nową poprawkę, ale zapomniał zaktualizować konfiguracje bazowe systemów, na które ta poprawka ma wpływ. Skanowanie pozwoliłoby zidentyfikować różnicę pomiędzy rzeczywistym środowiskiem a opisem w konfiguracji bazowej, co umożliwiłoby organizacji podjęcie stosownych działań. W innym przykładzie nowe narzędzie jest instalowane na stacjach roboczych kilku użytkowników końcowych systemu. Podczas instalacji narzędzie zmienia szereg ustawień konfiguracyjnych w przeglądarce na stacjach roboczych użytkowników, narażając je na atak. Skanowanie zidentyfikowałoby zmianę w konfiguracji stacji roboczej, umożliwiając podjęcie działań przez odpowiednie osoby.
- Wdrożenie zautomatyzowanych narzędzi do monitorowania zmian (np. narzędzia do zarządzania zmianami/konfiguracją, narzędzia do umieszczania aplikacji na białej liście). Nieautoryzowane zmiany w systemach mogą wskazywać, że systemy są atakowane lub że procedury SecCM nie są przestrzegane lub wymagają aktualizacji. Dostępne są zautomatyzowane narzędzia, które monitorują systemy pod kątem zmian i ostrzegają personel systemu w przypadku wystąpienia lub próby wprowadzenia nieautoryzowanych zmian.

- Przeszukiwanie zapisów audytu/monitoringu dzienników w celu identyfikacji nieautoryzowanych zdarzeń związanych ze zmianami.
- Przeprowadzanie kontroli integralności systemu w celu sprawdzenia, czy nie zostały zmienione konfiguracje bazowe.
- Przeglądanie dokumentacji kontroli zmian konfiguracji (w tym analiz wpływu na bezpieczeństwo) w celu weryfikacji zgodności z polityką i procedurami SecCM.

Gdy jest to możliwe, organizacje dążą do normalizacji danych w celu opisania systemu, aby różne dane wyjściowe z monitoringu mogły być łączone, korelowane, analizowane i raportowane w spójny sposób. Protokół SCAP dostarcza wspólnego języka do opisywania podatności na zagrożenia, błędnych konfiguracji oraz produktów i jest oczywistym punktem wyjścia dla organizacji poszukujących spójnego sposobu komunikacji na temat stanu bezpieczeństwa architektury korporacyjnej (patrz podrozdział 3.5).

Gdy w wyniku działań monitorujących zostaną odkryte niespójności, organizacja może podjąć działania zaradcze. Działania mogą być podejmowane metodami ręcznymi lub przy użyciu narzędzi automatycznych. Preferowane są narzędzia automatyczne, ponieważ działania nie zależą od interwencji człowieka i są podejmowane natychmiast po zidentyfikowaniu nieautoryzowanej zmiany. Przykłady możliwych działań:

- wdrażanie nieniszczących działań naprawczych (np. kwarantanna niezarejestrowanych urządzeń, blokowanie niezabezpieczonych protokołów itp.);
- wysłanie alertu ze szczegółami zmian do odpowiednich pracowników za pośrednictwem np. poczty elektronicznej;
- wycofywanie zmian i przywracanie danych z kopii zapasowych;
- aktualizacja wykazu w celu uwzględnienia nowo zidentyfikowanych komponentów;
- aktualizacja konfiguracji bazowych w oparciu o nowe konfiguracje.

Zmiany wykryte w wyniku działań monitorujących są porównywane z zatwierdzonymi zmianami. W szczególności, porównanie polega na wyjaśnieniu następujących kwestii:

- Kto wprowadził zmianę.
- Czy zmiana nastąpiła w zaplanowanym oknie serwisowym.
- Czy zmiana odpowiada wcześniej wykrytej i zatwierdzonej zmianie.
- Czy zmiana odpowiada zatwierdzonemu żądaniu zmiany, zgłoszeniu helpdesk lub wersji produktu.

Dodatkowo, wyniki działań monitorujących są analizowane w celu ustalenia przyczyny (przyczyn), dla których doszło do nieautoryzowanej zmiany. Istnieje wiele potencjalnych przyczyn nieautoryzowanych zmian. Mogą one wynikać z:

- wprowadzenia przypadkowych lub niezamierzonych zmian;
- złośliwych intencji/ataków;
- działań osób, które uważają, że procesy kontroli zmian konfiguracji ich nie dotyczą;
- działań osób, które nie są świadome procesu kontroli zmian konfiguracji;
- błędów popełnianych podczas wdrażania zmian;
- opóźnienia pomiędzy wprowadzeniem zmiany a aktualizacją inwentaryzacji i konfiguracji bazowej dla systemów, których dotyczy zmiana.

Analiza nieautoryzowanych zmian wykrytych przez monitoring może nie tylko zidentyfikować podatności, ale także dać organizacjom wgląd w potencjalne problemy systemowe związane z tym, jak zarządzany jest proces kontroli zmian konfiguracji. Gdy organizacje są świadome istnienia takich problemów, można podjąć działania, takie jak przeprojektowanie procesów, wdrożenie ulepszonych ograniczeń dostępu do zmian oraz zapewnienie szkoleń dotyczących procesów SecCM.

Monitorowanie może również wspomagać generowanie metryk związanych z działaniami SecCM. Analiza i konsolidacja raportów z monitoringu może generować metryki, takie jak procent systemów, które są wdrażane zgodnie z zatwierdzonymi konfiguracjami bazowymi, procent produktów informatycznych, które są skonfigurowane zgodnie z organizacyjnie zdefiniowanymi powszechnymi

bezpiecznymi konfiguracjami, czy procent zmian systemowych, które zostały poddane analizie wpływu na bezpieczeństwo. Tak więc, monitorowanie SecCM może być również źródłem informacji, które wspomagają wymagania metryki związane z ogólnym procesem ciągłego monitorowania organizacji.

Wyniki monitorowania SecCM są raportowane kierownictwu w sposób określony przez politykę organizacyjną i strategię SecCM. Różne rodzaje sprawozdawczości mogą być potrzebne do wspomagania zgodności z obowiązującymi przepisami, rozporządzeniami wykonawczymi, dyrektywami, politykami, przepisami, normami i standardami.

Strategia i procedury monitorowania SecCM są poddawane przeglądowi i rewizji w celu zapewnienia dalszego spełniania organizacyjnych wymogów bezpieczeństwa.

Etap SDLC: Etap eksploatacji i utrzymania.

Główne role: SAISO (odpowiada za wdrażanie narzędzi monitorowania w całej organizacji i nadzorowanie działań monitorujących, które potencjalnie mogą obejmować angażowanie niezależnych zespołów oceniających); właściciel systemu (odpowiada za zapewnienie, że monitorowanie konfiguracji jest wdrożone na poziomie systemu, jak określono w strategii).

Role pomocnicze: System Security Officer (SSO); Administrator systemu (SA); deweloper systemu/oprogramowania.

Oczekiwane dane wejściowe: Strategia monitorowania SecCM; automatyczne narzędzia; wykaz komponentów systemu; bieżące konfiguracje bazowe; zapisy z audytu; plan bezpieczeństwa systemu/wymogi bezpieczeństwa systemu.

Oczekiwane wyniki: Raporty z monitorowania SecCM, w tym raporty z oceny bezpieczeństwa i dane wyjściowe z automatycznych narzędzi, jak określono w strategii i harmonogramie.

3.4.2 Wdrażanie i zarządzanie narzędziami do monitorowania SecCM

Narzędzia monitorowania SecCM zidentyfikowane podczas etapu planowania są wdrażane i zarządzane podczas etapu monitorowania. Niektóre narzędzia mogą wspomagać działania SecCM na wielu etapach, tzn. narzędzia mogą być już wdrożone i wspomagać działania podczas etapu identyfikacji i wdrażania konfiguracji bądź etapu

kontrolowania zmian konfiguracji. Funkcjonalność takich narzędzi związana z monitorowaniem jest następnie wykorzystywana podczas etapu monitorowania.

Przed wdrożeniem automatycznych narzędzi monitorujących organizacje przeprowadzają analizę wpływu na bezpieczeństwo, aby się upewnić, że narzędzia nie będą miały negatywnego wpływu na istniejącą architekturę organizacji jako całości ani na poszczególne systemy/komponenty.

Należy pamiętać, że automatyczne narzędzia mogą nie obsługiwać wszystkich systemów organizacyjnych lub komponentów w ramach systemu lub nie być w stanie z nimi działać. Organizacje dokumentują systemy bądź komponenty, które nie są monitorowane za pomocą narzędzi automatycznych, a dla tych systemów/ komponentów opracowywany i wdrażany jest proces ręczny.

Etap SDLC: Etap wdrażania.

Główne role: Menadżer programu SecCM; właściciel systemu (SO).

Role pomocnicze: SAISO (jeśli nie jest menadżerem programu SecCM); CIO (dyrektor ds. informacji); Osoba autoryzująca (AO); System Security Officer (SSO); Administrator systemu (SA); deweloper systemu/aplikacji.

Oczekiwane dane wejściowe: Strategia monitorowania konfiguracji; informacje o architekturze organizacji bądź architekturze systemu; narzędzia zidentyfikowane podczas etapu planowania, informacje o innych produktach informatycznych, z którymi narzędzia monitorujące będą współdziałać.

Oczekiwane wyniki: Wdrożone narzędzia do monitorowania konfiguracji.

3.5 Wykorzystanie protokołu SCAP[34]

Protokół SCAP (ang. *Security Content Automation Protocol – SCAP*) to zestaw specyfikacji[35], które standaryzują format i nomenklaturę, za pomocą której można przekazywać informacje o błędach w oprogramowaniu i bezpiecznych konfiguracjach.

[34] NIST [SP 800-126] zawiera informacje na temat automatycznego protokołu zabezpieczeń zawartości.

[35] Oczekuje się, że z czasem zostaną dodane lub zaktualizowane specyfikacje SCAP. Aktualizacje można sprawdź na stronie https://scap.nist.gov/.

Narzędzia z obsługą SCAP mogą być wykorzystywane do utrzymywania bezpieczeństwa systemów organizacji, np. do automatycznego weryfikowania instalacji poprawek, sprawdzania ustawień konfiguracyjnych bezpieczeństwa systemu w stosunku do oczekiwanego poziomu bazowego oraz badania systemów pod kątem oznak naruszeń bezpieczeństwa.

W celu zautomatyzowania zarządzania konfiguracją i utworzenia dowodów oceny dla zabezpieczeń zawartych w [NSC 800-53], organizacje mogą korzystać z narzędzi obsługujących protokół SCAP w połączeniu z listami kontrolnymi przygotowanymi zgodnie z protokołem SCAP. Listy kontrolne przygotowane zgodnie z protokołem SCAP są dostosowywane w zależności od potrzeb do specyficznych wymagań organizacyjnych. Listy kontrolne przygotowane zgodnie z protokołem SCAP mogą mapować poszczególne ustawienia konfiguracji systemu do odpowiadających im wymagań bezpieczeństwa. Mapowanie ustawień i wymagań może pomóc w wykazaniu, że wdrożone ustawienia są zgodne z tymi wymaganiami. Mapowania osadzone w listach kontrolnych przygotowanych zgodnie z protokołem SCAP pozwalają narzędziom obsługującym protokół SCAP na automatyczne generowanie standardowych dowodów oceny i zgodności. Wbudowane mapowania w narzędziach obsługujących protokół SCAP mogą zapewnić znaczne oszczędności pracy i pieniędzy.

Zachęcamy producentów oprogramowania zabezpieczającego do włączenia obsługi znaczników Common Vulnerabilities and Exposures (CVE), Common Configuration Enumeration (CCE) oraz znaczników Software Identification (SWID) do swoich produktów. Ponadto zachęcamy wszystkich producentów oprogramowania do włączenia identyfikatorów CVE i CCE oraz identyfikatorów oprogramowania dostarczanych przez Common Platform Enumeration (CPE) i SWID do swoich porad dotyczących podatności na zagrożenia i stosowania poprawek.

KOMPONENTY SCAP WERSJA 1.3[36]

SPECYFIKACJE	OPIS ORYGINALNY (TŁUMACZONY DOSŁOWNIE)	NOWA POLSKA DEFINICJA
Języki		
Extensible Configuration Checklist Description Format (XCCDF) 1.2	Używany do tworzenia list kontrolnych/wzorców bezpieczeństwa oraz do raportowania wyników ich oceny.	Język wykorzystywany w celu budowy list kontrolnych SCAP oraz modeli zabezpieczeń, a także zgłaszania rezultatów przeprowadzonych ocen.
Open Vulnerability and Assessment Language (OVAL) 5.11.2	Używany do reprezentowania informacji o konfiguracji systemu, oceny stanu urządzenia i raportowania wyników oceny.	Język wykorzystywany w celu przedstawiania informacji na temat konfiguracji systemu, oceny stanu urządzenia oraz przekazywania jej wyników.
Open Checklist Interactive Language (OCIL) 2.0	Służy do przedstawiania informacji o konfiguracji systemu, oceny stanu urządzenia i raportowania wyników oceny.	Język stosowany w celu opisywania wyników testów, które obejmują gromadzenie danych od osób lub pobieranie ich z istniejących magazynów danych utworzonych w oparciu o inne metody gromadzenia danych.

[36] Informacje w tabeli pochodzą z dokumentu NIST [SP 800-126], wer. 3, rozdział 2. Oczekuje się dodania dodatkowych specyfikacji SCAP. Aktualizacje można sprawdzić na stronie https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol/SCAP-Releases.

SPECYFIKACJE	OPIS ORYGINALNY (TŁUMACZONY DOSŁOWNIE)	NOWA POLSKA DEFINICJA
Formaty raportowania		
Asset Reporting Format (ARF) 1.1	Używany do wyrażania informacji o aktywach oraz do definiowania relacji pomiędzy aktywami i raportami	Format wykorzystywany w celu gromadzenia informacji o zasobach oraz określania relacji pomiędzy poszczególnymi zasobami i opracowanymi raportami.
Asset Identification 1.1	Używany do jednoznacznej identyfikacji aktywów na podstawie znanych identyfikatorów i innych informacji o aktywach.	Format wykorzystywany w celu zapewnienia jednoznacznej identyfikacji zasobów na podstawie znanych identyfikatorów i innych dostępnych danych.
Systemy identyfikacji		
Common Platform Enumeration (CPE) 2.3	Nazewnictwo i słownik dotyczące sprzętu, systemów operacyjnych i aplikacji; metoda określania możliwości zastosowania do platform.	Zbiór pojęć oraz definicji dotyczących urządzeń, systemów operacyjnych i aplikacji, pozwalający na ustalenie, czy mają one zastosowanie do poszczególnych platform.
Znaczniki Software Identification (SWID) 2015	Ustrukturyzowany format metadanych do opisu opublikowanego produktu oprogramowania.	Format obejmujący ustrukturyzowane metadane opisujące wydane aplikacje i oprogramowanie.
Common Configuration Enumeration (CCE) 5	Nazewnictwo i słownik konfiguracji bezpieczeństwa oprogramowania.	Zbiór pojęć oraz definicji dotyczących zabezpieczeń oprogramowania.

SPECYFIKACJE	OPIS ORYGINALNY (TŁUMACZONY DOSŁOWNIE)	NOWA POLSKA DEFINICJA
Common Vulnerabilities and Exposures (CVE)	Nazewnictwo i słownik błędów oprogramowania związanych z bezpieczeństwem.	Zbiór pojęć oraz definicji dotyczących błędów i luk w zabezpieczeniach oprogramowania.
Systemy pomiaru i oceny		
Common Vulnerability Scoring System (CVSS) 3	Używany do pomiaru względnej istotności usterek oprogramowania.	System pomiaru i oceny wykorzystywany w celu określenia istotności oraz możliwego wpływu usterek oprogramowania.
Common Configuration Scoring System (CCSS) 1.0	Używany do pomiaru względnej istotności problemów z (błędną) konfiguracją zabezpieczeń urządzeń.	System pomiaru i oceny wykorzystywany w celu określenia potencjalnego wpływu błędów w konfiguracji zabezpieczeń urządzeń.
Integralność zawartości i wyników		
Trust Model for Security Automation Data (TMSAD) 1.0	Wytyczne dotyczące stosowania podpisów cyfrowych we wspólnym modelu zaufania stosowanym w specyfikacjach automatyzacji zabezpieczeń.	Wytyczne na temat wykorzystywania podpisów cyfrowych na potrzeby stosowania wspólnych modeli zaufania stosowanych w ramach specyfikacji związanych z automatyzacją zabezpieczeń.

ZAŁĄCZNIK A – REFERENCJE

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[37]	
NSC 199	Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199
NSC 200	Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych – na podstawie FIPS 200
NSC 800-30	Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne – na podstawie NIST SP 800-30
NSC 800-34	Poradnik planowania awaryjnego – na podstawie NIST SP 800-34
NSC 800-37	Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu – na podstawie NIST SP 800-37
NSC 800-39	Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego – na podstawie NIST SP 800-39
NSC 800-53	Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53
NSC 800-53A	Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informacyjnych oraz organizacji. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A
NSC 800-53B	Konfiguracje bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B

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

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[37]	
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[38]	
[40 USC 11331]	Title 40 U.S. Code, Sec. 11331, Responsibilities for Federal information systems standards. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017 - title40/USCODE- 2017-title40-subtitleIII-chap113-subchapIII-sec11331
[44 USC 3502]	Title 44 U.S. Code, Sec. 3502, Definitions. 2012 ed. https://www.govinfo.gov/app/details/USCODE-2017 - title44/USCODE- 2017-title44-chap35-subchapI-sec3502
[44 USC 3542]	Title 44 U.S. Code, Sec. 3542, Definitions. 2006 ed. https://www.govinfo.gov/app/details/USCODE-2008- title44/USCODE-2008-title44-chap35-subchapIII-sec3542
[44 USC 3544]	Title 44 U.S. Code, Sec. 3544, Definitions. 2006 ed. https://www.govinfo.gov/app/details/USCODE-2008- title44/USCODE-2008-title44-chap35-subchapIII-sec3544
[44 USC 3552]	Title 44 U.S. Code, Sec. 3552, Definitions. 2012 ed. https://www.govinfo.gov/app/details/USCODE-2017 - title44/USCODE- 2017-title44-chap35-subchapII-sec3552
[44 USC 3601]	Title 44 U.S. Code, Sec. 3601, Definitions. 2012 ed. https://www.govinfo.gov/app/details/USCODE-2017 - title44/USCODE- 2017-title44-chap36-sec3601
[CMMI]	Capability Maturity Model Integration (CMMI). https://cmmiinstitute.com/
[CNSS 4009]	Committee for National Security Systems (CNSS) Instruction 4009, Committee on National Security systems (CNSS) Glossary, April 2015. https: //www.cnss.gov/CNS S/issuances/Instructions.cfm
[FIPS 140-3]	National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 140-3. https://doi.org/10.6028/NIST.FIPS.140-3

[38] Publikacje angielski zostały podane w celach uzupełniających dla osób zainteresowanych.

Tłumaczenie

[FIPS 199]	National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199
[FIPS 200]	National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 200. https://doi.org/10.6028/NIST.FIPS.200
[FISMA]	Federal Information Security Modernization Act (P.L. 113-283), December 2014. https://www.govinfo.gov/app/details/PLAW-113publ283
[IEEE 828-2012]	IEEE 828-2012-IEEE Standard for Configuration Management in Software and Software Engineering. https://standards.ieee.org/standard/828-2012.html
[ISO 10007]	International Organization for Standardization (ISO) 10007:2017, Quality management - Guidelines for configuration management. https://www.iso.org/standard/70400.html
[ITIL]	Information Technology Infrastructure Library (ITIL). https://www.axelos.com/best-practice-solutions/itil
[NISTIR 7693]	Wunder J, Halbardier AM, Waltermire DA (2011) Specification for Asset Identification 1.1. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7693. https://doi.org/10.6028/NIST.IR.7693
[OMB A-130]	Office of Management and Budget Circular A-130, Managing Information as a Strategic Resource, July 2016. https://www.whitehouse.goV/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf
[SP 800-18]	Swanson MA, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-18, Rev. 1. https://doi.org/10.6028/NIST.SP.800-18r1

[SP 800-25]	Lyons-Burke K, Committee FPKIS (2000) Federal Agency Use of Public Key Technology for Digital Signatures and Authentication. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-25. https://doi.org/10.6028/NIST.SP.800-25
[SP 800-28]	Jansen W, Winograd T, Scarfone KA (2008) Guidelines on Active Content and Mobile Code. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-28, Version 2. https://doi.org/10.6028/NIST.SP.800-28ver2
[SP 800-30]	Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1
[SP 800-32]	Kuhn R, Hu VC, Polk T, Chang S-jH (2001) Introduction to Public Key Technology and the Federal PKI Infrastructure. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-32. https://doi.org/10.6028/NIST.SP.800-32
[SP 800-37]	Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2
[SP 800-39]	Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39
[SP 800-40]	Souppaya MP, Scarfone KA (2013) Guide to Enterprise Patch Management Technologies. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-40, Rev. 3. https://doi.org/10.6028/NIST.SP.800-40r3

[SP 800-41]	Scarfone KA, Hoffman P (2009) Guidelines on Firewalls and Firewall Policy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-41, Rev. 1. https://doi.org/10.6028/NIST.SP.800-41r1
[SP 800-44]	Tracy MC, Jansen W, Scarfone KA, Winograd T (2007) Guidelines on Securing Public Web Servers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-44, Version 2. https://doi.org/10.6028/NIST.SP.800-44ver2
[SP 800-45]	Tracy MC, Jansen W, Scarfone KA, Butterfield J (2007) Guidelines on Electronic Mail Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-45, Version 2. https://doi.org/10.6028/NIST.SP.800-45ver2
[SP 800-46]	Souppaya MP, Scarfone KA (2016) Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-46, Rev. 2. https://doi.org/10.6028/NIST.SP.800-46r2
[SP 800-47]	Grance T, Hash J, Peck S, Smith J, Korow-Diks K (2002) Security Guide for Interconnecting Information Technology Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-47. https://doi.org/10.6028/NIST.SP.800- 47
[SP 800-52]	Polk T, McKay KA, Chokhani S (2014) Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-52, Rev. 1. https://doi.org/10.6028/NIST.SP.800-52r1
[SP 800-53]	Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4

[SP 800-53A]	Joint Task Force Transformation Initiative (2014) Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 4, Includes updates as of December 18, 2014. https://doi.org/10.6028/NIST.SP.800-53Ar4
[SP 800-54]	Kuhn R, Sriram K, Montgomery DC (2007) Border Gateway Protocol Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-54. https://doi.org/10.6028/NIST.SP.800-54
[SP 800-55]	Chew E, Swanson MA, Stine KM, Bartol N, Brown A, Robinson W (2008) Performance Measurement Guide for Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-55, Rev. 1. https://doi.org/10.6028/NIST.SP.800-55r1
[SP 800-57P1]	Barker EB (2016) Recommendation for Key Management, Part 1: General. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 1, Rev. 4. https://doi.org/10.6028/NIST.SP.800-57pt1r4
[SP 800-57P2]	Barker EB, Barker WC (2019) Recommendation for Key Management: Part 2 - Best Practices for Key Management Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-57pt2r1
[SP 800-57P3]	Barker EB, Dang QH (2015) Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 3, Rev. 1. https://doi.org/10.6028/NIST.SP.800-57pt3r1
[SP 800-58]	Kuhn R, Walsh TJ, Fries S (2005) Security Considerations for Voice Over IP Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-58. https://doi.org/10.6028/NIST.SP.800-58

[SP 800-63B]	Grassi PA, Newton EM, Perlner RA, Regenscheid AR, Fenton JL, Burr WE, Richer JP, Lefkovitz NB, Danker JM, Choong Y-Y, Greene KK, Theofanos MF (2017) Digital Identity Guidelines: Authentication and Lifecycle Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800- 63B, Includes updates as of December 1, 2017. https://doi.org/10.6028/NIST.SP.800-63B
[SP 800-70]	Quinn SD, Souppaya MP, Cook MR, Scarfone KA (2018) National Checklist Program for IT Products: Guidelines for Checklist Users and Developers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-70, Rev. 4. https://doi.org/10.6028/NIST.SP.800-70r4
[SP 800-77]	Frankel SE, Kent K, Lewkowski R, Orebaugh AD, Ritchey RW, Sharma SR (2005) Guide to IPsec VPNs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-77. https://doi.org/10.6028/NIST.SP.800-77
[SP 800-81-2]	Chandramouli R, Rose SW (2013) Secure Domain Name System (DNS) Deployment Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-81-2. https://doi.org/10.6028/NIST.SP.800-81-2
[SP 800-82]	Stouffer KA, Lightman S, Pillitteri VY, Abrams M, Hahn A (2015) Guide to Industrial Control Systems (ICS) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-82, Rev. 2. https://doi.org/10.6028/NIST.SP.800- 82r2
[SP 800-92]	Kent K, Souppaya MP (2006) Guide to Computer Security Log Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-92. https://doi.org/10.6028/NIST.SP.800-92
[SP 800-94]	Scarfone KA, Mell PM (2007) Guide to Intrusion Detection and Prevention Systems (IDPS). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-94. https://doi.org/10.6028/NIST.SP.800-94

[SP 800-95]	Singhal A, Winograd T, Scarfone KA (2007) Guide to Secure Web Services. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-95. https://doi.org/10.6028/NIST.SP.800-95
[SP 800-97]	Frankel SE, Eydt B, Owens L, Scarfone KA (2007) Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-97. https://doi.org/10.6028/NIST.SP.800-97
[SP 800-98]	Karygiannis T, Eydt B, Barber G, Bunn L, Phillips T (2007) Guidelines for Securing Radio Frequency Identification (RFID) Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-98. https://doi.org/10.6028/NIST.SP.800- 98
[SP 800-107]	Dang QH (2012) Recommendation for Applications Using Approved Hash Algorithms. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-107, Rev. 1. https://doi.org/10.6028/NIST.SP.800-107r1
[SP 800-111]	Scarfone KA, Souppaya MP, Sexton M (2007) Guide to Storage Encryption Technologies for End User Devices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-111. https://doi.org/10.6028/NIST.SP.800-111
[SP 800-113]	Frankel SE, Hoffman P, Orebaugh AD, Park R (2008) Guide to SSL VPNs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-113. https://doi.org/10.6028/NIST.SP.800-113
[SP 800-115]	Scarfone KA, Souppaya MP, Cody A, Orebaugh AD (2008) Technical Guide to Information Security Testing and Assessment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-115. https://doi.org/10.6028/NIST.SP.800- 115
[SP 800-121]	Padgette J, Bahr J, Holtmann M, Batra M, Chen L, Smithbey R, Scarfone KA (2017) Guide to Bluetooth Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-121, Rev. 2. https://doi.org/10.6028/NIST.SP.800- 121r2

[SP 800-122]	McCallister E, Grance T, Scarfone KA (2010) Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-122. https://doi.org/10.6028/NIST.SP.800- 122
[SP 800-123]	Scarfone KA, Jansen W, Tracy MC (2008) Guide to General Server Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-123. https://doi.org/10.6028/NIST.SP.800-123
[SP 800-124]	Souppaya MP, Scarfone KA (2013) Guidelines for Managing the Security of Mobile Devices in the Enterprise. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-124, Rev. 1. https://doi.org/10.6028/NIST.SP.800- 124r1
[SP 800-126]	Waltermire DA, Quinn SD, Booth H, III, Scarfone KA, Prisaca D (2018) The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-126, Rev. 3. https://doi.org/10.6028/NIST.SP.800-126r3
[SP 800-130]	Barker EB, Smid ME, Branstad DK, Chokhani S (2013) A Framework for Designing Cryptographic Key Management Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-130. https://doi.org/10.6028/NIST.SP.800- 130
[SP 800-131A]	Barker EB, Roginsky A (2019) Transitioning the Use of Cryptographic Algorithms and Key Lengths. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-131A, Rev. 2. https://doi.org/10.6028/NIST.SP.800-131Ar2
[SP 800-132]	Sonmez Turan M, Barker EB, Burr WE, Chen L (2010) Recommendation for Password-Based Key Derivation: Part 1: Storage Applications. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-132. https://doi.org/10.6028/NIST.SP.800-132

[SP 800-135]	Dang QH (2011) Recommendation for Existing Application-Specific Key Derivation Functions. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-135, Rev. 1. https://doi.org/10.6028/NIST.SP.800-135r1
[SP 800-137]	Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh AD, Scholl MA, Stine KM (2011) Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-137. https://doi.org/10.6028/NIST.SP.800-137
[SP 800-161]	Boyens JM, Paulsen C, Moorthy R, Bartol N (2015) Supply Chain Risk Management Practices for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161. https://doi.org/10.6028/NIST.SP.800-161
[SP 800-167]	Sedgewick A, Souppaya MP, Scarfone KA (2015) Guide to Application Whitelisting. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-167. https://doi.org/10.6028/NIST.SP.800-167
[SP 800-171]	Ross RS, Dempsey KL, Viscuso P, Riddle M, Guissanie G (2016) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171, Rev. 1, Includes updates as of June 7, 2018. https://doi.org/10.6028/NIST.SP.800-171r1
[SP 800-171A]	Ross RS, Dempsey KL, Pillitteri VY (2018) Assessing Security Requirements for Controlled Unclassified Information. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171A. https://doi.org/10.6028/NIST.SP.800-171A

[SP 800-175B]	Barker EB (2016) Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-175B. https://doi.org/10.6028/NIST.SP.800-175B
[SP 800-179]	Trapnell M, Scarfone KA, Trapnell E, Badger ML, Souppaya MP, Yaga DJ (2016) Guide to Securing Apple OS X 10.10 Systems for IT Professionals: A NIST Security Configuration Checklist. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-179. https://doi.org/10.6028/NIST.SP.800- 179
[SP 800-181]	Newhouse WD, Witte GA, Scribner B, Keith S (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181. https://doi.org/10.6028/NIST.SP.800-181

ZAŁĄCZNIK B – SŁOWNIK

POWSZECHNE TERMINY I DEFINICJE

Załącznik B zawiera definicje pojęć z zakresu bezpieczeństwa, stosowane w publikacji NIST SP 800-128_wer. 1.0_PL. O ile nie zostały one wyraźnie zdefiniowane w niniejszym słowniku, wszystkie terminy użyte w niniejszej publikacji są zgodne z tymi definicjami oraz z definicjami zawartymi w [CNSS 4009], *National Information Assurance (IA) Glossary*.

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

Terminologia angielska	Terminologia polska	Definicja
adequate security [OMB A-130]	adekwatny poziom bezpieczeństwa	Bezpieczeństwo współmierne do ryzyka wynikającego z utraty, niewłaściwego użycia lub nieautoryzowanego dostępu do informacji lub ich modyfikacji. Obejmuje to zapewnienie, aby informacje przechowywane w imieniu organizacji oraz systemy i aplikacje informatyczne wykorzystywane przez organizację działały skutecznie i zapewniały odpowiednią ochronę poufności, integralności i dostępności poprzez zastosowanie opłacalnych środków bezpieczeństwa.
agency [OMB A-130]	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
asset identification	identyfikacja zasobów	Mechanizmy SCAP pozwalające na jednoznaczne określenie zasobów (komponentów) w oparciu o znane identyfikatory bądź dostępne informacje na ich temat.
asset reporting format (ARF)	format raportowania o aktywach (ARF)	Model danych wykorzystywany w ramach protokołu SCAP umożliwiający przenoszenie informacji o zasobach (komponentach) oraz relacjach pomiędzy poszczególnymi zasobami i raportami na ich temat.
authentication [FIPS 200]	uwierzytelnienie	Proces weryfikacji tożsamości lub innych atrybutów zgłaszanych przez podmiot lub przejętych od podmiotu (użytkownika, procesu lub urządzenia) albo sprawdzenie źródła i integralności danych. Synonim: Ustalanie tożsamości (*ang. Authenticate*)
authorizing official [OMB A-130]	osoba autoryzująca	Osoba lub komórka organizacyjna upoważniona do formalnego przejęcia odpowiedzialności za prowadzenie systemu informatycznego na akceptowalnym poziomie ryzyka dla operacji organizacji (w tym misji, funkcji, wizerunku lub reputacji), aktywów organizacji lub osób fizycznych. Synonim: Organ akredytacyjny (*ang. Accrediting Authority*)

Terminologia angielska	Terminologia polska	Definicja
baseline configuration	konfiguracja bazowa	Udokumentowany zestaw specyfikacji dla systemu lub elementu konfiguracji w ramach systemu, który został formalnie przejrzany i uzgodniony, i który może być zmieniony tylko po przeprowadzeniu procesu kontroli zmian.
checksum [CNSSI-4009]	suma kontrolna	Wartość obliczona na podstawie danych w celu wykrycia błędu lub manipulacji.
chief information officer [OMB A-130]	-----	Kluczowa osoba w jednostce organizacyjnej odpowiedzialna za technologie informacyjne, zwykle członek kierownictwa jednostki organizacyjnej.
common configuration enumeration (CCE)	-----	Specyfikacja w ramach protokołu SCAP, która zapewnia wyjątkowe, wspólne identyfikatory dla ustawień konfiguracyjnych występujących w szerokiej gamie produktów sprzętowych i programowych[39].
common configuration scoring system (CCSS)	-----	Specyfikacja w ramach protokołu SCAP pozwalająca na określenie stopnia istotności problemów z konfiguracją bezpieczeństwa oprogramowania.
common platform enumeration (CPE)	-----	Specyfikacja w ramach protokołu SCAP, która zapewnia standardową konwencję nazewnictwa dla systemów operacyjnych, sprzętu i aplikacji w celu zapewnienia spójnych, łatwych do analizowania nazw, które mogą być wykorzystywane przez wiele podmiotów i rozwiązań w celu odniesienia się do tego samego rodzaju platformy[40].

[39] Specyfikacja CCE jest utrzymywana przez NIST, zobacz https://csrc.nist.gov/projects/scap/specs/cce.

[40] NIST hostuje specyfikację CPE i utrzymuje oficjalny słownik CPE. Więcej informacji na temat CPE

Terminologia angielska	Terminologia polska	Definicja
common secure configuration	typowa bezpieczna konfiguracja	Uznany, znormalizowany i ustalony wzorzec (np. National Checklist Program, metodyki DISA STIG, CIS Benchmarks itp.), który określa konkretne ustawienia bezpiecznej konfiguracji dla danej platformy IT.
common vulnerabilities and exposures (CVE)	–––––	Specyfikacja w ramach protokołu SCAP, która zapewnia nadawanie wyjątkowych, powszechnie stosowanych nazw publicznie ujawnionych podatności systemów informatycznych na zagrożenia[41].
common vulnerability scoring system (CVSS)	–––––	Specyfikacja w ramach protokołu SCAP, która zapewnia otwarte ramy pozwalające na udostępnianie informacji dotyczących cech podatności oprogramowania oraz do obliczania ich względnej istotności[42].
component	komponent	Patrz *komponent systemu*.
configuration	konfiguracja	Możliwe warunki, parametry i specyfikacje, za pomocą których można opisać lub zorganizować system informacyjny lub element systemu.
configuration baseline	konfiguracja bazowa	Patrz: *konfiguracja bazowa*.

oraz oficjalny słownik CPE są dostępne na stronie https://csrc.nist.gov/projects/scap/specs/cpe.

41 Specyfikacja CVE jest utrzymywana przez MITRE, patrz https://cve.mitre.org/.

42 Specyfikacja CVSS jest utrzymywana przez forum zespołów reagowania na incydenty bezpieczeństwa (*ang. Forum of Incident Response and Security Teams – FIRST*), patrz https://www.first.org/cvss/.

Tłumaczenie

Terminologia angielska	Terminologia polska	Definicja
configuration control [CNSSI-4009]	Zabezpieczenia konfiguracyjne	Proces modyfikacji sprzętu, firmware, oprogramowania i jej dokumentowania w celu zabezpieczenia systemu informatycznego przed niewłaściwymi modyfikacjami przed, w trakcie i po wdrożeniu systemu (hardening).
configuration control board [CNSSI-4009]	zespół ds. zabezpieczeń konfiguracyjnych	Grupa wykwalifikowanych osób odpowiedzialnych za proces weryfikacji i zatwierdzania zmian sprzętu, oprogramowania układowego, oprogramowania i dokumentacji w całym cyklu rozwoju i życia operacyjnego systemu informacyjnego.
configuration item	element konfiguracji	Zbiór komponentów systemu informatycznego, które zostały wybrane na potrzeby procesu zarządzania konfiguracją i są klasyfikowane jako pojedynczy obiekt w procesie zarządzania konfiguracją.
configuration management	zarządzanie konfiguracją	Zbiór działań ukierunkowanych na ustanowienie i utrzymanie integralności produktów i systemów informatycznych, poprzez kontrolę procesów inicjowania, zmiany i monitorowania konfiguracji tych produktów i systemów w całym cyklu życia systemu.
configuration management plan	plan zarządzania konfiguracją	Kompleksowy opis ról, odpowiedzialności, zasad i procedur, które mają zastosowanie w ramach procesu zarządzania konfiguracją produktów i systemów.

Terminologia angielska	Terminologia polska	Definicja
configuration settings	ustawienia konfiguracyjne	Zestaw parametrów, które mogą być zmieniane w sprzęcie, aplikacjach lub oprogramowaniu układowym, które mają wpływ na bezpieczeństwo i/lub funkcjonalność systemu.
end-point protection platform	platforma ochrony punktów końcowych	Zabezpieczenia realizowane za pośrednictwem oprogramowania chroniącego komputery użytkowników końcowych, w tym stacje robocze i laptopy, przed atakami (na przykład oprogramowanie antywirusowe, zabezpieczające przed oprogramowaniem szpiegującym i adware, osobiste zapory ogniowe, systemy wykrywania i zapobiegania włamaniom działające na urządzeniu końcowym itp.)
enterprise architecture [44 USC 3601]	architektura korporacyjna	Opis systemów informacyjnych organizacji obejmujący konfigurację systemów, ich integrację, połączenie ze środowiskiem zewnętrznym, rolę we wspieraniu misji organizacji, zadania związane z zapewnieniem bezpieczeństwa.
executive agency [OMB A-130]	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

Terminologia angielska	Terminologia polska	Definicja
		wchodzące w skład Sił Zbrojnych RP, a także spółki państwowe oraz spółki z udziałem Skarbu Państwa.
extensible configuration checklist description format (XCCDF)	–––––	Język wykorzystywany w ramach protokołu SCAP w celu określania list kontrolnych i raportowania wyników ich weryfikacji.
federal information system [40 USC 11331]	rządowy system informacyjny	System informacyjny wykorzystywany lub obsługiwany przez agencję wykonawczą, przez kontrahenta agencji wykonawczej lub przez inną organizację w imieniu agencji wykonawczej.
host-based intrusion detection and prevention system [SP 800-94]	system wykrywania naruszeń i zapobiegania włamaniom oparty na hoście	Program, który monitoruje cechy pojedynczego hosta oraz zdarzenia zachodzące w obrębie tego hosta w celu identyfikacji i zatrzymania podejrzanej aktywności.
incident [44 USC 3552]	incydent	Zdarzenie, które faktycznie lub potencjalnie zagraża poufności, integralności lub dostępności systemu informatycznego lub informacji, które system przetwarza, przechowuje lub przesyła, a także zdarzenie, które stanowi naruszenie lub bezpośrednie zagrożenie naruszenia zasad bezpieczeństwa, procedur bezpieczeństwa lub zasad dopuszczalnego użytkowania. Synonim: • Incydent bezpieczeństwa informatycznego (*ang. Computer Security Incident*)

Terminologia angielska	Terminologia polska	Definicja
		• Incydent bezpieczeństwa (*ang. Security Incident*)
information resources [44 USC 3502]	zasoby informatyczne	Informacja i powiązane z nią zasoby takie jak nośniki, osoby, wyposażenie, fundusze i technologie informatyczne.
information security [44 USC 3552]	bezpieczeństwo informacji[	Ochrona informacji i systemów informatycznych przed nieuprawnionym dostępem, wykorzystaniem, ujawnieniem, uszkodzeniem, modyfikacją i zniszczeniem, w celu zapewnienia poufności, integralności i dostępności. Patrz: Bezpieczeństwo systemów informatycznych (ang. Information Systems Security)
information system [44 USC 3502]	system informatyczny (system teleinformatyczny / system informacyjny)	Określony zestaw zasobów utworzonych w celu gromadzenia, przetwarzania, konserwacji, użytkowania, udostępniania, rozpowszechniania lub usuwania informacji. Synonim: System (*ang. System*)
information system component	komponenty systemu informacyjnego	Obejmują sprzęt, oprogramowanie lub elementy oprogramowania układowego (np. Voice over Internet Protocol, kod mobilny, kopiarki cyfrowe, drukarki, skanery, urządzenia optyczne, technologie bezprzewodowe, urządzenia mobilne). Synonim: Produkt systemu informatycznego (*ang. Information Technology Product*)

Terminologia angielska	Terminologia polska	Definicja
information system component inventory	wykaz komponentów systemu informacyjnego	Opisowy wykaz komponentów wchodzących w skład systemu informatycznego.
information system security plan [OMB A-130]	plan bezpieczeństwa systemu informacyjnego	Formalny dokument, zawierający zestawienie wymogów dotyczących bezpieczeństwa systemu informatycznego oraz opis istniejących lub planowanych zabezpieczeń mających na celu spełnienie tych wymogów.
information technology [OMB A-130]	technologia informacyjna	Dowolny sprzęt lub połączony system lub podsystem sprzętu, wykorzystywany do automatycznego pozyskiwania, przechowywania, modyfikacji, zarządzania, przemieszczania, kontroli, wyświetlania, przełączania, wymiany, transmisji lub odbioru danych lub informacji przez organizację. W rozumieniu poprzedniego zdania, sprzęt jest wykorzystywany przez organizację, jeżeli sprzęt jest używany przez organizację lub jest wykorzystywany przez jej podwykonawcę na podstawie umowy z podwykonawcą, która: (I) wymaga użycia takiego sprzętu; lub (II) w znacznym stopniu wymaga użycia takiego sprzętu do wykonania usługi lub dostarczenia produktu. Pojęcie techniki informacyjnej obejmuje komputery, sprzęt pomocniczy, oprogramowanie (software), oprogramowanie układowe (firmware) i podobne procedury, usługi (w tym usługi wsparcia) i powiązane zasoby.

Terminologia angielska	Terminologia polska	Definicja
information technology product	komponent systemu informacyjnego	Dający się wyróżnić składnik zasobów technologii informacyjnych (np. sprzęt, oprogramowanie, oprogramowanie układowe), który stanowi element architektury systemu informacyjnego. Synonim: Komponent systemu (*ang. System Component*)
malicious code [SP 800-53]	kod złośliwy [SP 800-53]	Oprogramowanie lub firmware celowo stworzone do nieuprawnionych działań w systemie informacyjnym mających szkodliwy wpływ na bezpieczeństwo informacji lub systemu. Zalicza się do niego wirusy, robaki, konie trojańskie, a także inne rodzaje kodu, które infekują hosty systemu. Oprogramowanie szpiegujące oraz pewne formy adware także są zaliczane do oprogramowania złośliwego.
malware	oprogramowanie złośliwe	Łącznie: kod złośliwy, złośliwe aplety, złośliwa logika. Synonim: • Kod złośliwy (*ang. Malicious code*) • Szkodliwa logika (*ang. Malicious logic*)
media [FIPS 200]	nośniki	Urządzenia fizyczne, w tym między innymi taśmy magnetyczne, dyski optyczne, dyski magnetyczne, układy pamięci integracji dużej skali (ang. Large-Scale Integration - LSI), wydruki (ale nie zawierające nośników ekranu), na których informacje są rejestrowane, przechowywane lub drukowane w systemie informacyjnym.

Terminologia angielska	Terminologia polska	Definicja
media library	biblioteka nośników	Miejsce przechowywania, zabezpieczania i sprawdzania wszystkich autoryzowanych wersji elementów konfiguracji nośników.
misconfiguration	błędna konfiguracja	Nieprawidłowa lub nieoptymalna konfiguracja systemu informacyjnego lub komponentu systemu, która może prowadzić do powstania podatności.
mobile code [SP 800-53]	kod mobilny	Program lub jego część otrzymywane z zewnętrznego systemu informacyjnego, transmitowane poprzez sieć komputerową i wykonywane w systemie lokalnym bez wcześniejszej instalacji lub polecenia wykonania po stronie odbiorczej.
network-based intrusion detection and prevention system [SP 800-94]	sieciowy system wykrywania włamań i zapobiegania im	System wykrywania włamań i zapobiegania im, który monitoruje ruch sieciowy dla poszczególnych segmentów sieci lub urządzeń i analizuje aktywność protokołu sieciowego i aplikacyjnego w celu identyfikacji i zatrzymania podejrzanej aktywności.
Open Checklist Interactive Language (OCIL)	–––––	Język wykorzystywany w ramach protokołu SCAP do określania procesów oceny zabezpieczeń, które nie mogą być zrealizowane bez udziału człowieka lub bez informacji zwrotnej.
Open Vulnerability and Assessment Language (OVAL)	–––––	Język wykorzystywany w ramach protokołu SCAP do określania niskopoziomowych procedur testowych używanych w ramach list kontrolnych.

Terminologia angielska	Terminologia polska	Definicja
organization [FIPS 200, Adapted]	organizacja / podmiot	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.).
remote access [SP 800-53]	zdalny dostęp	Dostęp do systemów informacyjnych przez uprawnionego użytkownika, który łączy się z systemem poprzez zewnętrzną sieć komputerową.
risk executive (function) [SP 800-39]	zarządzanie ryzykiem (funkcja)	Osoba (lub grupa osób, kierowana przez wyższego rangą urzędnika w jednostce organizacyjnej) odpowiedzialna za zarządzanie ryzykiem. Posiada w całej organizacji uprawnienia nadzoru i kontroli w zakresie zarządzania ryzykiem. Podstawowe zadania: okresowa (tj. wynikająca z zapisów polityki bezpieczeństwa) kontrola poziomu ryzyka w organizacji; okresowa weryfikacja wartości poziomu akceptacji ryzyka; okresowa weryfikacja kluczowych wskaźników ryzyka; weryfikacja spójności administrowania ryzykiem we wszystkich obszarach działalności organizacji; kontrola zgodności działań w zakresie minimalizacji ryzyka z celami biznesowymi organizacji; nadzór nad działaniami właścicieli ryzyka w zakresie zarządzania ryzykiem; nadzór nad prowadzeniem rejestru ryzyka organizacji.

Terminologia angielska	Terminologia polska	Definicja
risk management [OMB A-130]	zarządzanie ryzykiem	Proces zarządczy związany z działaniami organizacji (w tym misją, funkcjami, wizerunkiem lub reputacją), zasobami organizacji lub osobami fizycznymi wynikającymi z działania systemu informacyjnego. Obejmuje: zarządzanie ryzykiem; analizę kosztów i korzyści; wybór, wdrożenie i ocenę środków bezpieczeństwa; oraz formalne upoważnienie do obsługi systemu. Proces uwzględnia skuteczność, wydajność i ograniczenia wynikające z przepisów prawa, dyrektyw, zasad. Patrz: Zdolność, Zarządzanie oraz Szacowanie Ryzyka (*ang. Capability, Manage and Assess Risk*)
Safeguards [CNSSI-4009, Adapted]	środki bezpieczeństwa / zabezpieczenia	Środki określone w celu spełnienia wymogów bezpieczeństwa (tj. poufności, integralności i dostępności) określonych dla systemu informacyjnego. Środki bezpieczeństwa mogą obejmować funkcje zabezpieczeń, ograniczenia zarządzania, bezpieczeństwo personelu i bezpieczeństwo struktur fizycznych, obszarów i urządzeń. Patrz: • Środki przeciwdziałania (*ang. Countermeasures*), • Zabezpieczenia / Środki bezpieczeństwa (*ang. Security controls*)

Terminologia angielska	Terminologia polska	Definicja
security configuration management (SecCM)	zarządzanie konfiguracją zorientowaną na bezpieczeństwo (*ang. security configuration management – SecCM*)	Zarządzanie konfiguracjami systemu informacyjnego w celu zapewnienia bezpieczeństwa i ułatwienia zarządzania ryzykiem oraz ich kontrola.
security content automation protocol (SCAP)	automatyczny protokół zabezpieczeń zawartości (SCAP)	Metoda z zastosowaniem określonych standardów w celu umożliwienia zautomatyzowanego zarządzania podatnościami, pomiarem i oceną zgodności z zasadami systemów wdrożonych w organizacji.
security control [OMB A-130]	zabezpieczenia / środki bezpieczeństwa / mechanizmy zabezpieczeń	Środki zarządcze, organizacyjne lub technologiczne stosowane w celu zapewnienia poufności, integralności i dostępności informacji i/lub dostępności systemu informacyjnego.
security impact analysis [CNSSI-4009, A adapted]	analiza wpływu na bezpieczeństwo	Analiza przeprowadzona przez pracownika organizacji, często na etapie ciągłego monitorowania procesu certyfikacji i akredytacji bezpieczeństwa, w celu określenia, w jakim stopniu zmiany w systemie informacyjnym wpłynęły na poziom bezpieczeństwa systemu.

Terminologia angielska	Terminologia polska	Definicja
security information and event management (SIEM) tool	bezpieczeństwo informacji i zarządzanie zdarzeniami	Aplikacja zapewniająca możliwość zbierania danych dotyczących bezpieczeństwa z komponentów systemu informacyjnego i przedstawiania tych danych jako informacji użytecznych za pomocą jednego interfejsu.
security posture [CNSSI-4009, Adapted]	stan bezpieczeństwa [CNSSI-4009, zaadaptowany]	Stan bezpieczeństwa sieci, informacji i systemów przedsiębiorstwa oparty na zasobach bezpieczeństwa informacji (np. ludzie, sprzęt, oprogramowanie, polityka) oraz możliwościach zarządzania obroną przedsiębiorstwa i reagowania na zmiany sytuacji. Synonim *statusu bezpieczeństwa*.
Senior Agency Information Security Officer [44 USC 3544]	–––––	Kluczowa osoba w jednostce organizacyjnej odpowiedzialna za bezpieczeństwo informacji. Inaczej Chief Information Security Officer (CISO); lub Senior Information Security Officer (SISO) – w zależności od kultury organizacyjnej jednostki organizacyjnej. Uwaga 1: W odniesieniu do SecCM, kierownik zarządzający ds. bezpieczeństwa informacji jest osobą, która zapewnia ogólnoorganizacyjne procedury bądź szablony dla SecCM, zarządza zespołem ds. zabezpieczeń konfiguracyjnych lub uczestniczy w jego działaniach bądź zapewnia personel techniczny do analiz wpływu na bezpieczeństwo. Uwaga 2: Organizacje podległe agencjom rządowym mogą używać terminu

Terminologia angielska	Terminologia polska	Definicja
senior information security officer	–––––	Patrz SAISO
spyware [CNSSI-4009]	oprogramowanie szpiegujące	Oprogramowanie instalowane w systemie informacyjnym w celu zbierania informacji na temat osób lub organizacji bez ich wiedzy, rodzaj kodu złośliwego.
system [CNSSI 4009]	system	Każdy zorganizowany zespół zasobów i procedur połączonych i regulowanych przez interakcję lub współzależność w celu uzyskania zestawu określonych funkcji. Uwaga: Do systemów zalicza się również systemy specjalistyczne, takie jak systemy przemysłowe/ sterowania procesami, centrale telefoniczne i prywatne centrale telefoniczne (ang. *Private Branch Exchange – PBX*) oraz systemy kontroli środowiska.
system administrator [SP 800-37]	administrator systemu	Osoba, grupa lub organizacja odpowiedzialna za konfigurację i utrzymanie systemu lub określonych elementów systemu; wdraża zatwierdzone konfiguracje bazowe, wprowadza bezpieczne ustawienia konfiguracyjne dla produktów informatycznych oraz przeprowadza/wspomaga w razie potrzeby działania związane z monitorowaniem konfiguracji.
system component	komponent systemu	Patrz: Komponent systemu informacyjnego *(ang. Information System Component)*

Tłumaczenie

Terminologia angielska	Terminologia polska	Definicja
system owner (or program manager) [SP 800-37]	właściciel systemu informacyjnego / właściciel systemu	Podmiot odpowiedzialny całościowo za zamówienia, rozwój, integrację, modyfikację lub obsługę i utrzymanie systemu informacyjnego.
system security officer [SP 800-37]	–––––	Osoba w organizacji, której przypisano odpowiedzialność za zapewnienie utrzymania odpowiedniego poziomu bezpieczeństwa operacyjnego dla systemu informacyjnego.
system security plan	plan bezpieczeństwa systemu	Oficjalny dokument, który zawiera przegląd wymagań dotyczących zabezpieczeń dla systemu informacyjnego i opisuje mechanizmy zabezpieczeń wykorzystywanych lub planowanych do spełnienia tych wymagań. Synonim: Plan Bezpieczeństwa Systemu Informacyjnego (ang. *Information System Security Plan*)
system user [SP 800-37]	użytkownik systemu	Osoba lub (system) proces działający w imieniu osoby, która jest upoważniona do dostępu do informacji i systemów informacyjnych w celu wykonania przydzielonych obowiązków. Uwaga: W odniesieniu do SecCM użytkownik systemu informacyjnego to osoba, która korzysta z funkcji tego systemu, inicjuje wnioski o zmianę i pomaga w wykonaniu testów funkcjonalnych.

Tłumaczenie

Terminologia angielska	Terminologia polska	Definicja
threat [SP 800-30]	zagrożenie	Wszelkie okoliczności lub zdarzenia mogące mieć negatywny wpływ na operacje organizacyjne (w tym misję, funkcje, wizerunek lub reputację), zasoby organizacyjne lub osoby fizyczne za pośrednictwem systemu informacyjnego poprzez nieautoryzowany dostęp, zniszczenie, ujawnienie, modyfikację informacji i/lub odmowę usługi. Ponadto, możliwość pomyślnego wykorzystania luki w zabezpieczeniach określonego systemu informacyjnego przez źródło zagrożenia. Synonim: Cyberzagrożenie (*ang. Cyber Threat*)
threat source [FIPS 200]	źródło zagrożenia	Intencja i metoda ukierunkowane na celowe wykorzystanie podatności w zabezpieczeniach lub sytuacje i metody, które mogą przypadkowo wykorzystać podatność. Synonim: Agent zagrożeń (*ang. Threat Agent*)
United States government configuration baseline (USGCB)[43]	–––––	United States Government Configuration Baseline (USGCB) zapewnia podstawy konfiguracje bazowego produktów informatycznych szeroko stosowanych w agencjach rządowych. Konfiguracja bazowa USGCB rozwinęło się z rządowego programu Desktop Core Configuration. USGCB jest inicjatywą rządu, która dostarcza agencjom wskazówek, co należy zrobić, aby poprawić i utrzymać efektywne ustawienia konfiguracji, skupiając się przede wszystkim na bezpieczeństwie.

[43] https://usgcb.nist.gov/

Terminologia angielska	Terminologia polska	Definicja
user	użytkownik	Patrz *użytkownik systemu*.
vulnerability [CNSSI-4009, Adapted]	podatność (luka w zabezpieczeniach)	Słabość systemu informatycznego, procedur bezpieczeństwa systemu, wewnętrznych zabezpieczeń lub implementacji, która może zostać wykorzystane lub wywołane przez źródło zagrożenia.
whitelist [SP 800-167]	biała lista	Lista odrębnych jednostek, takich jak hosty, adresy e-mail, numery portów sieciowych, procesy uruchomione lub aplikacje, które można instalować lub aktywować w systemie zgodnie z dobrze zdefiniowanym zabezpieczeniem bazowym.

ZAŁĄCZNIK C – AKRONIMY

Załącznik C zawiera stosowane skróty stosowane w publikacji NIST SP 800-128_wer. 1.0_PL.

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

Akronim	Terminologia angielska	Terminologia polska
AO	Authorizing Official	osoba autoryzująca
ARF	Asset Reporting Format	format raportowania o zasobach
BYOD	Bring Your Own Device	przynieś własne urządzenie
CCB	Configuration Control Board	zespół ds. zabezpieczeń konfiguracyjnych
CCE	Common Configuration Enumeration	ujednolicone identyfikatory problemów z konfiguracją systemu
CCSS	Common Configuration Scoring System	system oceny punktowej typowych konfiguracji
CD	Compact Disc	dysk CD
CI	Configuration Item	element konfiguracji
CIO	Chief Information Officer	dyrektor ds. informacji
CIS	Center for Internet Security	organizacja non-profit zajmująca się bezpieczeństwem w Internecie
CISO	Chief Information Security Officer	kierownik zarządzający ds. bezpieczeństwa informacji

Akronim	Terminologia angielska	Terminologia polska
CM	Configuration Management	zarządzanie konfiguracją
CMMI	Capability Maturity Model Integration	kompleksowy model dojrzałości organizacyjnej
CNSS	Committee on National Security Systems	amerykańska organizacja międzyrządowa zajmująca się opracowywaniem polityk bezpieczeństwa w systemach zabezpieczeń w USA
COTS	Commercial Off The Shelf	standardowy produkt komercyjny
CPE	Common Platform Enumeration	ustrukturyzowany schemat nazewnictwa dla systemów informacyjnych
CVE	Common Vulnerabilities and Exposures	słownik identyfikatorów odpowiadających powszechnie znanym podatnościom oraz zagrożeniom, a także standard ich nazewnictwa
CVSS	Common Vulnerability Scoring System	bezpłatny i otwarty standard branżowy służący do oceny stopnia zagrożenia bezpieczeństwa systemu komputerowego
DISA	Defense Information Systems Agency	agencja rządowa USA zajmująca się zagadnieniami związanymi z ochroną systemów informacyjnych

Akronim	Terminologia angielska	Terminologia polska
DMZ	Demilitarized Zone	strefa zdemilitaryzowana
DNS	Domain Name System	system nazw domen
DVD	Digital Video Disc	cyfrowy dysk uniwersalny, płyta kompaktowa
EPP	Endpoint Protection Platform	zintegrowany pakiet do ochrony punktów końcowych: antywirus, szyfrowanie danych i inne narzędzia
FIPS	Federal Information Processing Standards	publicznie ogłaszane standardy federalnego rządu Stanów Zjednoczonych, z których korzystają cywilne agencje rządowe
FISMA	Federal Information Security Modernization Act	ustawa federalna o modernizacji bezpieczeństwa informacji
IA	Information Assurance	wiarygodność informacji
ICS	Industrial Control System	system sterowania przemysłowego
IDPS	Intrusion Detection and Prevention Systems	system wykrywania i zapobiegania włamaniom
IEEE	Institute of Electrical and Electronics Engineers	Instytut Inżynierów Elektryków i Elektroników

Akronim	Terminologia angielska	Terminologia polska
IPSEC	Internet Protocol Security	zbiór protokołów służących implementacji bezpiecznych połączeń oraz wymiany kluczy szyfrowania pomiędzy komputerami
ISO	International Organization for Standardization	Międzynarodowa Organizacja Normalizacyjna
IT	Information Technology	technologia informacyjna
ITIL	Information Technology Infrastructure Library	zbiór publikacji zawierających najlepsze praktyki zarządzania usługami informatycznymi
ITL	Information Technology Laboratory	Laboratorium informatyczne
MAC	Media Access Control	kontrola dostępu do nośnika
NetBIOS	Network Basic Input/Output System	sieciowy podstawowy system wejścia-wyjścia
NIST	National Institute of Standards and Technology	Narodowy instytut standaryzacji i technologii
NISTIR	National Institute of Standards and Technology Interagency Report	Sprawozdanie międzyresortowe Narodowego instytutu standaryzacji i technologii
NVD	National Vulnerability Database	krajowa baza danych dotyczących podatności na zagrożenia

Akronim	Terminologia angielska	Terminologia polska
OCIL	Open Checklist Interactive Language	–––––
OMB	Office of Management and Budget	jednostka biura wykonawczego przy prezydencie USA
OS	Operating System	system operacyjny
OVAL	Open Vulnerability and Assessment Language	–––––
RFID	Radio Frequency Identification	systemy identyfikacji radiowej
RMF	Risk Management Framework	ramy zarządzania ryzykiem
SA	System Administrator	administrator systemu
SAISO	Senior Agency Information Security Officer	kierownik zarządzający ds. bezpieczeństwa informacji
SC	System Component	komponent systemu
SCAP	Security Content Automation Program	automatyczny protokół zabezpieczeń zawartości
SDLC	System Development Life Cycle	cykl życia systemu
SecCM	Security-Focused Configuration Management	zarządzanie konfiguracją zorientowaną na bezpieczeństwo
SIEM	Security Information and Event Management	bezpieczeństwo informacji i zarządzanie zdarzeniami

Akronim	Terminologia angielska	Terminologia polska
SLA	Service-Level Agreement	umowa gwarancji świadczenia usługi
SP	Special Publication	publikacja specjalna
SSH	Secure Shell	bezpieczna powłoka
SSL	Secure Socket Layer	protokół SSL
SSO	System Security Officer	kierownik ds. bezpieczeństwa systemu
STIG	Security Technical Implementation Guidelines	standard konfiguracji składający się z wymagań cyberbezpieczeństwa dla konkretnego produktu
SU	System User	użytkownik systemu
SWID	Software Identification	identyfikacja oprogramowania
TLS	Transport Layer Security	bezpieczeństwo warstwy transportowej
TMSAD	Trust Model for Security Automation Data	–––––
US-CERT	United States Computer Emergency Readiness Team[44]	zespół reagowania na incydenty komputerowe w USA[45]
USC	United States Code	Kodeks Stanów Zjednoczonych

[44] https://www.us-cert. gov/

[45] https://www.us-cert. gov/

Tłumaczenie

Akronim	Terminologia angielska	Terminologia polska
USGCB	United States Government Configuration Baseline	–––––
VOIP	Voice over Internet Protocol	–––––
VPN	Virtual Private Network	wirtualna sieć prywatna
XCCDF	Extensible Configuration Checklist Description Format	format opisu rozszerzonej listy kontrolnej
XML	Extensible Markup Language	–––––

ZAŁĄCZNIK D – PRZYKŁADOWY WZÓR PLANU ZARZĄDZANIA KONFIGURACJĄ ZORIENTOWANĄ NA BEZPIECZEŃSTWO

Poniżej przedstawiono zarys opracowania planu SecCM dla organizacji bądź systemu. Organizacje są zachęcane do dostosowania tego wzoru tak, aby był odpowiedni dla ich środowiska operacyjnego.

1. WPROWADZENIE
    - 1.1 ŚRODOWISKO *[Przegląd SecCM i jego cel]*
    - 1.2 PRZEGLĄD SYSTEMU [*Opis systemu; może zawierać odniesienie do odpowiedniego rozdziału Planu bezpieczeństwa systemu*]
        - 1.2.1 Misja systemu
        - 1.2.2 Opis przepływu danych
        - 1.2.3 Architektura systemu
        - 1.2.4 Działania związane z administrowaniem i zarządzaniem systemem
    - 1.3 CEL TEGO DOKUMENTU *[Wykorzystanie tego dokumentu]*
    - 1.4 ZAKRES *[Stosowanie tego planu]*
    - 1.5 STOSOWNE POLITYKI I PROCEDURY

[Wykaz obowiązujących polityk, standardów i procedur]

2. PROGRAM SecCM
    - 2.1. ROLE I OBOWIĄZKI W RAMACH SecCM *[Opis ról/odpowiedzialności w ramach SecCM]*
    - 2.2. ADMINISTROWANIE PROGRAMEM SecCM *[Polityki, Procedury, zespół CCB]*
        - 2.2.1. Polityki i procedury SecCM (włączone do niniejszego dokumentu lub referencje)
        - 2.2.2. Funkcje zespołu ds. zabezpieczeń konfiguracyjnych
        - 2.2.3. Ustanowienie zespołu ds. kontroli zmian na poziomie organizacji
        - 2.2.4. Ustanowienie zespołu ds. kontroli zmian na poziomie systemu
        - 2.2.5. Harmonogramy i wymagania dotyczące zasobów

2.3. NARZĘDZIA SecCM *[Narzędzia i lokalizacje archiwum dla zespołu CCB]*

2.3.1. Narzędzia SCM

2.3.2. Biblioteka SCM

2.4. RETENCJA, ARCHIWIZACJA, PRZECHOWYWANIE I USUWANIE SecCM

[Wymagania dotyczące zarządzania informacjami historycznymi o elementach konfiguracji, zmianach itp.]

3. DZIAŁANIA SecCM

3.1. IDENTYFIKOWANIE KONFIGURACJI

3.1.1. Typy elementów konfiguracji (CI) *[Opis kategorii elementów konfiguracji, takich jak sprzęt, dokumentacja, oprogramowanie i skrypty, strony WWW]*

3.1.2. Kryteria identyfikacji *[Jak określić, które komponenty systemu informacyjnego będą dołączone do których elementów konfiguracji]*

3.1.3. Oznaczanie elementu konfiguracji *[konwencja nazewnictwa dla elementów konfiguracji]*

3.2. USTALANIE POZIOMU BAZOWEGO KONFIGURACJI *[Określenie informacji, które mają być zawarte w konfiguracji bazowej dla każdego elementu konfiguracji]*

3.2.1. Identyfikowanie stosownych typowych konfiguracji zorientowanych na bezpieczeństwo;

3.2.2. Konfiguracje bazowe komponentu systemu informacyjnego będącego elementem konfiguracji

3.2.3. Konfiguracje bazowe komponentu systemu informacyjnego niebędącego elementem konfiguracji

3.3. KONTROLA ZMIAN KONFIGURACJI *[Wymagania związane z kontrolą zmian konfiguracji]*

3.3.1. Postępowanie z zaplanowanymi, niezaplanowanymi i nieautoryzowanymi zmianami

ZAŁĄCZNIK E – PRZYKŁADOWE ŻĄDANIE ZMIANY (SZABLON)

Poniżej znajduje się przykładowy szablon artefaktu żądania zmiany, który może być użyty w programie SecCM. Organizacje zachęca się do dostosowania żądania zmiany do swoich potrzeb.

1. **Data przygotowania:**
2. **Tytuł żądania zmiany:**
3. **Inicjator zmiany / menadżer projektu:**
4. **Opis zmiany:**
5. **Ocena zmiany:**
6. **Pilność zmiany:** {Planowana/Pilna/Nieplanowana}
7. **Komponenty systemu / Elementy konfiguracji do zmiany:**
8. **Inne komponenty systemu, elementy konfiguracji lub systemy, na które zmiana będzie miała wpływ:**
9. **Personel zaangażowany w zmianę:**
10. **Oczekiwany wpływ zmiany na bezpieczeństwo:**
11. **Oczekiwany wpływ zmiany na funkcjonalność:**
12. **Oczekiwany wpływ braku wprowadzenia zmiany:**
13. **Potencjalne problemy z interfejsem/integracją:**
14. **Wymagane zmiany w istniejących aplikacjach:**
15. **Plan pracy nad projektem zawierający datę wdrożenia zmiany, rezultaty i plan wycofania:**
16. **Finansowanie wymagane do wdrożenia zmiany:**

Zmiana zatwierdzona/niezatwierdzona (należy dołączyć uzasadnienie bądź dalsze działania, które trzeba podjąć w przypadku braku zatwierdzenia):

Autoryzowane podpisy:

UWAGA: Do wniosku o zmianę można dołączyć dokumentację uzupełniającą.

ZAŁĄCZNIK F – NAJLEPSZE PRAKTYKI W ZAKRESIE TWORZENIA BEZPIECZNYCH KONFIGURACJI

Nie ma jednego uniwersalnego podejścia do SecCM, jednak istnieją praktyki, które organizacje rozważają podczas opracowywania i wdrażania bezpiecznych konfiguracji, w tym:

1. Użycie typowych bezpiecznych konfiguracji dla ustawień

Organizacje traktują dostępne typowe bezpieczne konfiguracje jako podstawę do ustanowienia bezpiecznych ustawień konfiguracyjnych. Obszernym źródłem informacji na temat ustawień konfiguracyjnych jest National Checklist Program (https://checklists.nist.gov). Listy kontrolne obejmują szeroki zakres produktów komercyjnych i są napisane w standardowym formacie, aby ułatwić automatyczną ocenę za pomocą narzędzi obsługujących SCAP.

Powiązane środki bezpieczeństwa [NSC 800-53]: zabezpieczenie CM-6.

Bibliografia:

NIST [SP 800-70]: *National Checklist Program for IT Products-Guidelines for Checklist Users and Developers*;

https://nvd.nist.gov.

2. Centralizacja zasad i typowych bezpiecznych konfiguracji dla ustawień konfiguracyjnych

Tam, gdzie to możliwe i właściwe, bezpieczne konfiguracje są opracowywane i wdrażane odgórnie, aby zapewnić spójność w całej organizacji. Przykładem jest wdrożenie funkcjonalności polityki grupowej, która może być wykorzystana do dystrybucji polityki bezpiecznej konfiguracji w sposób scentralizowany, w ramach ustanowionych domen. Wyjątki od polityki organizacji mogą być potrzebne, aby dostosować konfiguracje do konkretnego systemu oraz lokalnych ograniczeń lub wymagań. Takie wyjątki są dokumentowane i zatwierdzane jako część konfiguracji bazowej dla danego systemu informacyjnego.

Powiązane środki bezpieczeństwa[NSC 800-53]: zabezpieczenia CM-1; CM-6.

Bibliografia: Brak.

3. Dostosowanie konfiguracji zorientowanych na bezpieczeństwo do funkcji i roli systemu/komponentu

Ustawienia konfiguracji zorientowanej na bezpieczeństwo są dostosowane do funkcji komponentu systemu. Na przykład serwer działający jako kontroler domeny Windows może mieć bardziej rygorystyczne wymagania dotyczące audytu (np. audytu udanych i nieudanych logowań konta) niż serwer plików. Serwer WWW z dostępem publicznym w strefie zdemilitaryzowanej (DMZ) może wymagać uruchomienia mniejszej liczby usług niż w przypadku serwera WWW za zaporą organizacji obsługującej intranet.

Powiązane środki bezpieczeństwa [NSC 800-53]: zabezpieczenia CM-6; RA-3.

Bibliografia:

NIST [SP 800-41]: *Guidelines on Firewalls and Firewall Policy*;

NIST [SP 800-44]: *Guidelines on Securing Public Web Servers*;

NIST [SP 800-45]: *Guidelines on Electronic Mail Security*;

NIST [SP 800-46]: *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*;

NIST [SP 800-52]: *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*;

NIST [SP 800-54]: *Border Gateway Protocol Security*;

NIST [SP 800-58]: *Security Considerations for Voice Over IP Systems*;

NIST [SP 800-77]: *Guide to IPsec VPNs*;

NIST [SP 800-81-2]: *Secure Domain Name System (DNS) Deployment Guide*;

NIST [SP 800-82]: *Guide to Industrial Control Systems (ICS) Security*;

NIST [SP 800-92]: *Guide to Computer Security Log Management*;

NIST [SP 800-95]: *Guide to Secure Web Services*;

NIST [SP 800-97]: *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*;

NIST [SP 800-98]: *Guidelines for Securing Radio Frequency Identification (RFID)* Systems;

NIST [SP 800-113]: *Guide to SSL VPNs;*

NIST [SP 800-121]: *Guide to Bluetooth Security;*

NIST [SP 800-123]: *Guide to General Server Security; oraz*

NIST [SP 800-124]: *Guidelines for Managing the Security of Mobile Devices in the Enterprise.*

4. Wyeliminowanie zbędnych portów, usług i protokołów (zasada minimalnej funkcjonalności)

Urządzenia są skonfigurowane tak, aby dopuszczały tylko niezbędne porty, protokoły i usługi zgodnie z potrzebami funkcjonalnymi i tolerancją ryzyka w organizacji. Otwarte porty oraz dostępne protokoły i usługi są zachęcającym celem dla atakujących, zwłaszcza jeśli z danym portem, protokołem lub usługą związane są znane podatności. Źródła takie jak NIST National Vulnerability Database (NVD) mogą służyć do wskazania podatności w różnych komponentach systemu.

Powiązane środki bezpieczeństwa [NSC 800-53]: zabezpieczenie CM-7.

Bibliografia: https://nvd.nist.gov/.

5. Ograniczanie korzystania z połączeń zdalnych

Zdalne podłączanie się do systemów zapewnia większą elastyczność w wykonywaniu pracy przez użytkowników i administratorów, ale otwiera również drogę ataku popularną wśród hakerów. Korzystanie z połączeń zdalnych jest ograniczone tylko do tych, które są absolutnie niezbędne do wykonania misji.

Powiązane środki bezpieczeństwa [NSC 800-53]: zabezpieczenie AC-17.

Bibliografia:

NIST [SP 800-41]: *Guidelines on Firewalls and Firewall Policy*;

NIST [SP 800-46]: *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security;*

NIST [SP 800-47]: *Security Guide for Interconnecting Information Technology Systems*;

NIST [SP 800-52]: *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*;

NIST [SP 800-54]: *Border Gateway Protocol Security*;

NIST [SP 800-77]: *Guide to IPsec VPNs*;

NIST [SP 800-81-2]: *Secure Domain Name System (DNS) Deployment Guide*;

NIST [SP 800-95]: *Guide to Secure Web Services*; oraz

NIST [SP 800-113]: *Guide to SSL VPNs*.

6. Opracowanie zasad dotyczących silnych haseł

Hasła pozostają powszechnym mechanizmem uwierzytelniania tożsamości użytkowników i jeśli są źle zaimplementowane lub używane, atakujący może pokonać najlepiej zabezpieczoną konfigurację. Organizacje określają politykę haseł i związane z nią wymagania na poziomie odpowiednim do ochrony dostępu do zasobów organizacji.

Powiązane środki bezpieczeństwa [PNSC 800-53]: zabezpieczenia IA-2, IA-5.

Bibliografia:

NIST [SP 800-63B]: *Digital Identity Guidelines, Authentication and Lifecycle Management*; NIST [SP 800-132]: *Recommendation for Password-Based Key Derivation Part 1: Storage Applications*; oraz

NIST [SP 800-135]: *Recommendation for Existing Application-Specific Key Derivation Functions*.

7. Wdrożenie platform ochrony punktów końcowych (*ang. Endpoint Protection Platforms - EPP*)

Punkty końcowe (np. laptopy, desktopy, urządzenia mobilne) są fundamentalną częścią każdego systemu organizacyjnego. Punkty końcowe stanowią ważne źródło połączenia użytkowników końcowych z sieciami i systemami, a także są głównym źródłem luk w zabezpieczeniach i częstym celem napastników chcących przeniknąć do

sieci. Zachowanie użytkownika jest trudne do kontrolowania i przewidzenia, a jego działania, czy to kliknięcie łącza, które uruchamia złośliwe oprogramowanie, czy zmiana ustawienia zabezpieczeń w celu poprawy użyteczności punktu końcowego, często umożliwiają wykorzystanie podatności. Komercyjni dostawcy oferują wiele produktów poprawiających bezpieczeństwo w „punktach końcowych" sieci. Platformy ochrony punktów końcowych (EPP) obejmują:

a. Oprogramowanie antywirusowe

Aplikacje antywirusowe są częścią typowych konfiguracji zorientowanych na bezpieczeństwo komponentów systemu. Oprogramowanie antywirusowe wykorzystuje szeroką gamę sygnatur i schematów wykrywania, automatycznie aktualizuje sygnatury, nie zezwala na modyfikację przez użytkowników, uruchamia skanowanie według ustalonego harmonogramu, zawiera funkcję samoochrony ustawioną na automatyczne skanowanie po wykonaniu czynności przez użytkownika (np. otwarciu lub skopiowaniu pliku) i może zapewniać ochronę przed atakami typu „zero-day". W przypadku platform, dla których oprogramowanie antywirusowe nie jest dostępne, można zastosować inne formy oprogramowania antywirusowego, takie jak detektory programów typu rootkit.

b. Osobiste zapory sieciowe

Osobiste zapory sieciowe zapewniają szeroki zakres ochrony dla hostów, w tym ograniczenie dostępu do portów i usług, ochronę przed złośliwymi programami, które wykonują się na hoście, zabezpieczenie urządzeń wymiennych, takich jak urządzenia USB, dyski, oraz możliwość audytu i rejestrowania.

c. System wykrywania i zapobiegania włamaniom (*ang. Intrusion Detection and Prevention System - IDPS*) oparty na hoście

System wykrywania i zapobiegania włamaniom oparty na hoście monitoruje cechy pojedynczego hosta oraz zdarzenia zachodzące w obrębie tego hosta w celu identyfikacji i zatrzymania podejrzanej aktywności. Różni się od systemu IDPS opartego na sieci, który jest systemem wykrywania włamań i zapobiegania im, monitorującym ruch sieciowy dla poszczególnych segmentów sieci lub

urządzeń i analizuje aktywność protokołu sieciowego i aplikacyjnego w celu identyfikacji i zatrzymania podejrzanej aktywności.

d. Ograniczenie stosowania kodu mobilnego

Organizacje powinny zachować ostrożność, zezwalając na stosowanie „kodu mobilnego", takiego jak ActiveX, Java i JavaScript. Atakujący może łatwo dołączyć skrypt – do adresu URL na stronie internetowej lub do wiadomości e-mail – który po kliknięciu wykona złośliwy kod w przeglądarce komputera.

Powiązane środki bezpieczeństwa [NSC 800-531]: zabezpieczenia SC-7, SC-18, SI-3, SI-4

Bibliografia:

NIST [SP 800-28]: *Guidelines on Active Content and Mobile Code;*

NIST [SP 800-41]: *Guidelines on Firewalls and Firewall Policy;*

NIST [SP 800-47]: *Security Guide for Interconnecting Information Technology Systems;*

NIST [SP 800-54]: *Border Gateway Protocol Security;*

NIST [SP 800-94]: *Guide to Intrusion Detection and Prevention Systems (IDPS);*

NIST [SP 800-124]: *Guidelines for Managing the Security of Mobile Devices in the Enterprise;* oraz

NIST [SP 800-179]: *Guide to Securing Apple OSX 10.10 System for IT Professional: A NIST Security Configuration Checklist.*

8. Użycie kryptografii

W wielu systemach, zwłaszcza tych przetwarzających, przechowujących lub przesyłających informacje o umiarkowanym lub wyższym poziomie wpływu na poufność, kryptografia jest uważana za część konfiguracji zorientowanej na bezpieczeństwo systemu. Istnieje wiele miejsc, w których można zaimplementować kryptografię do ochrony danych, w tym szyfrowanie pojedynczych plików, pełne szyfrowanie dysku, połączenia Virtual Private Network itp.

Powiązane środki bezpieczeństwa [NSC 800-531]: zabezpieczenie SC-13

Bibliografia:

[FIPS 140-3]: *Security Requirements for Cryptography Modules;*

NIST [SP 800-25]: *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*;

NIST [SP 800-32]: *Introduction to Public Key Technology and the Federal PKI Infrastructure*, NIST SP 800-57: *Recommendation for Key Management, Part 1: General;*

NIST [SP 800-57]: *Recommendation for Key Management, Part 2: Best Practices for Key Management Organization;*

NIST [SP 800-57]: *Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance;*

NIST [SP 800-107]: *Recommendation for Applications Using Approved Hash Algorithms;*

NIST [SP 800-111]: *Guide to Storage Encryption Technologies for End User Devices*;

NIST [SP 800-130]: *A Framework for Designing Cryptographic Key Management Systems;*
NIST [SP 800-131A]: *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*; and

NIST [SP 800-175B]: *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms.*

9. Opracowanie procesu zarządzania poprawkami

Solidny proces zarządzania poprawkami jest ważny dla redukcji podatności w systemie. Ponieważ poprawki w znacznym stopniu wpływają na bezpieczną konfigurację systemu, proces zarządzania poprawkami jest zintegrowany z SecCM w wielu punktach w ramach czterech etapów SecCM, w tym w:

- Wykonywaniu analizy wpływu poprawek na bezpieczeństwo;
- Testowaniu i zatwierdzaniu poprawek w ramach procesu kontroli zmian konfiguracji;
- Aktualizacji konfiguracji bazowych w celu uwzględnienia bieżącego poziomu poprawek;
- Ocenie poprawek w celu zapewnienia ich właściwego wdrożenia; oraz

- Monitorowaniu systemów/komponentów pod kątem bieżącego stanu poprawek.

Powiązane środki bezpieczeństwa [NSC 800-53]: zabezpieczenia CM-2, CM-3, CM-4, SI-2.

Bibliografia:

NIST [SP 800-40]: *Guide to Enterprise Patch Management Technologies.*

10. Środki bezpieczeństwa podczas instalowania oprogramowania

Instalacja oprogramowania jest etapem, w którym do systemu organizacyjnego wprowadzanych jest wiele podatności. Złośliwe lub niezabezpieczone oprogramowanie może dać napastnikom łatwy dostęp do nawet ściśle chronionej sieci organizacji. Chociaż najprostszym podejściem jest zablokowanie komputerów i zarządzanie instalacją oprogramowania centralnie (tj. na poziomie organizacji), dla niektórych organizacji nie zawsze jest to wykonalne. Do innych metod kontrolowania instalacji oprogramowania należą:

- Umieszczanie programów na białej liście – całe oprogramowanie jest sprawdzane pod kątem listy zatwierdzonej przez organizację.
- Sumy kontrolne – całe oprogramowanie jest sprawdzane, aby upewnić się, że kod nie uległ zmianie.
- Certyfikaty – używane jest tylko oprogramowanie z podpisanymi certyfikatami od zaufanego dostawcy.
- Ścieżka lub domena – oprogramowanie można zainstalować tylko w obrębie danego katalogu lub domeny.
- Rozszerzenie pliku – oprogramowanie z niektórymi rozszerzeniami plików, takimi jak .bat, nie może zostać zainstalowane.

Powiązane środki bezpieczeństwa [NSC 800-53]: zabezpieczenia CM-5, CM-7, CM-11, SI-7.

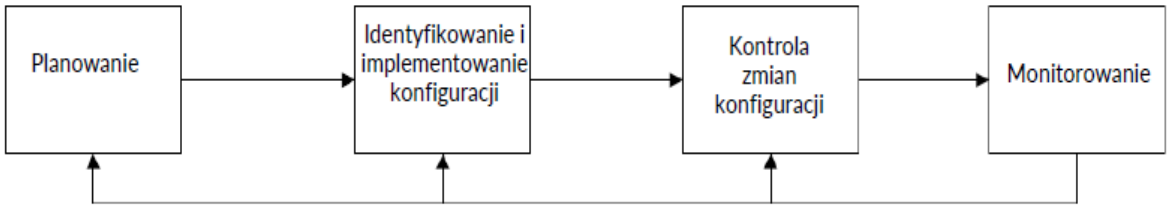
Bibliografia:

NIST [SP 800-167]: *Guide to Application Whitelisting.*

ZAŁĄCZNIK G – SCHEMATY PRZEPŁYWU PROCESU SECCM

Poniższe schematy blokowe przedstawiają przykłady etapów i działań SecCM dla tych etapów, które można rozważyć przy opracowywaniu procesów SecCM. Organizacje są zachęcane do dostosowania schematów blokowych do swojego środowiska operacyjnego.

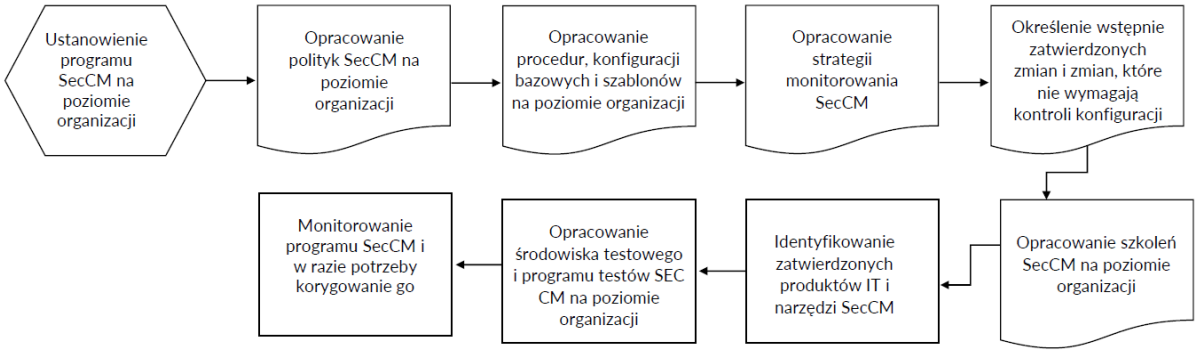
Etapy zarządzania konfiguracją zorientowaną na bezpieczeństwo



Program zarządzania konfiguracją zorientowaną na bezpieczeństwo na poziomie organizacji

Planowanie - zadania w ramach etapu

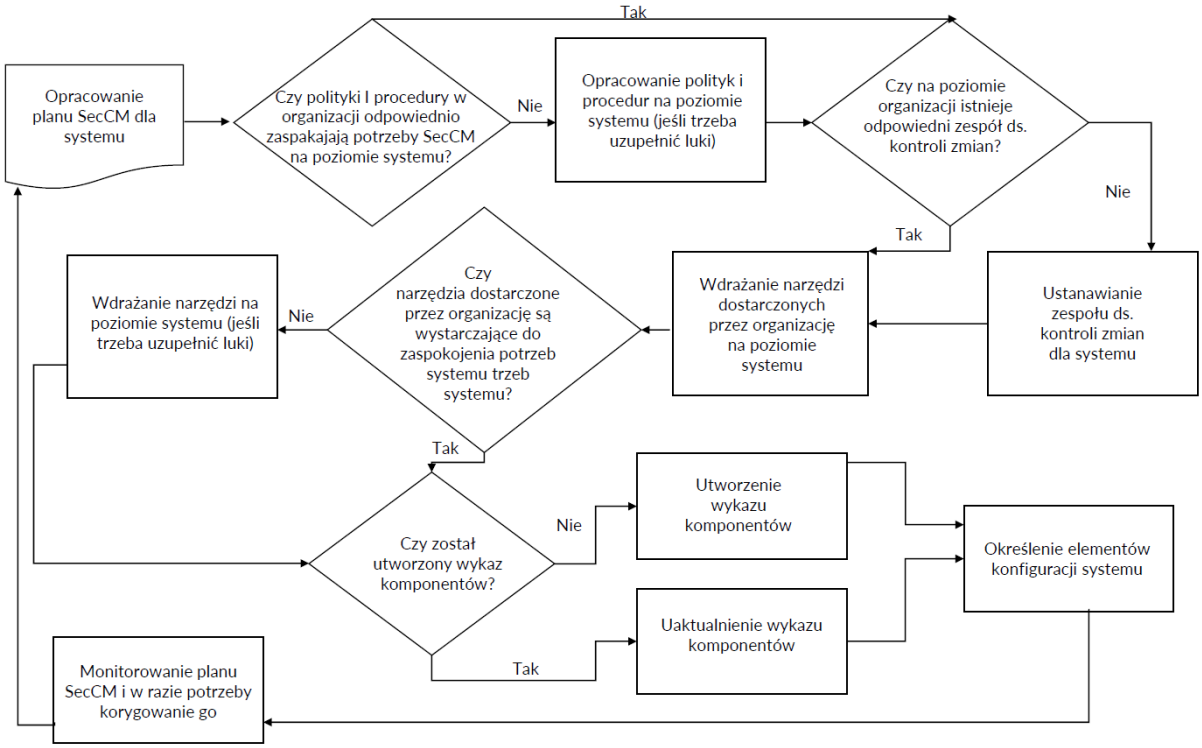
(Rozdział 3.1.1)



Program zarządzania konfiguracją zorientowaną na bezpieczeństwo na poziomie systemu

Planowanie - zadania w ramach etapu

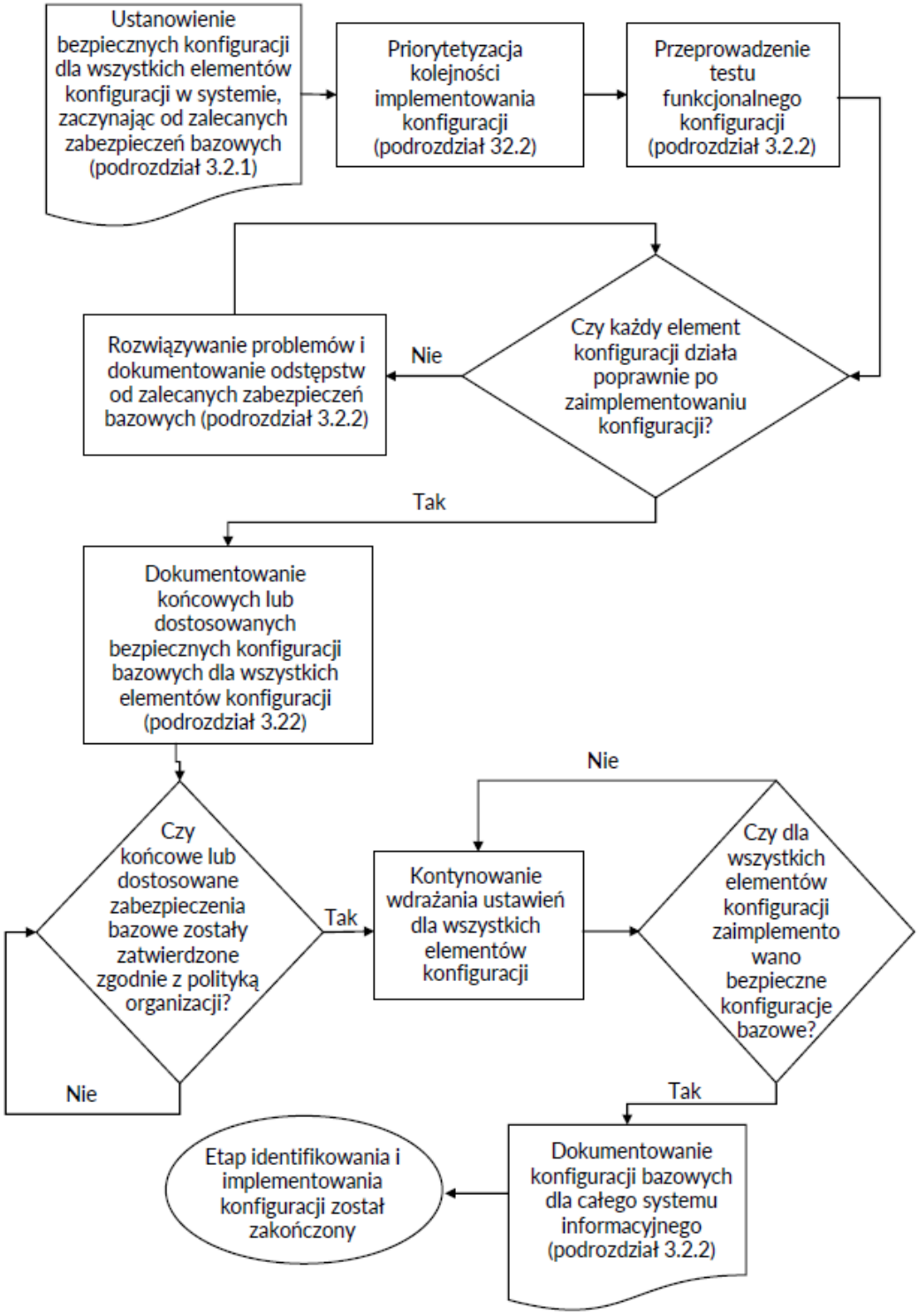
(Rozdział 3.1.2)



Zarządzanie konfiguracją zorientowaną na bezpieczeństwo na poziomie systemu

Identyfikowanie i wdrażanie konfiguracji – zadania w ramach etapu

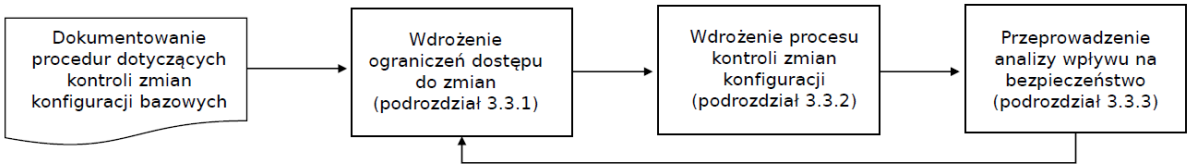
(Rozdział 3.2)



Zarządzanie konfiguracją zorientowaną na bezpieczeństwo na poziomie systemu

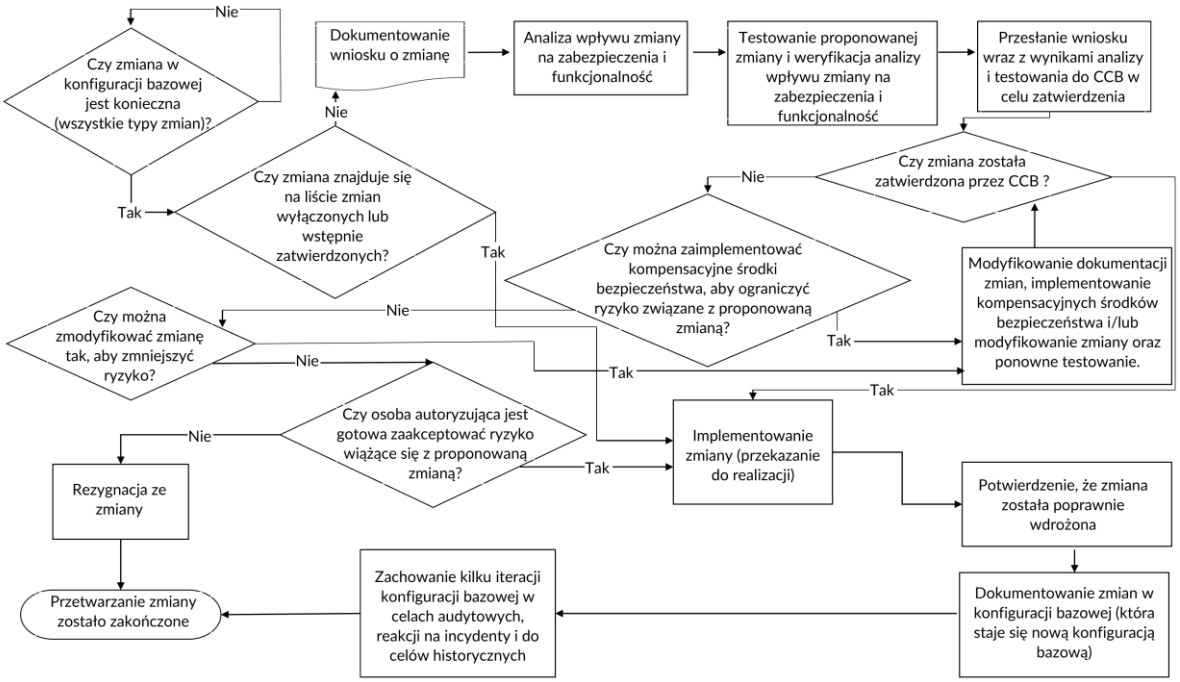
Kontrola zmian konfiguracji – zadania w ramach etapu

(Rozdział 3.3)



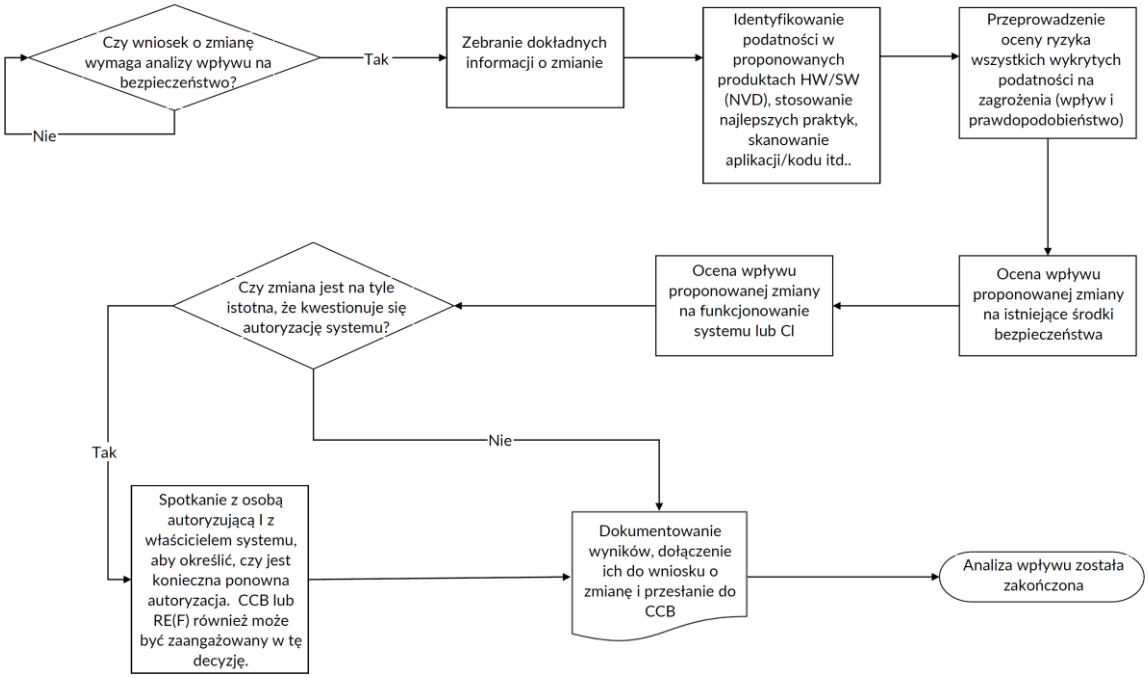
Kontrola zmian konfiguracji – wdrożenie procesu kontroli zmian konfiguracji

(Rozdział 3.3.2)



Kontrola zmian konfiguracji – przeprowadzenie analizy wpływu na bezpieczeństwo

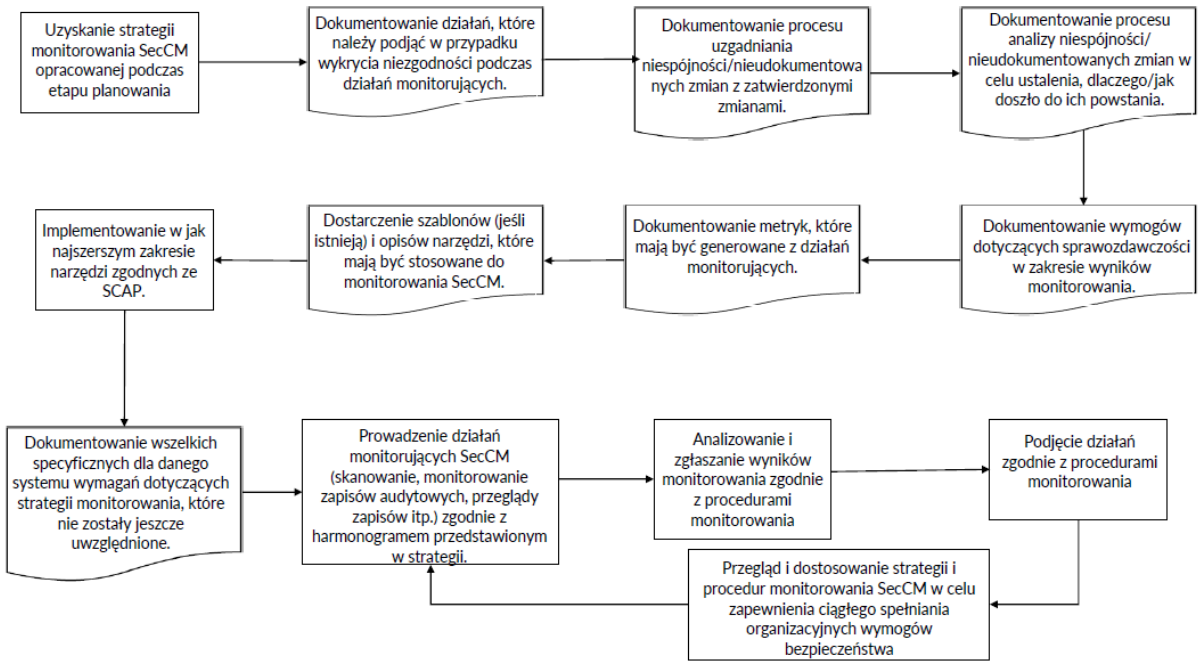
(Rozdział 3.3.3)



Program zarządzania konfiguracją zorientowaną na bezpieczeństwo na poziomie organizacji – etap monitorowania

Wdrożenie strategii i harmonogramu monitorowania SecCM

(Rozdział 3.4)



ZAŁĄCZNIK H – PRZYKŁAD STATUTU ZESPOŁU CCB

Poniżej znajduje się przykładowy szablon statutu zespołu CCB, który może być użyty w programie SecCM. Organizacje zachęca się do dostosowania go do swoich potrzeb.

Statut zespołu ds. zabezpieczeń konfiguracyjnych

CEL

<Należy opisać cele zespołu CCB. Może to być przykładowo: „Zespół ds. zabezpieczeń konfiguracyjnych (CCB) reprezentuje interesy zarządzania programem i projektem przez zapewnienie, że do rozważenia proponowanych zmian i włączenia ich do określonej wersji produktu stosowany jest ustrukturyzowany proces. Zespół CCB żąda przeprowadzenia analizy wpływu proponowanych zmian, dokonuje przeglądu wniosków o zmianę, podejmuje decyzje i informuje o podjętych decyzjach zainteresowane grupy i osoby". Należy określić relacje tego zespołu CCB z innymi zespołami CCB w organizacji lub innymi organami decyzyjnymi, takimi jak zespół zarządzający projektem.>

ZAKRES UPRAWNIEŃ

<Wskazać zakres decyzji, które podejmuje zespół CCB. Zakres ten może dotyczyć określonego zasięgu organizacyjnego; projektu, grupy projektów (programu) lub podprojektu; maksymalnego wpływu na budżet lub harmonogram. To ograniczenie zakresu oddziela decyzje, które może podjąć zespół CCB, od tych, które trzeba przekazać do zespołu CCB wyższego szczebla lub menadżera wyższego szczebla w celu ich rozwiązania.>

CZŁONKOSTWO

<Lista członków danego zespołu CCB. W skład zespołu CCB wchodzą zazwyczaj przedstawiciele kierownictwa programu, zarządzania projektem, inżynierii oprogramowania, inżynierii sprzętu, testowania, dokumentacji, obsługi klienta i marketingu. Jedna osoba jest wyznaczana na lidera zespołu CCB. Należy utrzymywać zespół CCB w jak najmniejszym składzie, aby ułatwić mu podejmowanie szybkich decyzji, ale trzeba się upewnić, że w zespole są reprezentowane najważniejsze perspektywy.>

PROCEDURY OPERACYJNE

<Należy określić częstotliwość regularnych spotkań zespołu CCB oraz warunki, które powodują zwołanie spotkania specjalnego. Należy opisać sposób prowadzenia spotkań, liczbę członków zespołu CCB, którzy stanowią kworum do podejmowania decyzji, oraz role, które muszą być reprezentowane, aby spotkanie mogło się odbyć. Określenie, czy w spotkaniu mogą uczestniczyć osoby zaproszone, na przykład osoby, które zaproponowały wnioski o zmianę rozpatrywane na danym spotkaniu.>

PROCES PODEJMOWANIA DECYZJI

<Należy opisać, w jaki sposób zespół CCB będzie podejmować decyzje. Wskazać, czy do podejmowania decyzji wykorzystywane jest głosowanie, konsensus, jednomyślność, delegowanie do konkretnej osoby, czy też jakaś inna zasada. Należy określić, czy lider zespołu CCB lub inny menadżer ma prawo uchylić decyzję zbiorową zespołu CCB.>

STAN KOMUNIKACJI

<Opisać, w jaki sposób każda decyzja podjęta przez zespół CCB zostanie przekazana osobie, która wnioskowała o zmianę, kierownictwu wyższego szczebla, kierownictwu projektu, członkom zespołu, który musi wdrożyć zmianę, zespołowi CCB wyższego lub niższego szczebla oraz wszystkim innym zainteresowanym stronom. Wskazać miejsce przechowywania decyzji i wszelkich informacji pomocniczych, uzasadnienia lub danych.>

ZAŁĄCZNIK I – PRZYKŁADOWY SZABLON ANALIZY WPŁYWU NA BEZPIECZEŃSTWO

Poniżej znajduje się przykładowy szablon analizy wpływu na bezpieczeństwo, który może zostać użyty w programie SecCM. Organizacje zachęca się do dostosowania go do swoich potrzeb.

[*Wstawić odpowiednie strony, np. zespół kontroli konfiguracji, właściciel systemu, kierownik ds. bezpieczeństwa systemu (SSO), administratorzy systemu, audytorzy ds. bezpieczeństwa*] uzupełniają tabele 1-5, które posłużą do przeglądu zmiany i określenia wymagań.

Tabela 1: Podstawowe informacje o inicjatywie/wersji

[UWAGA DO SZABLONU: Wstępnie wypełnione informacje w tabeli 1 mają charakter jedynie poglądowy i powinny być zastąpione informacjami mającymi zastosowanie do poszczególnych organizacji.]

Nazwa inicjatywy/wersji	
Typ projektu:	[Przykłady]: - **Nowe wdrożenie**: *[wstawić opis]* - **Rozszerzenie**: *[wstawić opis]* - **Utrzymanie**: *[wstawić opis]* *[Wstawić typy projektów i opisy, jeśli mają zastosowanie]*
Zmiany w systemie	**Przedstawić przegląd zmian.**
Zmiany w konfiguracji bazowej	**Przedstawić opis nowej konfiguracji bazowej.**
Ryzyko dotyczące bezpieczeństwa	**Przedstawić wszelkie zagrożenia i wpływy na system.**
Planowana data rozpoczęcia wdrożenia	

Nazwa inicjatywy/wersji	
Planowana data zakończenia wdrożenia	
Systemy, na które zmiana ma wpływ:	
Bieżąca kategoryzacja bezpieczeństwa systemów, na które zmiana ma wpływ:	
[W stosownych przypadkach wpisać dodatkowe informacje dotyczące inicjatywy/wersji wymaganej przez organizację]	

Tabela 2: Opis inicjatywy/wersji i potencjalnych problemów związanych z bezpieczeństwem

[UWAGA DO SZABLONU: Wstępnie wypełnione informacje w tabeli 2 mają charakter jedynie poglądowy i powinny być zastąpione informacjami mającymi zastosowanie do poszczególnych organizacji.]

Jakie są wymagania biznesowe wymuszające zmianę?
Przedstawić opis proponowanej zmiany (zmian), w tym WSZYSTKIE uzupełnienia, usunięcia i modyfikacje.
Czy lider techniczny bądź lider projektu są świadomi wszelkich potencjalnych kwestii związanych z bezpieczeństwem lub wyzwań związanych z tą zmianą? Jeśli tak, krótko opisać lub dodać załącznik z ich opisem.

Tabela 3: Typ zmiany – Arkusz roboczy

Zapoznaj się z poniższą listą typów zmian. W drugiej kolumnie zaznacz znakiem „X” każdy obowiązujący typ zmiany. W trzeciej kolumnie należy podać krótkie wyjaśnienie

dotyczące wyboru odpowiednich typów zmian. Typy zmian nie wykluczają się wzajemnie, dlatego dla jednej inicjatywy/wersji można wybrać wiele typów zmian. Jeśli żaden z typów zmian nie ma zastosowania, należy zaznaczyć „Inna zmiana" i podać jej opis w trzeciej kolumnie.

[UWAGA DO SZABLONU: *Typy zmian podane w tabeli 3 mają jedynie charakter poglądowy i powinny zostać zastąpione typami zmian mającymi zastosowanie do poszczególnych organizacji.*]

Typ zmiany	**Czy dotyczy? (zaznacz znakiem X, jeśli dotyczy)**	**Wyjaśnienie (jeśli dotyczy)**
Nowe urządzenia sieciowe (np. router, przełącznik, zapora, brama VPN)		
Nowe serwery		
Nowe stacje robocze (komputery stacjonarne lub laptopy)		
Inny nowy sprzęt		
Likwidacja istniejącego sprzętu		
Nowy serwer wirtualny		
Nowy system operacyjny		
Aktualizacja istniejącego systemu operacyjnego		
Nowa aplikacja COTS		
Aktualizacja lub wgranie poprawek aplikacji COTS		
Nowa niestandardowa aplikacja		

Typ zmiany	**Czy dotyczy? (zaznacz znakiem X, jeśli dotyczy)**	**Wyjaśnienie (jeśli dotyczy)**
Aktualizacja lub poprawka błędu dla istniejącej aplikacji niestandardowej		
Nowy system zarządzania bazą danych (np. Microsoft SQL Server lub Oracle)		
Aktualizacja istniejącego systemu zarządzania bazą danych (np. Oracle 9i do 10g)		
Dodanie nowej instancji bazy danych		
Modyfikacja istniejącej instancji bazy danych (np. zmiany w tabeli)		
Nowa lub zmodernizowana aplikacja lub usługa pośrednicząca		
Modyfikacje portów, protokołów i usług używanych lub dostarczanych przez system		
Zmiany mające na celu spełnienie wymagań bezpieczeństwa lub poprawę/modyfikację bezpieczeństwa systemu (np. moduły kryptograficzne, poprawki bezpieczeństwa, uwierzytelnianie, autoryzacja, zmiana ról)		
Nowy typ informacji przetwarzany, przechowywany lub przekazywany w systemie		
Zmiana interfejsu (dodanie/usunięcie)		
Zmiana lokalizacji		
Inna zmiana		

Tabela 4: Wpływ urządzenia – Arkusz roboczy

[UWAGA DO SZABLONU: Nagłówki w tabeli 4 mają jedynie charakter poglądowy i powinny zostać zastąpione informacjami mającymi zastosowanie do poszczególnych organizacji.]

Nazwa systemu	Nazwa urządzenia	Adres IP	Model producenta	Nr seryjny	Identyfikator komponentu/zasobu	OS	Oprogramowanie	Opis

Tabela 5: Testowanie – Arkusz roboczy

[UWAGA DO SZABLONU: Wstępnie wypełnione informacje w tabeli 5 mają charakter jedynie poglądowy i powinny być zastąpione informacjami mającymi zastosowanie do poszczególnych organizacji.]

Należy opisać testy, które zostały przeprowadzone dla danej zmiany.
Opisać wyniki testów dla każdej zmiany (lub podać odniesienie do innego dokumentu z wynikami testów).

Tabela 6: Analiza – Arkusz roboczy

[UWAGA DO SZABLONU: Wstępnie wypełnione informacje w tabeli 5 mają charakter jedynie poglądowy i powinny być zastąpione informacjami mającymi zastosowanie do poszczególnych organizacji].

Analiza, zalecenia i wymagania
[Sprawdził: nazwisko (tytuł)]

Podpis

_____ _____

[Wstaw odpowiednią rolę] [Data]

Podpis

_____ _____

[Wstaw odpowiednią rolę] [Data]

Podpis

_____ _____

[Wstaw odpowiednią rolę] [Data]

DODATEK I

WPŁYW NA BEZPIECZEŃSTWO – ARKUSZ ROBOCZY

1. AC[46]: Czy zmiany w systemie wpłyną na ograniczenia systemu: (I) dostęp do systemu dla upoważnionych użytkowników, procesy działające w imieniu upoważnionych użytkowników lub urządzeń (w tym inne systemy); oraz (II) rodzaje transakcji i funkcji, które upoważnieni użytkownicy mogą wykonywać.

Jeśli tak, opisz.

2. AT: Czy zmiany wpłyną na wymagane szkolenia systemowe w celu zapewnienia, że personel jest odpowiednio przeszkolony do wykonywania przydzielonych mu obowiązków i zadań związanych z bezpieczeństwem informacji?

Jeśli tak, opisz.

3. AU: Czy zmiany wpłyną na sposób spełnienia wymagań dotyczących audytu systemu w ramach (I) tworzenia, ochrony i przechowywania zapisów audytu systemu w zakresie niezbędnym do umożliwienia monitorowania, analizowania, badania i zgłaszania bezprawnych, nieautoryzowanych lub niewłaściwych działań w systemie; oraz (II) zapewnienia, że działania poszczególnych użytkowników systemu mogą być do nich jednoznacznie przypisane, tak aby można było pociągnąć ich do odpowiedzialności.

Jeśli tak, opisz.

4. CM: Czy zmiany w systemie wpłyną na (I) konfigurację bazową i inwentaryzację systemów organizacyjnych; (II) ustanowienie i egzekwowanie ustawień konfiguracji bezpieczeństwa; oraz (III) zdolność do monitorowania i kontrolowania zmian w konfiguracjach bazowych oraz w komponentach składowych systemów (w tym w sprzęcie, oprogramowaniu, oprogramowaniu układowym i dokumentacji) w całym cyklu życia danego systemu.

Jeśli tak, opisz.

[46] Akronim kategorii zabezpieczeń - zgodnie z NSC 800-53. Dotyczy pkt. 1 do 10 załącznika I.

5. **IA:** Czy zmiany w systemie wpłyną na to, jak (I) są identyfikowani użytkownicy systemu, procesy działające w imieniu użytkowników lub urządzenia oraz (II) jest uwierzytelniana lub weryfikowana tożsamość tych użytkowników, procesów lub urządzeń, jako warunek wstępny umożliwienia dostępu do systemów organizacji.

Jeśli tak, opisz.

6. **MA:** Czy zmiany w systemie wpłyną na sposób (I) przeprowadzania okresowych i terminowych działań związanych z utrzymaniem systemów; oraz (II) zapewniania skutecznych środków bezpieczeństwa dotyczących narzędzi, technik, mechanizmów i personelu wykorzystywanych do utrzymania systemu.

Jeśli tak, opisz.

7. **MP:** Czy zmiany w systemie wpłyną na sposób, w jaki (I) chronione są informacje zawarte w systemach w formie drukowanej lub na nośnikach cyfrowych; (II) dostęp do informacji w formie drukowanej lub na nośnikach cyfrowych usuniętych z systemów jest ograniczony do uprawnionych użytkowników; oraz (III) nośniki cyfrowe są oczyszczane lub niszczone przed usunięciem lub dopuszczeniem do ponownego użycia.

Jeśli tak, opisz.

8. **PE:** Czy zmiany w systemie/środowisku systemowym zmienią sposób, w jaki (I) jest ograniczany do uprawnionych osób fizyczny dostęp do systemów, urządzeń i poszczególnych środowisk produkcyjnych (II) jest chroniony fizyczny obiekt i infrastruktura wspierająca systemy; (III) są dostarczane narzędzia wspierające działanie systemów; (IV) systemy są chronione przed zagrożeniami środowiskowymi; oraz (V) są zapewniane odpowiednie środowiskowe środki bezpieczeństwa w obiektach zawierających systemy.

Jeśli tak, opisz.

9. **SC:** Czy zmiany w systemie wpłyną na: (I) komunikację (tj. informacje przesyłane lub odbierane przez systemy organizacyjne) – jak jest ona monitorowana, kontrolowana i chroniona na granicach zewnętrznych i kluczowych granicach wewnętrznych systemów; oraz (II) sposób wdrażania projektów architektury, technik rozwoju oprogramowania

i zasad inżynierii systemów, które promują skuteczne bezpieczeństwo informacji.

Jeśli tak, opisz.

10.SI: Czy zmiany w systemie wpłyną na to, jak (I) błędy w systemie są identyfikowane, zgłaszane i poprawiane w odpowiednim czasie; (II) jest stosowana ochrona przed złośliwym kodem; (III) są monitorowane i wykrywane zdarzenia systemowe; (IV) jest weryfikowane prawidłowe działanie funkcji bezpieczeństwa; oraz (V) informacje są sprawdzane pod kątem dokładności, kompletności, ważności i autentyczności.

Jeśli tak, opisz.