MC

Tłumaczenie standardów i rekomendacji
w zakresie cyberbezpieczeństwa

Praktyki zarządzania ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw dla systemów i organizacji

NIST SP 800-161r1_wer. 1.0_PL

NIST SP 800-161r1_wer. 1.0_PL

14 czerwca 2024

Praktyki zarządzania ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw dla systemów i organizacji

Publikacja dostępna pod adresem:

Rekomendacje cyberbezpieczeństwa

NIST Special Publication
NIST SP 800-161r1

Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

Jon Boyens
Angela Smith
Nadya Bartol
Kris Winkler
Alex Holbrook
Matthew Fallon

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-161r1

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

Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

Jon Boyens
Angela Smith
Computer Security Division Information Technology Laboratory

Nadya Bartol
Kris Winkler
Alex Holbrook
Matthew Fallon
Boston Consulting Group

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-161r1

May 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Undersecretary of Commerce for Standards and Technology

O PUBLIKACJI

Niniejsze opracowanie **NIST SP 800-161r1_wer. 1.0_PL**, ***Praktyki zarządzania ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw dla systemów i organizacji***, stanowi tłumaczenie publikacji NIST SP 800-161, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, 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

KLAUZULA PRAWNA

Niniejszy dokument został przygotowany na podstawie dokumentu opracowanego przez amerykański Narodowy Instytut Standaryzacji i Technologii (NIST) zgodnie z jego ustawowymi obowiązkami wynikającymi z ustawy rządu federalnego Stanów Zjednoczonych dotyczącej modernizacji zasad bezpieczeństwa informacji (ang. Federal Information Security Modernization Act FISMA) z 2014 roku [44 U.S.C. § 3551 i n.], Public Law (P. L.) 113 283. Obszar odpowiedzialności NIST obejmuje opracowywanie norm oraz wytycznych w zakresie bezpieczeństwa informacji, w tym minimalnych wymagań dotyczących federalnych systemów informatycznych. Opracowane normy i wytyczne nie mogą być jednak stosowane w odniesieniu do krajowych systemów bezpieczeństwa bez wyraźnej zgody stosownych urzędników federalnych odpowiedzialnych za ustalanie zasad dotyczących tych systemów. Wytyczne zawarte w niniejszym dokumencie są zgodne z wymogami opisanymi w okólniku A 120 Biura ds. Zarządzania i Budżetu (ang. Office of Management and Budget – OMB).

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

W niniejszym dokumencie zostały wymienione nazwy wybranych dostępnych na rynku urządzeń, narzędzi, programów lub innych materiałów, zarówno o charakterze komercyjnym, jak i niekomercyjnym. Wykorzystanie takich nazw służy wyłącznie przedstawieniu odpowiednich opisów procedur eksperymentalnych. Wskazanie to nie stanowi reklamy ani promocji jakiegokolwiek produktu lub usługi przez NIST, jak również nie oznacza, że wskazane materiały lub urządzenia stanowią najlepsze dostępne rozwiązania służące osiągnięciu danego celu. Niniejsza publikacja może zawierać odniesienia do innych publikacji opracowywanych przez NIST zgodnie z obowiązkami statutowymi przypisanymi tej organizacji. Informacje zawarte w niniejszej publikacji, w tym koncepcje i metodologie, mogą znaleźć zastosowanie w agencjach federalnych nawet przed ukończeniem wszelkich publikacji towarzyszących. W związku z tym, do czasu zakończenia prac nad każdą publikacją, istniejące wymagania, wytyczne i procedury pozostają w mocy. W związku z celami dotyczącymi planowania i zmian, agencje federalne powinny uważnie śledzić rozwój nowych publikacji NIST. Zachęcamy organizacje do zapoznawania się z publikowanymi wersjami roboczymi publikacji udostępnionymi w celu zgłaszania uwag oraz przekazywania swoich opinii do NIST. Wiele publikacji NIST dotyczących cyberbezpieczeństwa, poza publikacjami wymienionymi powyżej, są dostępne w witrynie internetowej https://csrc.nist.gov/publications.

SPRAWOZDANIA DOTYCZĄCE TECHNOLOGII SYSTEMÓW INFORMACYJNYCH

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

STRESZCZENIE

Organizacje obawiają się ryzyka związanego z produktami i usługami, które mogą zawierać złośliwe funkcje, mogą być podrobione lub mogą zawierać podatności wynikające z niedostatecznie dobrych praktyk produkcyjnych i rozwojowych wykorzystywanych w ramach łańcucha dostaw. Ryzyko to wiąże się z mniejszą widocznością i zrozumieniem przez podmioty sposobu, w jaki nabywana technologia jest rozwijana, integrowana i wdrażana, a także procesów, procedur, standardów i praktyk stosowanych w celu zapewnienia bezpieczeństwa, odporności, niezawodności, integralności i jakości produktów i usług.

Niniejsza publikacja zawiera szereg rekomendacji dla organizacji dotyczących określania, oceny i ograniczania ryzyk związanych z cyberbezpieczeństwem w całym łańcuchu dostaw na wszystkich szczeblach. Publikacja opisuje zarządzanie ryzykiem

Tłumaczenie

dotyczącym cyberbezpieczeństwa w łańcuchu dostaw (*ang. cybersecurity supply chain risk management – C-SCRM*) oraz działania w zakresie zarządzania ryzykiem poprzez zastosowanie wielopoziomowego podejścia opracowanego z myślą o tym obszarze, w tym wytycznych dotyczących opracowania planów wdrażania strategii C-SCRM, polityki C-SCRM, planów C-SCRM oraz oceny ryzyka dla produktów i usług.

SŁOWA KLUCZOWE

Nabywanie (*ang. acquire*); zarządzanie ryzykiem dotyczącym cyberbezpieczeństwa w łańcuchu dostaw cybersecurity supply chain; (*ang. cybersecurity supply chain risk management*- C-SCRM), cyberbezpieczeństwo łańcucha dostaw (*ang. cybersecurity supply chain*); technologie informacyjne i komunikacyjne (*ang. information and communication technology- ICT*); zarządzanie ryzykiem (*ang. risk management*); dostawca (*ang. supplier)*; łańcuch dostaw (*ang. supply chain*); ocena ryzyka w łańcuchu dostaw (*ang. supply chain risk assessment*); zapewnienie łańcucha dostaw (*ang. supply chain assurance*); ryzyko w łańcuchu dostaw (*ang. supply chain risk*); bezpieczeństwo łańcucha dostaw (*ang. supply chain security*).

SPIS TREŚCI

Tłumaczenie

Tłumaczenie

Tłumaczenie

Tłumaczenie

Tłumaczenie

SPIS ILUSTRACJI

SPIS TABEL

1. WSTĘP

Technologie informacyjno-komunikacyjne (ICT)[2] oraz technologie operacyjne i procesy przemysłowe (*ang. operational technology* – OT) wykorzystują złożony i rozproszony na całym świecie, rozległy i wzajemnie powiązany ekosystem łańcucha dostaw, w którego skład wchodzą zróżnicowane trasy oraz zewnętrzni wykonawcy i dostawcy na każdym szczeblu.

W skład ekosystemu wchodzą podmioty sektorów publicznego i prywatnego (w tym między innymi nabywcy, dostawcy, deweloperzy, integratorzy systemów, dostawcy zewnętrznych usług systemowych oraz inni dostawcy usług ICT/OT)[3], które współdziałają ze sobą w celu badania, rozwijania, projektowania, wytwarzania, nabywania, dostarczania, integrowania, obsługiwania, utrzymywania, utylizacji oraz innego wykorzystywania produktów i usług ICT/OT lub zarządzania nimi. Interakcje te są kształtowane przez zróżnicowane technologie, prawa, polityki, procedury oraz praktyki.

Ekosystem ten powstał w celu zapewnienia zaawansowanych, przystępnych cenowo oraz nadających się do wielokrotnego wykorzystania rozwiązań. Podmioty sektora publicznego i prywatnego szybko przyjęły ten ekosystem rozwiązań i zwiększyły swoją zależność od dostępnych na rynku produktów, wsparcia integratorów systemów w przypadku systemów budowanych na zamówienie oraz dostawców zewnętrznych usług. Taka praktyka z kolei spowodowała wzrost złożoności, różnorodności i skali działania tych podmiotów.

W niniejszym dokumencie termin łańcuch dostaw odnosi się do powiązanego zestawu zasobów i procesów zachodzących pomiędzy wieloma poziomami organizacji, z których każdy jest nabywcą, a które rozpoczynają się wraz z pozyskiwaniem produktów i usług i rozciągają się na cały cykl życia produktu i usługi.

[2] *Ang. Information and communications technology (ICT)*

[3] Definicje pojęć takich jak dostawcy, deweloperzy, integratorzy systemów, dostawcy zewnętrznych usług systemowych oraz dostawców innych usług dotyczących ICT/OT znajdują się w Załączniku H, *Słownik*.

Tłumaczenie

Biorąc pod uwagę treść definicji łańcucha dostaw, ***pojęcie ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw***[45] należy rozumieć jako potencjalne szkody lub naruszenia zasad ochrony danych, które mogą powstać w związku z dostawcami, ich łańcuchami dostaw, a także oferowanymi produktami lub usługami. Ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw wynika z zagrożeń wykorzystujących podatności lub luki występujące w produktach i usługach, które przemieszczają się w całym łańcuchu dostaw, a także z zagrożeń wykorzystujących podatności lub luki występujące w samym łańcuchu dostaw. Przykłady zagrożeń cyberbezpieczeństwa w całym łańcuchu dostaw obejmują:

1. Kradzież materiałów projektowych producenta, w co spowodowało utratę własności intelektualnej i udziału w rynku.
2. Zakłócenia w dostawach przez producent kluczowych elementów i podzespołów wymaganych do wytwarzania produktów, spowodowanych atakiem wykorzystującym oprogramowanie ransomware na dostawcę znajdującego się trzy poziomy niżej w łańcuchu dostaw.
3. Naruszenie bezpieczeństwa danych osobowych w sieci sklepów w związane z dostawcą urządzeń grzewczych, wentylacyjnych i klimatyzacyjnych, który miał dostęp do portalu sieci sklepów wykorzystywanego w celu współdzielenia danych.

Należy pamiętać o tym, że zarówno zarządzanie ryzykiem w łańcuchu dostaw, jak i zarządzanie ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw – określane odpowiednio skrótami SCRM oraz C-SCRM – odnoszą się w publikacjach

[4] W wersji normy SP 800-161 z 2015 roku Narodowy Instytut Standaryzacji i Technologii użył terminu „łańcuch dostaw ICT" (*ang. „ICT supply chain"*). W najnowszym wydaniu niniejszego dokumentu NIST celowo odchodzi od tego terminu, jako że ryzyka związane z cyberbezpieczeństwem mogą wystąpić we wszystkich łańcuchach dostaw produktów i usług, w tym zarówno w łańcuchach dostaw technologii informacyjno-komunikacyjnych, jak i łańcuchach dostaw niezwiązanych z technologią.

[5] W ramach działań mających na celu ujednolicenie terminologii, na potrzeby niniejszego dokumentu termin „ryzyko związane z cyberbezpieczeństwem w łańcuchach dostaw" jest równoznaczny z terminem „cyberryzyko w łańcuchach dostaw". Również wyrażenie „zarządzanie ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw" należy uznać za równoważne z wyrażeniem „zarządzanie ryzykiem cyberbezpieczeństwa w łańcuchach dostaw".

Narodowego Instytutu Standaryzacji i Technologii do tej samej koncepcji. W praktyce zarządzanie ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw jest obszarem znajdującym się w punkcie styku tradycyjnego zarządzania ryzykiem w łańcuchu dostaw oraz tradycyjnego bezpieczeństwa informacji. Poszczególne organizacje działające na rynku mogą stosować różne terminy oraz definicje dotyczące SCRM, które nie są objęte zakresem niniejszej publikacji. Niniejsza publikacja nie omawia wielu aspektów SCRM, które nie są związane z cyberbezpieczeństwem.

Rozwiązania technologiczne dostarczane za pośrednictwem łańcucha dostaw, w którego skład wchodzą konkurujący ze sobą dostawcy i sprzedawcy, niosą ze sobą wiele znaczących korzyści – w tym niskie koszty, interoperacyjność, szybkie wprowadzanie innowacyjnych rozwiązań oraz zróżnicowanie funkcji produktów. Niezależnie od tego, czy mowa o rozwiązaniach własnościowych, opracowanych przez organizacje rządowe lub rozwiązaniach otwartoźródłowych (*ang. open source*), każde z takich rozwiązań może zaspokajać potrzeby klientów z sektora publicznego i prywatnego na całym świecie. Jednocześnie te same czynniki, które przyczyniają się do powstawania takich korzyści, zwiększają również ryzyko wystąpienia zagrożeń związanych z cyberbezpieczeństwem, które są bezpośrednio lub pośrednio związane z łańcuchem dostaw. Ryzyka związane z cyberbezpieczeństwem w całym łańcuchu dostaw w wielu przypadkach pozostają niewykryte i mają wpływ zarówno na nabywców technologii i usług, jak i na ich użytkowników końcowych. Wdrożone oprogramowanie zwykle jest produktem komercyjnym obejmującym mniejsze elementy, które także mogą stanowić rozwiązania komercyjne lub otwartoźródłowe, rozwijane lub opracowane przez wiele zróżnicowanych podmiotów. Aktualizacje oprogramowania wdrażanego w podmiotach często nie obejmują aktualizacji jego elementów składowych, które zawierają znane podatności. Dotyczy to także przypadków, w których podatności te można wykorzystać w kontekście oprogramowania wdrożonego w podmiocie. Użytkownicy końcowi oprogramowania często nie mają świadomości lub nie są w stanie wykryć podatności występujących w elementach składowych produktów komercyjnych ze względu na brak przejrzystości, niewystarczające praktyki zarządzania podatnościami oraz inne

czynniki. Ze względu na brak standaryzacji i normalizacji praktyk C-SCRM pojawia się dodatkowa warstwa złożoności – takie działania utrudniają kompleksowy i spójny pomiar zagrożeń oraz zarządzanie ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw zarówno organizacji zamawiającej, jak i poszczególnym podmiotom będącym częścią jej łańcucha dostaw – dostawcom, deweloperom, integratorom systemów, dostawcom zewnętrznych usług systemowych i innym usługodawcom rozwiązań i usług ICT/OT.

Na potrzeby niniejszego dokumentu praktyki oraz regulacje dotyczące zarządzania ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw (C-SCRM) odnoszą się zarówno do środowisk technologii informatycznych (IT), jak i technologii operacyjnych (OT), w tym do urządzeń i technologii internetu rzeczy (IoT). Podobnie jak środowiska IT, które opierają się na produktach i usługach ICT, środowiska OT opierają się na produktach i usługach OT i ICT, przy czym zagrożenia związane z cyberbezpieczeństwem wiążą się z produktami i usługami ICT/OT, a także dostawcami oraz ich łańcuchami dostaw. Podmioty powinny włączyć w zakres swoich działań dotyczących obszaru C-SCRM dostawców rozwiązań OT, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT.

Podczas współpracy z dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych i innymi dostawcami usług związanych z ICT/OT, organizacje powinny uwzględnić szeroki zakres oddziaływania państwa i wysokie prawdopodobieństwo, że poszczególne organizacje mogą egzekwować różne i sprzeczne wymagania dotyczące obszaru C-SCRM. Rozwiązanie tego problemu wymaga koordynacji działań oraz współpracy między organizacjami. o C-SCRM.

Na potrzeby niniejszej publikacji termin „podmiot” jest używany do opisywania poziomu 1 hierarchii zarządzania ryzykiem. Mianem organizacji określamy jednostkę o dowolnej wielkości, złożoności lub umiejscowieniu w ramach większej struktury podmiotu (np. urząd, agencja lub w stosownych przypadkach, któregokolwiek z jego elementów operacyjnych). W świetle tej definicji podmiot jest organizacją, która

funkcjonuje na najwyższym szczeblu hierarchii, gdzie poszczególni liderzy wyższego szczebla ponoszą szczególną odpowiedzialność za zarządzanie ryzykiem [NISTIR 8286]. W skład podmiotu może wchodzić wiele organizacji. W opisanej sytuacji podmiot ma wiele poziomów 1, a zarówno interesariusze, jak i działania są definiowane zarówno na poziomie podmiotu, jak i organizacji. Działania dotyczące poziomu 1 realizowane na szczeblu podmiotu powinny wpływać na działania realizowane w ramach podległych organizacji. Podmioty i organizacje stosują praktyki C-SCRM opisane w niniejszej publikacji w sposób dostosowany do swojej struktury. W niniejszej publikacji występują fragmenty, w których termin „organizacja" został zaczerpnięty z cytowanego źródła, np. innej publikacje NIST bądź stosownych przepisów. Dodatkowe informacje na ten temat znajdują się w dokumencie NISTIR 8286 – *Integrating Cybersecurity and Enterprise Risk Management (ERM)*.

1.1. CEL

Zarządzanie ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw (*ang. Cybersecurity Supply Chain Risk Management – C-SCRM*) to systematyczny proces zarządzania ekspozycją na ryzyko związane z cyberbezpieczeństwem na każdym etapie łańcucha dostaw oraz opracowywania odpowiednich strategii reagowania, stosownych polityk, procesów i procedur. Celem niniejszej publikacji jest dostarczenie podmiotom wskazówek dotyczących identyfikacji, oceny, wyboru i wdrażania procesów zarządzania ryzykiem oraz środków zaradczych w całym podmiocie, aby pomóc w zarządzaniu ryzykiem dotyczącym cyberbezpieczeństwa w całym łańcuchu dostaw. Treść niniejszego dokumentu dotyczy odpowiedzialności różnych obszarów, które charakteryzują się różnymi punktami widzenia na temat zarządzania ryzykiem w łańcuchach dostaw, zarządzanych przez różne podmioty i podlegające różnym przepisom prawa.

Rekomendacje dotyczące zarządzania ryzykiem związanym z cyberbezpieczeństwem w łańcuchach dostaw zawarte w niniejszym dokumencie nie mają uniwersalnego charakteru. Każdy podmiot powinien zatem przeanalizować informacje przedstawione w tej publikacji i dostosować je do własnej sytuacji, uwzględniając przy tym wielkość, dostępne zasoby i okoliczności, a także zagrożenia i ryzyka. Podmioty wdrażające

przedstawione wskazówki mogą wprowadzać i realizować praktyki C-SCRM w różne sposoby. Z tego powodu niniejsza publikacja opisuje praktyki C-SCRM zaobserwowane w podmiotach i przedstawia priorytety wdrażania rzeczonych praktyk, dzieląc je na praktyki podstawowe, podtrzymujące oraz rozwojowe[6], które podmioty mogą wziąć pod uwagę w procesie wdrażania i rozwijania działań w tym zakresie. Dokument ten nie zawiera jednak konkretnych planów, które podmioty mogą wdrażać w celu realizacji takich działań i osiągania ich wymagalności.

Procesy oraz działania opisane w niniejszym dokumencie mogą być modyfikowane lub uzupełniane o specyficzne dla danego podmiotu wymagania wynikające z polityk, wytycznych, strategii reagowania oraz innych źródeł. Publikacja ta umożliwia podmiotom opracowanie strategii C-SCRM dostosowanych do ich specyficznych misji i potrzeb biznesowych, a także konkretnych zagrożeń i środowisk operacyjnych.

1.2. ODBIORCY DOCELOWI

Zarządzanie ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw jest procesem dotyczącym całego podmiotu i jako takie powinno być rozważane z punktu widzenia zarządzania, niezależnie od konkretnej struktury podmiotu.

Z tego powodu niniejsza publikacja ma stanowić pomoc dla zróżnicowanej grupy odbiorców zajmujących się zagadnieniem C-SCRM, do których należą między innymi:

- osoby odpowiedzialne za zarządzanie i nadzór nad systemami, bezpieczeństwem informacji, prywatnością lub ryzykiem, w tym osoby autoryzujące (AO), CIO, CISO, SAOP[7];
- osoby odpowiedzialne za rozwój systemów, w tym osoby odpowiedzialne za realizację misji lub celów biznesowych, menedżerowie programów, inżynierowie systemowi, inżynierowie bezpieczeństwa systemów, inżynierowie ds. ochrony prywatności, osoby odpowiedzialne za rozwój sprzętu i oprogramowania, integratorzy systemów oraz osoby zajmujące się zaopatrzeniem bądź zakupami;

[6] Więcej informacji na ten temat znajduje się w rozdziale 3.4 niniejszej publikacji.

[7] Opisy funkcji / ról – patrz NSC 7298, NSC 800-37. Wymieniając różne tytuły w organizacji nie sugeruje się żadnych szczególnych relacji (partnerskich lub innych) ani linii władzy.

- osoby pełniące obowiązki związane z zarządzaniem projektami, w tym certyfikowani kierownicy projektów oraz członkowie zintegrowanych zespołów projektowych (*ang. Integrated Project Team – IPT*);
- osoby odpowiedzialne za zaopatrzenie i udzielanie zamówień, w tym kierownicy ds. zaopatrzenia oraz kierownicy odpowiedzialni za zamówienia;
- osoby odpowiedzialne za logistykę, w tym menedżerowie programów, kierownicy odpowiedzialni za zamówienia, integratorzy systemów i zarządcy nieruchomości;
- osoby odpowiedzialne za wdrażanie i funkcjonowanie systemów bezpieczeństwa i prywatności, w tym osoby odpowiedzialne za realizację misji lub celów biznesowych, osoby odpowiedzialne za systemy, właściciele informacji lub władający informacjami, administratorzy systemów, osoby odpowiedzialne za planowanie ciągłości działalności oraz kierownicy ds. bezpieczeństwa lub prywatności;
- osoby odpowiedzialne za ocenę i monitorowanie bezpieczeństwa i prywatności, w tym audytorzy, osoby odpowiedzialne za ocenę systemów, osoby szacujące zabezpieczenia, niezależni weryfikatorzy i osoby zatwierdzające, a także analitycy oraz
- podmioty komercyjne, w tym partnerzy przemysłowi, którzy wytwarzają produkty i systemy składowe, tworzą technologie związane z bezpieczeństwem i prywatnością, świadczą usługi lub zapewniają możliwości zwiększające bezpieczeństwo lub prywatność informacji.

1.3. WYTYCZNE DLA DOSTAWCÓW USŁUG CHMUROWYCH

Do omawianych w niniejszej publikacji *dostawców zewnętrznych usług systemowych* należą także dostawcy *usług chmurowych*. Niniejsza publikacja nie zastępuje wytycznych dotyczących oceny bezpieczeństwa dostawców usług chmurowych przez krajowy organ bezpieczeństwa. W ramach stosowania tej publikacji w kontekście dostawców usług chmurowych, podmioty publiczne powinny najpierw skorzystać z wytycznych dotyczących bezpieczeństwa usług chmurowych określonych w uchwale nr 97 Rady Ministrów dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa”[8].

[8] MP. z 2019 r., poz. 862

1.4. PROFILE GRUP DOCELOWYCH ORAZ WSKAZÓWKI DOTYCZĄCE KORZYSTANIA Z NINIEJSZEGO DOKUMENTU

Ze względu na szeroki krąg odbiorców niniejszej publikacji, autorzy określili kilka profili czytelników, aby skuteczniej wskazać im te części dokumentu, które w największym stopniu odpowiadają ich potrzebom. Niektórzy czytelnicy niniejszej publikacji będą należeć do wielu grup – w takiej sytuacji powinni rozważyć przeczytanie wszystkich stosownych sekcji. Każdy czytelnik odpowiedzialny za wdrożenie programów lub działań związanych z obszarem C-SCRM w danym podmiocie, niezależnie od roli, powinien uznać cały niniejszy dokument jako istotny z punktu widzenia tego celu.

1.4.1. Osoby odpowiedzialne za zarządzanie ryzykiem w podmiocie oraz osoby odpowiedzialne i operatorzy C-SCRM

Czytelnicy należący do tej grupy to osoby odpowiedzialne za zarządzanie ryzykiem w podmiocie oraz zarządzanie ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw. Czytelnicy ci mogą pomagać w opracowywaniu polityk i standardów C-SCRM, przeprowadzić ocenę ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw oraz pełnić rolę ekspertów merytorycznych dla reszty podmiotu. Czytelnicy o takim profilu powinni przeczytać cały niniejszy dokument.

1.4.2. Osoby odpowiedzialne za procesy, misję, procesy biznesowe oraz operatorzy podmiotów i organizacji

Czytelnicy o takim profilu to osoby odpowiedzialne za działania, które prowadzą do powstania ryzyka w podmiocie lub wiążą się z zarządzaniem ryzykiem. Mogą być także osobami odpowiedzialnymi za ryzyko w ramach swoich obowiązków związanych z realizacją misji lub procesów biznesowych. Mogą być odpowiedzialni za zarządzanie ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw podmiotu. Czytelnicy należący do tej grupy mogą poszukiwać ogólnej wiedzy i wytycznych dotyczących zarządzania ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw. Polecane treści obejmują między innymi:

- Rozdział 1: Wprowadzenie,
- Rozdział 2: Integracja praktyk C-SCRM z zarządzaniem ryzykiem w skali całego podmiotu,

- Rozdział 3.3: Świadomość i szkolenie w zakresie C-SCRM,
- Rozdział 3.4: Kluczowe praktyki w zakresie C-SCRM,
- Rozdział 3.6: Materiały,
- Załącznik A: Środki bezpieczeństwa związane z C-SCRM,
- Załącznik B: Podsumowanie środków bezpieczeństwa związanych z C-SCRM,
- Załącznik E: FASCSA.

1.4.3. Operatorzy oraz osoby odpowiedzialne za zaopatrzenie i zamówienia

Czytelnicy należący do tej grupy to osoby, na których spoczywa odpowiedzialność za praktyki w zakresie C-SCRM w ramach pracy na stanowisku osób odpowiedzialnych za zamówienia oraz zaopatrzenie podmiotu. Osoby zajmujące się zamówieniami mogą realizować działania związane z C-SCRM w ramach swoich ogólnych obowiązków w cyklu życia zamówień i zaopatrzenia. Osoby te ściśle współpracują z osobami odpowiedzialnymi za praktyki C-SCRM w podmiocie w celu realizacji działań C-SCRM w obszarze zamówień oraz zaopatrzenia. Polecane treści obejmują między innymi:

- Rozdział 1: Wprowadzenie;
- Rozdział 2.1: Uzasadnienie biznesowe dotyczące praktyk C-SCRM;
- Rozdział 2.2: Ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw;
- Rozdział 3.1: Praktyki C-SCRM w zamówieniach;
- Rozdział 3.3: Świadomość i szkolenie w zakresie C-SCRM;
- Załącznik A: Środki bezpieczeństwa związane z C-SCRM;

  Czytelnicy powinni zwrócić szczególną uwagę na wymagane zabezpieczenia dotyczące umów z dostawcami i uwzględnić je w umowach zarówno z wykonawcami głównymi, jak i podwykonawcami;
- Załącznik F: Wytyczne dotyczące bezpieczeństwa łańcucha dostaw oprogramowania.

1.4.4. Operatorzy zajmujący się bezpieczeństwem informacji, prywatnością lub cyberbezpieczeństwem

Czytelnicy należący do tej grupy są odpowiedzialni za ochronę poufności, integralności i dostępności kluczowych procesów i systemów informacyjnych podmiotu. W ramach tych obowiązków czytelnicy ci mogą być bezpośrednio lub pośrednio zaangażowani w przeprowadzanie oceny ryzyka związanego z cyberbezpieczeństwem w łańcuchu dostaw, a także wybór oraz wdrożenie środków bezpieczeństwa związanych z C-SCRM. W mniejszych podmiotach osoby te mogą ponosić odpowiedzialność za wdrożenie praktyk C-SCRM, w związku z czym powinny zapoznać się z rozdziałem 1.3.1 w celu uzyskania dodatkowych wskazówek. Polecane treści obejmują między innymi:

- Rozdział 1: Wprowadzenie,
- Rozdział 2.1: Uzasadnienie biznesowe dotyczące praktyk C-SCRM,
- Rozdział 2.2: Ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw,
- Rozdział 3.2: Wymiana informacji dotyczących łańcucha dostaw,
- Rozdział 3.4: Kluczowe praktyki w zakresie C-SCRM,
- Załącznik A: Środki bezpieczeństwa związane z C-SCRM,
- Załącznik B: Podsumowanie środków bezpieczeństwa związanych z C-SCRM,
- Załącznik C: Ramy narażenia na ryzyko,
- Załącznik G: Działania związane z C-SCRM w procesie zarządzania ryzykiem,
- Załącznik E: FASCSA,
- Załącznik F: Wytyczne dotyczące bezpieczeństwa łańcucha dostaw oprogramowania.

1.4.5. Osoby odpowiedzialne za rozwój systemów, inżynierię systemów oraz wdrożenia systemów

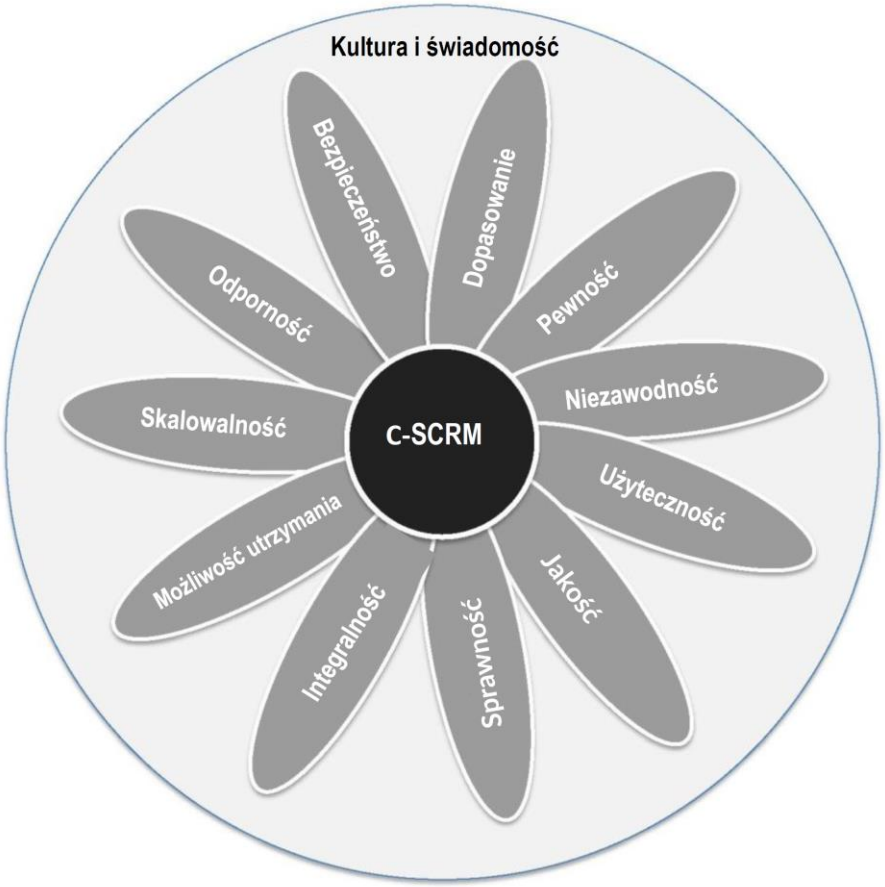
Czytelnicy należący do tej grupy są odpowiedzialni za wykonywanie czynności w ramach cyklu życia systemu. W ramach obowiązków w tym zakresie, czytelnicy ci odpowiadają za realizację działań związanych z C-SCRM na poziomie operacyjnym.

W szczególności osoby te mogą zajmować się wdrożeniem środków bezpieczeństwa związanych z C-SCRM w celu zarządzania ryzykiem dotyczącym cyberbezpieczeństwa wynikającym z produktów i usług dostarczanych za pośrednictwem łańcucha dostaw w zakresie obsługiwanych systemów. Polecane treści obejmują między innymi:

- Rozdział 1: Wprowadzenie,
- Rozdział 2.1: Uzasadnienie biznesowe dotyczące praktyk C-SCRM,
- Rozdział 2.2: Ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw,
- Rozdział 2.3.4: Poziom 3 – operacyjny,
- Załącznik A: Środki bezpieczeństwa związane z C-SCRM,
- Załącznik B: Podsumowanie środków bezpieczeństwa związanych z C-SCRM,
- Załącznik C: Ramy narażenia na ryzyko,
- Załącznik F: Wytyczne dotyczące bezpieczeństwa łańcucha dostaw oprogramowania,
- Załącznik G: Działania związane z C-SCRM w procesie zarządzania ryzykiem.

1.5. INFORMACJE OGÓLNE

C-SCRM obejmuje działania obejmujące cały cykl życia systemu, w tym działalność badawczo-rozwojową, projektowanie, rozwój, zamówienia, dostawy, integrację, obsługę, utrzymanie, utylizację, a także ogólne zarządzanie produktami i usługami podmiotu. Podmioty powinny włączyć działania związane z C-SCRM w ramach cyklu życia systemu, ze względu na fakt, że jest to obszar kluczowy dla rozwiązywania problemów dotyczących cyberbezpieczeństwa w całym łańcuchu dostaw. Praktyki C-SCRM to zorganizowane i celowe zarządzanie ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw. Wdrożenie C-SCRM wymaga od podmiotu świadomości oraz zrozumienia problematyki. Jako obszar łączy w sobie wymiary związane z bezpieczeństwem, niezawodnością, użytecznością, jakością, integralnością, wydajnością, skalowalnością, możliwością utrzymania, a także odpornością – dodatkowe informacje znajdują się na rys. 1-1. Każdy z tych wymiarów jest obszarem, które poszczególne podmioty muszą wziąć pod uwagę w ramach swojego podejścia do działań związanych z C-SCRM. Co więcej, każde realizowane działania związane z C-SCRM powinny mieć pozytywny wpływ na te procesy.



Rysunek 1-1: Wymiary C-SCRM

- **Kultura i świadomość (*ang. Culture and Awareness*)** to zbiór wspólnych wartości, praktyk, celów i postaw organizacji, które umożliwiają skuteczne wdrożenie praktyk związanych z C-SCRM. Obszar ten obejmuje proces nauki, który wpływa na postawy i rozumienie jednostki i podmiotu w celu uświadomienia znaczenia C-SCRM i negatywnych konsekwencji zaniedbań w tym obszarze[9].
- **Bezpieczeństwo (*ang. Security*)** zapewnia poufność, integralność i dostępność (a) informacji opisujących łańcuch dostaw (takich jak informacje o ścieżkach produktów i usług, zarówno logicznych, jak i fizycznych); (b) informacji, produktów i usług, które przemieszczają się w łańcuchu dostaw (np. własności intelektualnej zawartej w produktach i usługach); bądź (c) informacji o uczestnikach łańcucha dostaw (tj. osób stykających się z produktem lub usługą w całym cyklu życia).

[9] NIST SP 800-16

- **Odpowiedniość (*ang. Suitability*)** to aspekt gwarantujący, że łańcuch dostaw oraz dostarczane produkty i usługi były właściwe i odpowiednie z punktu widzenia podmiotu i realizowanego celu.
- **Pewność (*ang. Safety*)** gwarantuje, że produkt lub usługa nie mogą spowodować śmierci, obrażeń, chorób zawodowych, uszkodzeń lub zniszczenia sprzętu lub mienia, a także zniszczeń środowiskowych[10].
- **Niezawodność (*ang. Reliability*)** koncentruje się na zdolności produktu lub usługi do funkcjonowania zgodnie z przeznaczeniem przez określony czas w przewidywalny sposób[11].
- **Użyteczność (*ang. Usability*)** dotyczy stopnia, w jakim produkt lub usługa mogą być używane przez określonych użytkowników do osiągnięcia określonych celów ze stosowną efektywnością, wydajnością i satysfakcją w określonym kontekście użytkowania[12].
- **Jakość (*ang. Quality*)** koncentruje się na spełnianiu lub przekraczaniu specyfikacji wydajnościowych, technicznych i funkcjonalnych przy jednoczesnym ograniczaniu podatności i słabości, które mogą ograniczać zamierzoną funkcję komponentu lub realizację usługi, prowadzić do awarii komponentu lub usługi lub stwarzać możliwości przeprowadzenia ataku.
- **Efektywność (*ang. Efficiency*)** skupia się na terminowości zamierzonego rezultatu działania produktu lub usługi.
- **Możliwość utrzymania (*ang. Maintainability*)** dotyczy łatwości wprowadzenia zmian i ulepszeń na podstawie przeszłych doświadczeń w celu rozszerzenia przyszłych korzyści.
- **Integralność (*ang. Integrity*)** skupia się na ochronie produktów i ich składników przed modyfikacją lub manipulacją oraz zapewnieniu autentyczności i weryfikowalnej historii.

[10] NIST SP 800-160 Vol.2

[11] NIST SP 800-160 Vol.2

[12] NIST SP 800-63-3

- **Skalowalność (*ang. Scalability*)** określa możliwość obsługi zwiększonego wzrostu i zapotrzebowania przez produkt lub usługę.
- **Odporność (*ang. Resilience*)** skupia się na zapewnieniu, że produkt, usługa lub łańcuch dostaw wspierają zdolność podmiotu do przygotowania się i dostosowania do zmieniających się warunków, a także skutecznego przetrwania oraz szybkiego powrotu do normalnego funkcjonowania w przypadku zakłóceń. Odporność obejmuje możliwość ochrony przed celowymi atakami oraz odzyskania sprawności po ich zakończeniu, a także odzyskania sprawności po wypadkach, zdarzeniach naturalnych lub katastrofach.

1.5.1. Łańcuch dostaw podmiotu

Współczesne podmioty wykorzystują złożone systemy i sieci informacyjne w celu realizacji swoich misji. Te systemy i sieci informacyjne składają się z produktów i komponentów ICT/OT[13] udostępnianych przez *dostawców*, *deweloperów* oraz *integratorów systemów*. Podmioty nabywają i wdrażają również szereg produktów i usług, w tym:

- Oprogramowanie na zamówienie wykorzystywane w systemach informacyjnych, tworzonej udostępnione przez *deweloperów* z myślą o wdrożeniu przez podmioty.
- Wsparcie operacyjne, utrzymaniowe oraz utylizacyjne w zakresie systemów informacyjnych oraz sieci informatycznych w obrębie podmiotu i poza nim[14], realizowane przez *integratorów systemów lub innych dostawców usług związanych z ICT/OT*.
- Usługi zewnętrzne wspierające działalność podmiotu, które znajdują się zarówno wewnątrz, jak i na zewnątrz granic autoryzacji, udostępniane przez *dostawców zewnętrznych usług systemowych*.

[13] Definicja Technologii operacyjnej (*ang. Operational Technology - OT*) – patrz NSC 7298.

[14] W przypadku systemów informacyjnych podmiotów publicznych mowa o granicy autoryzacji zdefiniowanej w NSC 7298.

Usługi te mogą obejmować cały cykl życia systemu informacyjnego lub usługi i mogą być:

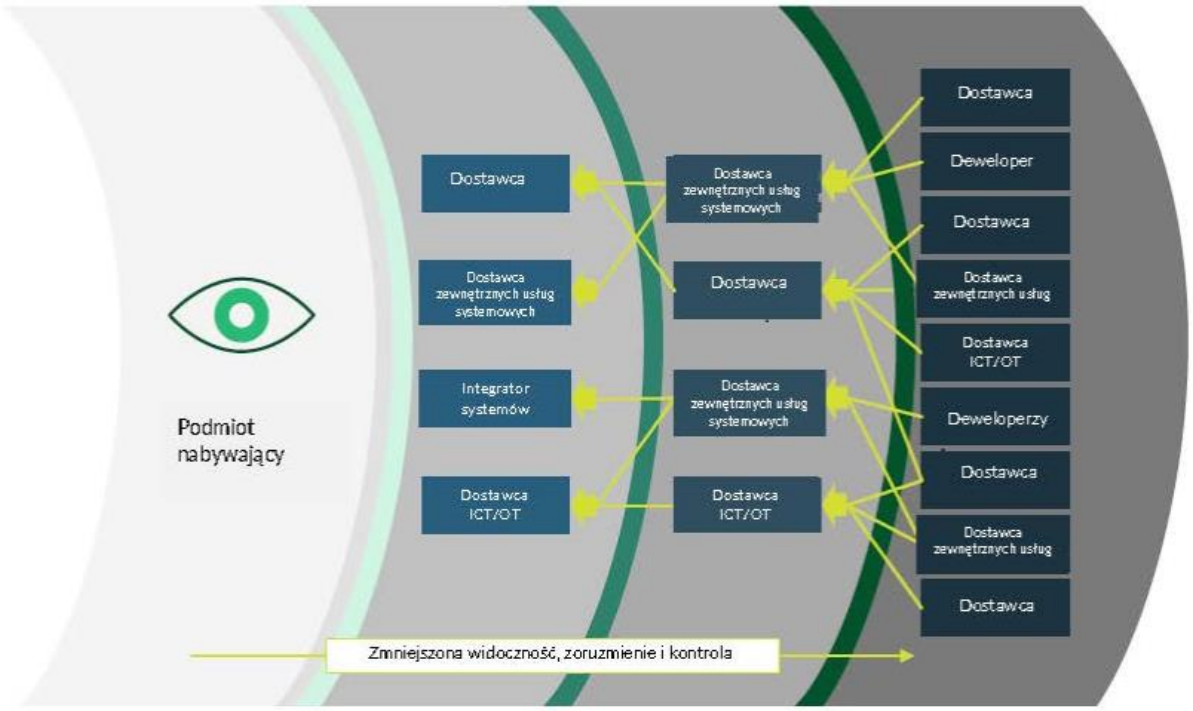
- realizowane przez pracowników zatrudnionych przez podmiot, dewelopera, integratora systemu lub dostawcę zewnętrznych usług systemowych;
- fizycznie hostowane przez podmiot, dewelopera, integratora systemu lub dostawcę zewnętrznych usług systemowych;
- wspierane przez lub składające się ze środowisk rozwojowych, środowisk logistycznych/dostawy, które pozwalają na transport systemów informacyjnych oraz ich elementów, a także stosownych interfejsów systemowych i komunikacyjnych;
- sprzęt i oprogramowanie własnościowe, otwartoźródłowe lub komercyjne.

Odpowiedzialność za usługi i związane z nimi działania wykonywane przez różne strony w ramach tego ekosystemu jest zazwyczaj określana w dokumentach umownych pomiędzy podmiotem a jego dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych oraz innymi dostawcami usług związanych z ICT/OT.

1.5.2. Relacje pomiędzy dostawcami a podmiotami

Podmioty są uzależnione od łańcucha dostaw w zakresie dostarczania różnorodnych produktów i usług, które umożliwiają im realizację celów strategicznych i operacyjnych. Identyfikację ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw komplikuje asymetria informacji występująca pomiędzy podmiotami nabywającymi a ich dostawcami i usługodawcami. Podmioty nabywające często nie mają informacji i nie rozumieją, w jaki sposób nabyta technologia jest rozwijana, integrowana i wdrażana oraz w jaki sposób świadczone są nabywane przez nich usługi. Ponadto podmioty nabywające, w których procesy, procedury i praktyki związane z C-SCRM są niedostateczne lub nie istnieją, mogą być narażone na zwiększone ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw. Poziom narażenia na ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw zależy w dużej mierze od związku między dostarczanymi produktami i usługami a kluczowym charakterem misji, procesów biznesowych i systemów, które

wspierają. Podmioty utrzymują różnorodne relacje ze swoimi dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych oraz innymi dostawcami usług związanych z ICT/OT. Rysunek 1-2 przedstawia, w jaki sposób te różnorodne relacje wpływają na widoczność i kontrolę podmiotów nad łańcuchami dostaw.



Rysunek 1-2: Widoczność, zrozumienie i kontrola łańcucha dostaw przez podmioty

Niektóre relacje w łańcuchu dostaw są ze sobą ściśle powiązane, na przykład opracowanie przez integratora systemu złożonego systemu informacyjnego działającego w granicach autoryzacji podmiotu publicznego lub zarządzanie systemami i zasobami informacyjnymi podmiotu publicznego przez zewnętrznego usługodawcę. Relacje te są zwykle oparte na umowie lub kontrakcie – dokumencie, który ustanawia szczegółowe wymagania funkcjonalne, techniczne oraz dotyczące bezpieczeństwa, a dodatkowo może przewidywać opracowanie na zamówienie lub znaczące dostosowanie produktów i usług do określonych potrzeb i wymagań. W przypadku tych relacji, integratorzy systemów i dostawcy zewnętrznych usług są prawdopodobnie w stanie współpracować z podmiotem w celu wdrożenia takich procesów i zabezpieczeń (wymienionych w niniejszym dokumencie), które są uznane

za stosowne w oparciu o wyniki oceny krytyczności i ryzyka oraz analizę kosztów i korzyści. Może to obejmować stawianie wymagań na wyższym szczeblu łańcucha dostaw, aby w większym stopniu zagwarantować realizację niezbędnych celów w zakresie wiarygodności. Każda decyzja o postawieniu takich wymagań musi obejmować także ocenę wykonalności i opłacalności takiego przedsięwzięcia. Rozważając poziom oczekiwań wobec integratorów systemów i dostawców zewnętrznych usług w zakresie wdrażania procesów oraz zabezpieczeń dotyczących działań w zakresie C-SCRM należy uwzględnić ryzyko, jakie dla podmiotu stanowi nieprzestrzeganie tych dodatkowych wymogów. W wielu przypadkach bezpośrednia współpraca z integratorami systemów i dostawcami zewnętrznych usług w celu proaktywnego określenia odpowiednich procesów łagodzenia i zabezpieczeń pozwala opracować bardziej opłacalną strategię.

Zamawianie produktów ICT/OT od dostawców powoduje nawiązanie bezpośredniej relacji pomiędzy tymi dostawcami a podmiotami nabywającymi. Także ta relacja często opiera się na umowie pomiędzy podmiotem nabywającym i dostawcą. Komercyjne technologie ICT/OT opracowane przez dostawców są zwykle projektowane do celów ogólnych na potrzeby rynku globalnego i nie są dostosowane do specyficznych środowisk operacyjnych lub zagrożeń dotyczących poszczególnych klientów. Podmioty powinny przeprowadzić szczegółowe analizy oraz badania dotyczące specyficznych wymagań w zakresie C-SCRM, aby określić, czy rozwiązanie IT jest odpowiednie do określonego celu[15], czy zawiera wymagane opcje i możliwości bezpieczeństwa, czy spełnia oczekiwania dotyczące jakości i odporności oraz wymaga wsparcia ze strony dostawcy dla produktu lub jego komponentów w całym cyklu życia.

Oceny wyników analiz produktu przez nabywcę, które mogą obejmować między innymi bezpośrednie rozmowy z dostawcami, gdy tylko jest to możliwe, pomoże nabywcom zrozumieć cechy i możliwości istniejących produktów i usług ICT/OT,

[15] Użyte określenie jest wykorzystywane do nieformalnego opisania procesu, elementu konfiguracji, usługi IT lub innych rozwiązań zdolnych do spełnienia swoich celów lub zapewnienia usługi na odpowiednim poziomie. Spełnienie tego wymogu wymaga odpowiedniego projektu, wdrożenia, zabezpieczeń oraz utrzymania. (Pojęcie zostało zaadaptowane z dokumentu Information Technology Infrastructure Library (ITIL) Service Strategy [ITIL Service Strategy]).

określić oczekiwania i wymagania wobec dostawców oraz zidentyfikować potrzeby w zakresie C-SCRM niezaspokojone jeszcze przez rynek. Może również pomóc w identyfikacji nowych rozwiązań, które mogą przynajmniej częściowo zaspokoić potrzeby nabywcy. Takie analizy i kontakt z dostawcami pozwalają nabywcy na lepsze sformułowanie swoich wymagań, aby dostosować je do produktów dostępnych na rynku, kierować rozwojem rozwiązań, a także podejmować oparte na ryzyku decyzje dotyczące zamówień, konfiguracji i wykorzystania produktów w swoim środowisku.

Zarządzanie kosztami i zasobami

Zrównoważenie narażenia na ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw z kosztami i korzyściami wynikającymi z wdrożenia praktyk i środków bezpieczeństwa C-SCRM powinno być kluczowym elementem ogólnego podejścia podmiotu zamawiającego do C-SCRM.

Podmioty powinny mieć świadomość, że wdrożenie praktyk i środków bezpieczeństwa C-SCRM wymaga dodatkowych zasobów finansowych i ludzkich. Wymaganie większego poziomu testów, dokumentacji lub zabezpieczeń od dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT może spowodować wzrost ceny produktu lub usługi, co może skutkować zwiększeniem kosztów dla podmiotu zamawiającego. Dotyczy to zwłaszcza tych produktów i usług, które zostały opracowane do zastosowań ogólnych i nie są dostosowane do specyficznych wymagań podmiotu w zakresie bezpieczeństwa lub C-SCRM. Podejmując decyzje w zakresie wymagań oraz wdrażania praktyk i zabezpieczeń C-SCRM, podmioty zamawiające powinny wziąć pod uwagę zarówno koszty wdrożenia tych środków zabezpieczających, jak i ryzyko zaniechania ich wdrożenia.

Jeśli jest to możliwe i stosowne, podmioty zamawiające powinny umożliwić dostawcom, deweloperom, integratorom systemów, dostawcom zewnętrznym usług systemowych oraz innym dostawcom usług związanych z ICT/OT ponowne wykorzystanie stosownych istniejących danych i dokumentacji, które mogą stanowić dowód wdrożenia praktyk w zakresie C-SCRM, takich jak na przykład certyfikacja dostawcy na zgodność z odpowiednią normą, taką jak ISO 27001. Takie postępowanie skutkuje oszczędnością kosztów dla zamawiającego i dostawcy. W niektórych przypadkach ponowne

wykorzystanie dokumentacji może nie być właściwym rozwiązaniem, ponieważ mogą być potrzebne dodatkowe lub inne informacje, a także może być wymagana ponowna szacowania – taka sytuacja może mieć miejsce, na przykład, gdy uprzednio kontrolowany dostawca opracował nowy produkt, który jeszcze nie trafił do produkcji.

Niezależnie od tego, podmioty zamawiające powinny określić i uwzględnić kwestie bezpieczeństwa na wczesnym etapie procesu zamówienia.

1.6. METODOLOGIA TWORZENIA WYTYCZNYCH C-SCRM NA PODSTAWIE DOKUMENTÓW NSC 800-39; NSC 800-37 ORAZ NSC 800-53 WER. 2

Niniejsza publikacja opiera się na wielopoziomowym podejściu do zarządzania ryzykiem opisanym w dokumencie [NSC 800-39] opisując wytyczne dotyczące C-SCRM na szczeblu podmiotu, misji i operacji. Wprowadza również system nawigacji dotyczący dokumentu [NSC-37] pozwalający użytkownikom łatwiej skupić się na odpowiednich rozdziałach niniejszej publikacji. Zawiera także rozszerzony opis konkretnych zabezpieczeń dotyczących działań w zakresie C-SCRM, oparty na dokumencie [NSC 800-53, wer. 2].

Rekomendacje oraz zabezpieczenia opisane w niniejszej publikacji opierają się na istniejących praktykach multidyscyplinarnych i mają na celu zwiększenie zdolności podmiotów do ograniczania ryzyk związanych z cyberbezpieczeństwem w całym łańcuchu dostaw przez cały cykl życia systemów, produktów i usług. Warto mieć na uwadze, że niniejsza publikacja zapewnia podmiotom elastyczność w zakresie opracowania samodzielnej dokumentacji obejmującej polityki, plany oceny oraz autoryzacji, a także strategii C-SCRM lub zintegrowania jej z istniejącą dokumentacją.

W przypadku poszczególnych systemów wytyczne te powinny być stosowane do wszystkich systemów informacyjnych we wszystkich kategoriach wpływu, zgodnie z dokumentem [NSC 199]. Podmioty publiczne mogą zdecydować o priorytetowym zastosowaniu niniejszych wytycznych do systemów o wyższym poziomie wpływu lub do określonych komponentów systemów. Co więcej, niniejszy dokument opisuje opracowanie i wdrożenie Strategii i Planów Wdrożenia C-SCRM w zakresie rozwoju na szczeblu podmiotu, biznesu oraz misji, a także planu systemu C-SCRM na poziomie operacyjnym podmiotu. Plan C-SCRM na poziomie operacyjnym opiera się na ocenach ryzyka związanego z cyberbezpieczeństwem w łańcuchu dostaw i powinien zawierać

środki zabezpieczające C-SCRM dostosowane do konkretnych misji i potrzeb biznesowych organizacji, środowisk operacyjnych oraz technologii wykonawczych.

Włączenie do procesu zarządzania ryzykiem

Procesy zawarte w niniejszej publikacji powinny być zintegrowane z istniejącymi cyklami życia systemów podmiotu oraz środowiskami na wszystkich poziomach procesów i hierarchii zarządzania ryzykiem, zgodnie z opisem zawartym w dokumencie [NSC 800-39]. W rozdziale 2 przedstawiono przegląd hierarchii i podejścia do zarządzania ryzykiem [NSC 800-39] oraz zidentyfikowano działania C-SCRM w procesie zarządzania ryzykiem. Załącznik C opiera się na rozdziale 2 dokumentu [NSC 800-39] i zawiera opisy oraz objaśnienia zarządzania ryzykiem w łańcuchu dostaw rozwiązań ICT/OT. Struktura załącznika C odzwierciedla dokument [NSC 800-39].

Wdrażanie C-SCRM w kontekście dokumentu NIST SP/NSC 800-37, Revision 2

Działania C-SCRM opisane w niniejszej publikacji są ściśle związane z Ramami Zarządzania Ryzykiem opisanymi w dokumencie [NSC 800-37]. Procesy C-SCRM realizowane na szczeblu operacyjnym powinny ściśle odzwierciedlać bądź służyć jako dane wejściowe do kroków wykonanych na podstawie dokumentu [NSC 800-37]. Działania C-SCRM zrealizowane na poziomach 1 i 2 powinny dostarczyć danych wejściowych (np. wyników oceny ryzyka) do procesów na poziomie operacyjnym i procesów związanych z ramami zarządzania ryzykiem tam, gdzie jest to możliwe i gdzie ma to zastosowanie. Rozdział 2 i załącznik C opisują bardziej szczegółowo powiązania między praktykami C-SCRM oraz dokumentem [NSC 800-37].

1.7. ZWIĄZEK Z INNYMI PUBLIKACJAMI I PODSUMOWANIE PUBLIKACJI

Niniejsza publikacja opiera się na koncepcjach proponowanych w innych publikacjach NIST i dostosowuje te koncepcje do wykorzystania w ramach zarządzania ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw. Ze względu na ten fakt niniejsza publikacja zawiera wiele koncepcji i odwołuje się do innych publikacji NIST w celu dogłębnego opisania podstawowych ram, koncepcji i metodologii. Lista rzeczonych publikacji NIST obejmuje:

- **NIST Cybersecurity Framework (CSF) Version 1.1:** Dobrowolne wytyczne oparte na istniejących normach, wytycznych i praktykach dla organizacji w celu lepszego zarządzania ryzykiem związanym z cyberbezpieczeństwem oraz jego ograniczania. Dokument został opracowany z myślą o wspieraniu komunikacji w zakresie zarządzania ryzykiem i cyberbezpieczeństwem zarówno wśród wewnętrznych, jak i zewnętrznych interesariuszy organizacji.
- **NSC 199, *Standardy kategoryzacji bezpieczeństwa*:** Rekomendacja dotycząca kategoryzacji informacji i systemów informacyjnych w podmiotach [publicznych na podstawie zastrzeżeń dotyczących poufności, integralności oraz dostępności, a także potencjalnego wpływu na aktywa i operacje organizacji w przypadku, gdyby ich informacje i systemy informacyjne zostały skompromitowane poprzez nieautoryzowany dostęp, wykorzystanie, ujawnienie, zakłócenie, modyfikację lub zniszczenie.
- **NSC 800-30 Przewodnik dotyczący postępowania w zakresie oceny ryzyka w podmiotach realizujących zadania publiczne:** Rekomendacje do przeprowadzania oceny ryzyka systemów informacyjnych i podmiotów publicznych, rozbudowujące wskazówki zawarte w dokumencie NSC 800-39. Ocena ryzyka przeprowadzane na wszystkich trzech szczeblach hierarchii zarządzania ryzykiem są częścią ogólnego procesu zarządzania ryzykiem, który dostarcza liderom/dyrektorom wyższego szczebla informacji niezbędnych do określenia odpowiednich kierunków działania w odpowiedzi na zidentyfikowane ryzyko.
- NSC 800-37, *Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu*: Opisuje ramy zarządzania ryzykiem i przedstawia rekomendacje dotyczące stosowania tych ram w systemach informacyjnych i organizacjach. Ramy zarządzania ryzykiem stanowią zdyscyplinowany, uporządkowany i elastyczny proces zarządzania ryzykiem w zakresie bezpieczeństwa i ochrony prywatności, który obejmuje kategoryzację bezpieczeństwa informacji, wybór, wdrożenie i ocena zabezpieczeń, zabezpieczenia wspólne oraz autoryzację systemów, a także ciągłe monitorowanie.

- **NSC 800-39, *Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego*:** Dokument zawiera wskazówki dotyczące zintegrowanego, obejmującego całą organizację programu zarządzania ryzykiem bezpieczeństwa informacji dotyczącego operacji organizacyjnych – misji, funkcji, wizerunku i reputacji, aktywów organizacji, osób fizycznych, innych organizacji i państwa wynikającym z działania i użytkowania systemów informacyjnych.
- **NSC 800-53, wer. 2, *Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji*:** Dokument zawiera katalog środków bezpieczeństwa oraz zapewniania prywatności dotyczący systemów informacyjnych oraz organizacji w celu ochrony operacji i aktywów organizacyjnych, osób fizycznych, innych organizacji i państwa przed zróżnicowanymi zagrożeniami i ryzykiem, które obejmują wrogie ataki, błędy ludzkie, klęski żywiołowe, awarie, działalność obcych wywiadów oraz zagrożenia dla prywatności.
- **NSC 800-53B, *Zabezpieczenia bazowe systemów informacyjnych oraz organizacji*:** Dokument zawiera zestaw minimalnych zabezpieczeń prywatności i środków bezpieczeństwa dla organizacji. Istnieją trzy zestawy minimalnych zabezpieczeń – po jednym dla każdego poziomu wpływu systemu (tj. niskiego, umiarkowanego i wysokiego), a także zestaw minimalnych zabezpieczeń prywatności stosowanych w przypadku systemów niezależnie od poziomu wpływu;
- **NIST SP 800-160 Vol. 1, *Systems Security Engineering*:** Prezentuje punkt widzenia inżynierii oraz działania niezbędne do rozwoju systemów lepiej przystosowanych do obrony oraz wytrzymałych systemów, w tym maszyn, elementów fizycznych i ludzkich składających się na systemy, a także możliwości i usługi realizowane przez te systemy.
- **NIST SP 800-160 Vol. 2, Revision 1, *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*:** Podręcznik zawierający rekomendacje pozwalające na osiągnięcie określonych rezultatów w zakresie cyberbezpieczeństwa oparty na perspektywie inżynierii systemów

Tłumaczenie

z uwzględnieniem procesów cyklu życia w połączeniu z procesami zarządzania ryzykiem, który pomaga organizacjom w wykorzystaniu doświadczenia i wiedzy do określenia właściwych rozwiązań dostosowanych do potrzeb i celów.

- **NIST SP 800-181, Revision 1, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*:** Podstawowy dokument dotyczący opisywania i udostępniania informacji o działaniach w zakresie cyberbezpieczeństwa. Informacje na ten temat są opisane w postaci stwierdzeń dotyczących zadań, wiedzy i umiejętności, które stanowią podstawę dla osób zgłębiających to zagadnienie, w tym studentów, osób poszukujących pracy i pracowników.
- **NISTIR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems*:** Dokument opisuje różnorodne praktyki, które pomagają zmniejszyć ryzyko związane z łańcuchem dostaw dotyczące systemów informacyjnych. Celem opracowania tego dokumentu było wyposażenie organizacji w zestaw powtarzalnych i komercyjnie uzasadnionych metod i praktyk zapewniania wiarygodności łańcucha dostaw, obejmujące działania pozwalające na zrozumienie oraz uzyskanie widoczności w całym łańcuchu dostaw.
- **NISTIR 8179, *Criticality Analysis Process Model: Prioritizing Systems and Components*:** Dokument pomaga organizacjom w identyfikacji najistotniejszych systemów i ich komponentów, które mogą wymagać dodatkowego zabezpieczenia lub innej ochrony.
- **NISTIR 8276, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*:** Dokument przedstawia zestaw najważniejszych praktyk, które każda organizacja może wykorzystać do zarządzania ryzykiem związanym z cyberbezpieczeństwem w swoich łańcuchach dostaw. Najważniejsze praktyki przedstawione w tym dokumencie mogą być wykorzystane do wdrożenia działań związanych z C-SCRM w organizacji niezależnie od jej wielkości, zasięgu bądź złożoności. Praktyki te łączą informacje zawarte w istniejących materiałach standaryzacyjnych i branżowych dotyczących zagadnienia C-SCRM z informacjami zebranymi podczas inicjatyw badawczych NIST realizowanymi w 2015 i 2019 roku.

- **NISTIR 8286, *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (ERM)*:** Dokument pomaga poszczególnym organizacjom wchodzącym w skład podmiotów ulepszyć informacje dotyczące ryzyk związanych z cyberbezpieczeństwem, które stanowią informacje na potrzeby procesów związanych z zarządzaniem ryzykiem w podmiocie poprzez komunikację i udostępnianie informacji o ryzyku.
- **NISTIR 8286A, *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management*:** Dokument zawiera przykłady i informacje ilustrujące tolerowanie ryzyka, apetyt na ryzyko[16] oraz metody określania ryzyka w tym kontekście. Sprawozdanie opisuje dokumentację różnych scenariuszy opartych na potencjalnym wpływie zagrożeń i podatności na aktywa podmiotu w celu usprawnienia procesu opracowywania rejestru ryzyka podmiotu. Udokumentowanie prawdopodobieństw i wpływu różnych zagrożeń w rejestrach ryzyka związanego z cyberbezpieczeństwem połączone z profilem ryzyka podmiotu pomaga w późniejszym ustaleniu priorytetów i komunikacji w zakresie reagowania i monitorowania ryzyka.
- **NISTIR 8286B, *Prioritizing Cybersecurity Risk for Enterprise Risk Management*:** Dokument opisuje szczegółowe wskazówki dotyczące ryzyka dla interesariuszy oraz identyfikacji i analizy ryzyka. Publikacja opisuje potrzebę określenia priorytetu każdego ryzyka w świetle ich potencjalnego wpływu na cele podmiotu, jak również opcje radzenia sobie z ryzykiem. Autorzy sprawozdania opisują, w jaki sposób priorytety ryzyka i informacje dotyczące reakcji na ryzyko są dodawane do rejestru ryzyka dotyczącego cyberbezpieczeństwa (*ang. Cybersecurity Risk Register – CSRR*) w ramach ogólnego rejestru ryzyka utrzymywanego przez podmiot. Informacje o wyborze i przewidywanych kosztach reakcji na ryzyko będą wykorzystywane do utrzymania kompleksowej widoczności ryzyka związanego z cyberbezpieczeństwem całego podmiotu,

[16] Apetyt na ryzyko określa maksymalny poziom dopuszczalnego ryzyka przy wyznaczaniu limitów i ograniczeń na poszczególne ryzyka cząstkowe oraz poziom, po przekroczeniu którego podejmowane są określone działania zarządcze niezbędne do ograniczenia dalszego wzrostu ryzyka.

który można wykorzystać do potwierdzenia i dostosowania strategii dotyczącej ryzyka w celu zapewnienia skutecznej realizacji jego misji.

W publikacji wykorzystano również koncepcje i prace opracowane na potrzeby innych przepisów, norm, sprawozdań, wytycznych i najlepszych praktyk. Pełna lista tych zasobów znajduje się w załączniku J do niniejszego dokumentu.

Najważniejsze wnioski[17]

Łańcuch dostaw. Systemy ICT/OT opierają się na globalnie rozproszonym, wzajemnie połączonym ekosystemie łańcucha dostaw, w którego skład wchodzą podmioty sektora publicznego i prywatnego (w tym nabywcy, dostawcy, deweloperzy, integratorzy systemów, dostawcy zewnętrznych usług systemowych i dostawcy innych usług związanych z ICT/OT).

Produkty i usługi łańcucha dostaw. Produkty i usługi, w zakresie których podmioty polegają na łańcuchu dostaw; obejmują dostarczanie systemów i komponentów systemów, oprogramowania otwartoźródłowego oraz oprogramowania na zamówienie, usługi wsparcia operacyjnego, hosting systemów i usług oraz wsparcie systemów.

Korzyści i ryzyko w łańcuchu dostaw. Ekosystem oferuje szereg korzyści, obejmujących oszczędność kosztów, interoperacyjność, szybsze tempo wdrażania innowacji, zróżnicowanie funkcjonalności produktów oraz możliwość wyboru pomiędzy konkurującymi dostawcami. Mechanizmy, które zapewniają te korzyści, mogą również być źródłem wielu zagrożeń związanych z cyberbezpieczeństwem w całym łańcuchu dostaw – na przykład w wyniku przerwy w działalności dostawcy powodującej obniżenie poziomu usług i prowadzącej do niezadowolenia klientów podmiotu.

Zarządzanie ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw (ang. Cybersecurity Supply Chain Risk Management – C-SCRM). Jak opisano w niniejszej publikacji, zarządzanie ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw (C-SCRM) to systematyczny proces, który ma na celu pomóc

[17] Najważniejsze wnioski opisują kluczowe informacje zawarte w tekście rozdziału. Definicje znajdują się w glosariuszu, który stanowi Załącznik H do niniejszego dokumentu.

podmiotom w zarządzaniu ryzykiem w tym obszarze działalności. Podmioty powinny określić, wdrożyć i dostosować praktyki opisane w niniejszym dokumencie w sposób możliwie najlepiej dostosowany do swojego wyjątkowego kontekstu strategicznego, operacyjnego i ryzyka.

Zakres C-SCRM. C-SCRM obejmuje szeroki wachlarz grup interesariuszy zajmujących się obszarami takimi jak bezpieczeństwo i prywatność informacji, deweloperów systemów oraz podmioty odpowiedzialne za ich wdrożenie, a także osoby odpowiedzialne za zamówienia, zaopatrzenie, kwestie prawne oraz kadrowe. C-SCRM obejmuje działania, dotyczące całego cyklu życia systemu, począwszy od rozpoczęcia prac, a kończąc na jego utylizacji. Ponadto określone ryzyka związane z cyberbezpieczeństwem w całym łańcuchu dostaw powinny być zagregowane i umieszczone w kontekście procesów zarządzania ryzykiem w podmiocie, aby zapewnić, że podmiot rozumie globalne narażenie swoich kluczowych operacji na różne rodzaje ryzyka (np. ryzyko finansowe, ryzyko strategiczne).

2. INTEGRACJA DZIAŁAŃ W OBSZARZE C-SCRM Z ZARZĄDZANIEM RYZYKIEM W SKALI CAŁEGO PODMIOTU[18]

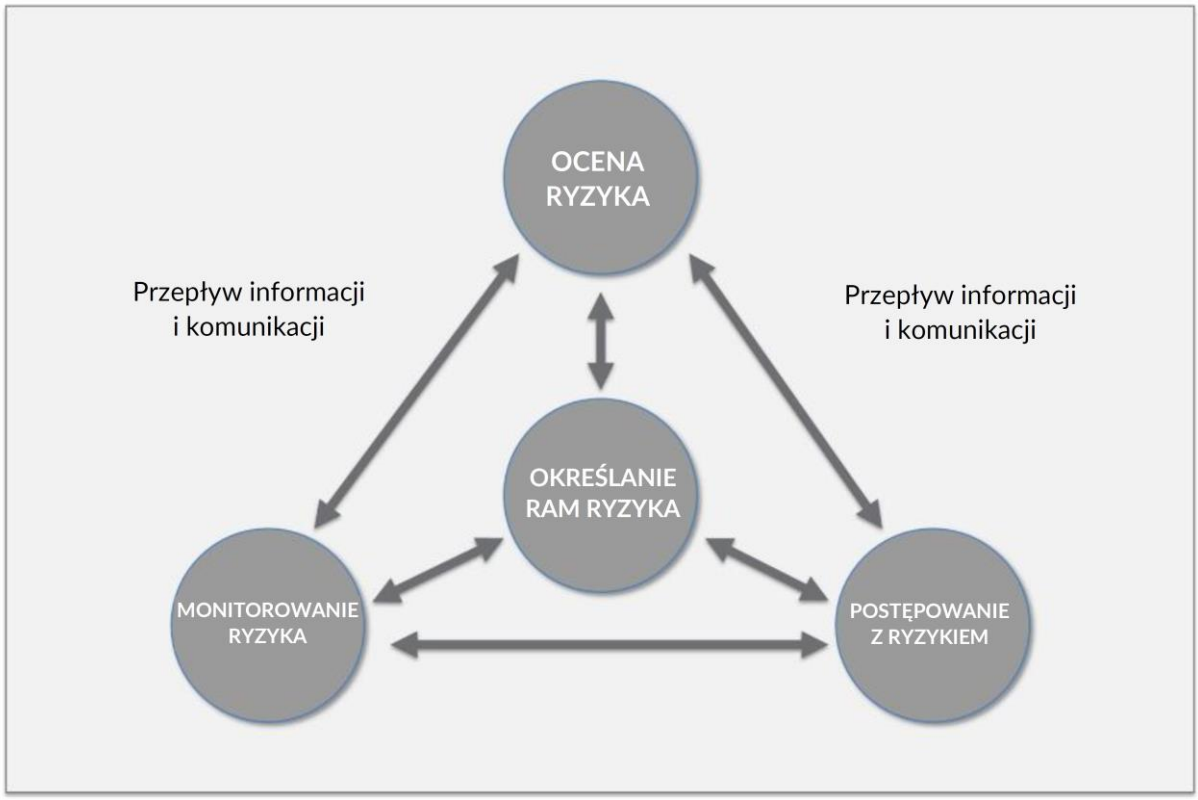
Praktyki dotyczące C-SCRM powinny zostać włączone do procesu zarządzania ryzykiem w skali całego podmiotu opisanego w dokumencie [NSC 800-39] i przedstawionego na rys. 2-1. Proces ten obejmuje następujące etapy realizowane w sposób ciągły oraz w ramach procesów iteracyjnych:

- *Ramy ryzyka (ang. Frame risk).* Ustalenie kontekstu dla decyzji związanych z ryzykiem oraz aktualnego stanu technologii i usług informacyjno-komunikacyjnych podmiotu, a także związanych z nim łańcuchów dostaw.
- *Ocena ryzyka (ang. Assess risk).* Przegląd i interpretacja krytyczności, zagrożenia, podatności, prawdopodobieństwa[19], wpływu oraz powiązanych informacji.
- *Postępowanie z ryzykiem (ang. Respond to risk).* Wybór, dostosowanie i wdrożenie środków zaradczych na podstawie wyników oceny ryzyka.
- *Monitorowanie ryzyka (ang. Monitor risk).* Stałe monitorowanie narażenia na ryzyko i skuteczności ograniczania ryzyka, w tym monitorowanie zmian w systemie informacyjnym lub łańcuchu dostaw przy użyciu skutecznej komunikacji w podmiocie i informacji zwrotnych w celu ciągłego doskonalenia.

Tłumaczenie

[18] Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

[19] W związku z praktykami C-SCRM, pojęcie prawdopodobieństwa (*ang. likelihood*) jest definiowane jako częstość/pewność (*ang. probability*) wykorzystania luki przez zagrożenie w określonym czasie. Warto zauważyć, że w matematyce prawdopodobieństwo oraz rachunek prawdopodobieństwa stanowią zasadniczo różne pojęcia, jednak opis różnicy między nimi wykracza poza zakres niniejszej publikacji.



Rysunek 2-1: Proces zarządzania ryzykiem

Zarządzanie ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw jest złożonym przedsięwzięciem, które wymaga transformacji kulturowej, a także wdrożenia skoordynowanego, wielodyscyplinarnego podejścia w całym podmiocie.

Skuteczne zarządzanie ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw (C-SCRM) wymaga zaangażowania interesariuszy wewnątrz podmiotu (np. poszczególnych działów i procesów), a także poza nim (np. dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT) do aktywnej współpracy, komunikacji i podejmowania działań w celu zapewnienia skuteczności praktyk C-SCRM. Skuteczność praktyk C-SCRM wymaga zmiany kulturowej w całym podmiocie, prowadzącej do osiągnięcia stanu podwyższonej świadomości i gotowości w odniesieniu do potencjalnych konsekwencji zagrożeń związanych z cyberbezpieczeństwem w całym łańcuchu dostaw.

Podmioty powinny dążyć do tego, aby w swoich podejściach do zarządzania ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw uwzględniać punkty widzenia przedstawicieli wielu obszarów i procesów – bezpieczeństwa informacji, zaopatrzenia, zarządzania ryzykiem w podmiocie, inżynierii, rozwoju oprogramowania, IT, działów prawnych, działów kadr itd. Podmioty mogą określić wyraźne role w celu połączenia i zintegrowania tych procesów w ramach szerszych działań w zakresie zarządzania ryzykiem. To kompleksowe podejście stanowi ważną część starań mających na celu określenie priorytetów działań w zakresie C-SCRM, opracowania rozwiązań i włączenia C-SCRM do ogólnych decyzji dotyczących zarządzania ryzykiem. Podmioty powinny realizować działania w zakresie C-SCRM w ramach procesów zamówień, cyklu życia systemów oraz szeroko pojętych procesów zarządzania ryzykiem. Zintegrowane działania w zakresie C-SCRM obejmują określenie krytyczności funkcji i ich zależności od dostarczanych produktów i usług, identyfikację i ocenę istniejących ryzyk, określenie odpowiednich działań łagodzących, dokumentowanie wybranych reakcji na ryzyko oraz monitorowanie wyników działań C-SCRM. ze względu na to, że narażenie na ryzyko związane z łańcuchem dostaw różni się w zależności od podmiotu, a czasem nawet w jego obrębie. Strategie i polityki związane z działalnością i misją powinny nadawać ton i kierunek działań C-SCRM w całym podmiocie.

Organizacje powinny dołożyć wszelkich starań, by dostosowane plany C-SCRM były projektowane tak, aby:

- występowało w nich zarządzanie ryzykiem, zamiast jego eliminacji – ryzyko jest nieodłączną częścią dążenia do zwiększania wartości;
- gwarantowały, że operacje będą w stanie dostosować się do nowych lub rozwojowych zagrożeń;
- odpowiadały na zmiany w obrębie organizacji, programów i wspierających je systemów informacyjnych oraz
- dostosowywały się do szybko zmieniających się praktyk w globalnym łańcuchu dostaw ICT w sektorze prywatnym.

2.1. UZASADNIENIE BIZNESOWE DOTYCZĄCE PRAKTYK C-SCRM

Obecnie każdy podmiot w dużym stopniu wykorzystuje technologię cyfrową w realizacji swojej działalności oraz misji. Technologie te obejmują produkty ICT/OT realizowane dzięki usługom oraz wspierane przez nie. Działania w zakresie C-SCRM jest krytyczną zdolnością, którą musi posiąść każdy podmiot zamierzający rozwiązać problem zagrożeń związanych z cyberbezpieczeństwem w całym łańcuchu dostaw, które wynikają z wykorzystania technologii cyfrowych. Głębokość, zakres i dojrzałość działań dotyczących obszaru C-SCRM realizowanych przez każdy podmiot powinna być oparta na wyjątkowości jego działalności lub misji, specyficznych dla podmiotu wymogach zgodności, środowisku operacyjnym, apetycie na ryzyko oraz tolerowaniu ryzyka.

Stworzenie oraz utrzymanie działań w zakresie C-SCRM stwarza szereg istotnych korzyści:

- Ustanowienie działań w zakresie C-SCRM pozwala podmiotom zrozumieć, które z kluczowych aktywów są najbardziej podatne na i zakłócenia w łańcuchu dostaw.
- Działania w zakresie C-SCRM zmniejszają prawdopodobieństwo kompromitacji łańcucha dostaw w związku z zagrożeniami związanymi z cyberbezpieczeństwem poprzez zwiększenie zdolności podmiotu do skutecznego wykrywania zdarzeń, reagowania na nie oraz powrotu do normalnego działania po zdarzeniach, które skutkują znacznymi zakłóceniami działalności w przypadku naruszenia zasad ochrony C-SCRM.
- Efektywność operacyjna i podmiotu jest osiągana dzięki jasnej strukturze, celom oraz dostosowaniu do możliwości C-SCRM, a także wyznaczanie priorytetów, konsolidację i usprawnienie istniejących procesów C-SCRM.
- Działania w tym zakresie dają większą pewność, że nabywane produkty są wysokiej jakości, wiarygodne, niezawodne, odporne, możliwe do utrzymania, bezpieczne i pewne.
- Działania dają większą pewność, że dostawcy, usługodawcy oraz dostarczane przez nich produkty i usługi technologiczne są godne zaufania i można na nich polegać w zakresie spełniania wymagań dotyczących wydajności.

Działania w zakresie C-SCRM mają fundamentalne znaczenie dla wszelkich wysiłków ukierunkowanych na ograniczanie narażenia na ryzyko wynikające z działalności podmiotu. Wdrożenie procesów i środków zabezpieczających związanych z praktykami C-SCRM wymaga inwestycji w pracowników, narzędzia i infrastrukturę ze strony podmiotów zamawiających, a także deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT. Podmioty mają jednak ograniczone zasoby, które mogą przeznaczyć na ustanowienie i wdrożenie procesów i zabezpieczeń związanych z praktykami dotyczącymi C-SCRM. W związku z tym podmioty powinny dokładnie przeanalizować potencjalne koszty i korzyści w procesie podejmowania decyzji o podjęciu działań związanych z zarządzaniem ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw. Ponadto, wszelkie decyzje powinny być podejmowane w oparciu o jasne zrozumienie wszelkich implikacji związanych z narażeniem na ryzyko, które może wynikać z zaniedbania kwestii C-SCRM.

Chociaż należy uwzględnić kompromisy między kosztami a korzyściami, potrzeba lepszego zabezpieczenia łańcuchów dostaw jest koniecznością zarówno dla sektora publicznego, jak i sektora prywatnego.

2.2. RYZYKO ZWIĄZANE Z CYBERBEZPIECZEŃSTWEM W ŁAŃCUCHACH DOSTAW

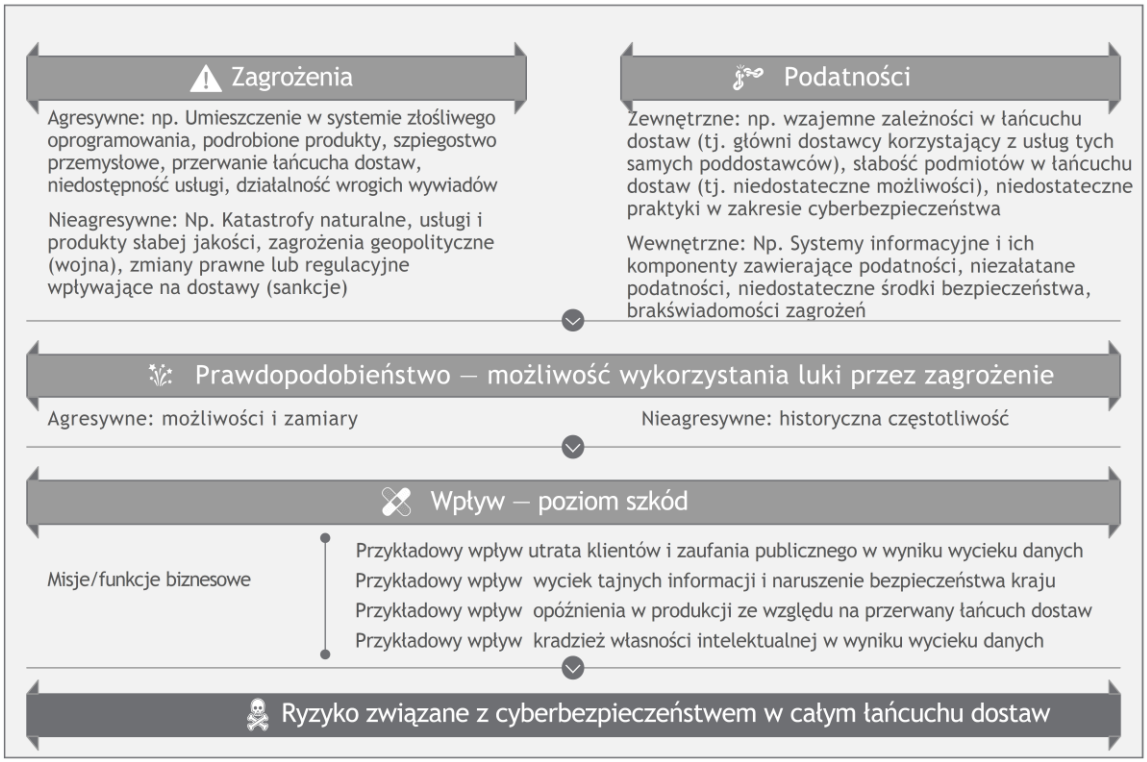
Ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw odnosi się do potencjalnych zniszczeń lub skompromitowania systemów, które wynikają z ryzyka związanego z cyberbezpieczeństwem stwarzanego przez dostawców, ich łańcuchy dostaw oraz ich produkty lub usługi. Przykłady tych zagrożeń obejmują:

- Kradzież wrażliwej własności intelektualnej przez pracowników integratora systemów, co spowoduje utratę znacznej przewagi konkurencyjnej[20].
- Wprowadzenie złośliwego oprogramowania do dostarczanych przez dostawców komponentów produktów używanych w systemach sprzedawanych organizacjom przez przedstawiciela innego państwa. Naruszenie skutkujące utratą kontraktów handlowych.

[20] Kwalifikacja ryzyka w zakresie cyberbezpieczeństwa w całym łańcuchu dostaw dotycząca zagrożeń wewnętrznych dotyczy w szczególności przypadków zagrożeń wewnętrznych ze strony osób trzecich.

- Ponowne wykorzystanie kodu zawierającego podatności przez integratora systemów, co prowadzi do wycieku danych o kluczowym znaczeniu dla bezpieczeństwa narodowego.
- Wprowadzenie na rynek podrobionych produktów przez zorganizowaną grupę przestępczą, co powoduje utratę zaufania klientów.
- Wymiana etykiet na produktach dostarczonych przez niesprawdzonych dostawców przez podmiot zatrudniony do wytwarzania kluczowego komponentu bardziej złożonego systemu. Naruszenie skutkujące wdrożeniem do systemu niezaufanego komponentu przy braku zaufanego dostawcy części zamiennych.

Do realizacji takiego ryzyka dochodzi, gdy zagrożenia związane z cyberbezpieczeństwem w łańcuchu dostaw wykorzystują istniejące luki. Rysunek 2-2 przedstawia ryzyko związane z cyberbezpieczeństwem w łańcuchu dostaw wynikające z prawdopodobieństwa wykorzystania podatności przez odpowiednie zagrożenia oraz wynikające z tego potencjalne skutki.



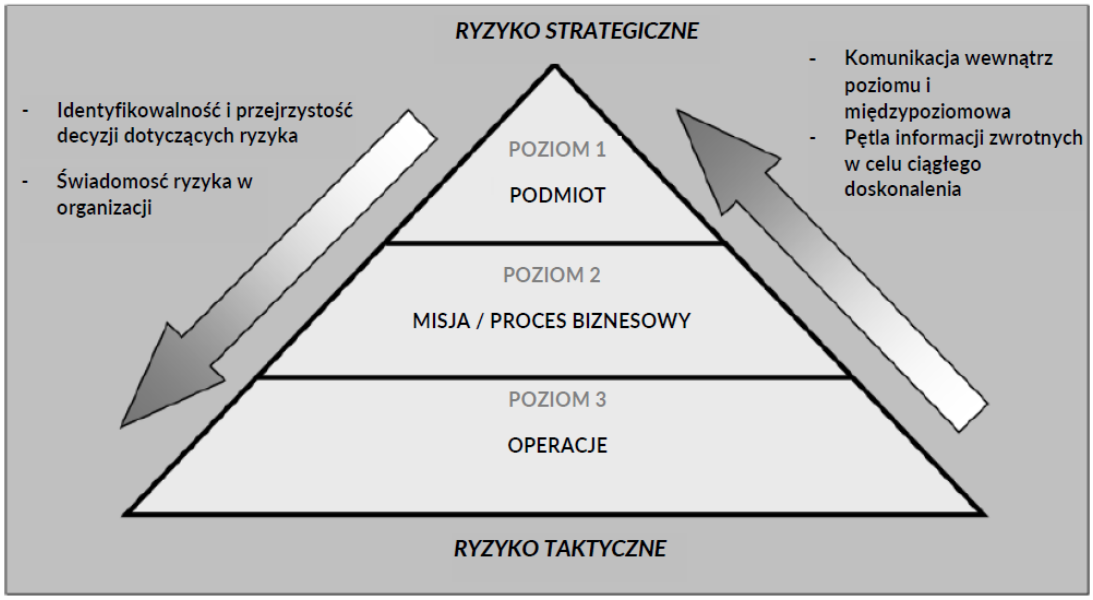
Rysunek 2-2: Zagrożenia związane z cyberbezpieczeństwem w całym łańcuchu dostaw

Tłumaczenie

Podatności dotyczące cyberbezpieczeństwa w łańcuchu dostaw mogą prowadzić do trwałego negatywnego wpływu na realizację misji przez podmiot, począwszy od obniżenia poziomu usług prowadzącego do niezadowolenia klientów, po kradzież własności intelektualnej lub degradację krytycznych działań i procesów biznesowych. Wykorzystanie lub odkrycie takich podatności może jednak zająć lata. Trudne może być również ustalenie, czy dane zdarzenie było bezpośrednim wynikiem podatności łańcucha dostaw. Podatności w łańcuchu dostaw są często wzajemnie powiązane i mogą narażać podmiot na kaskadowe ryzyko związane z cyberbezpieczeństwem. Na przykład przerwa w świadczeniu usług na dużą skalę u ważnego dostawcy usług chmurowych może spowodować zakłócenia w świadczeniu usług lub produkcji dla wielu organizacji w łańcuchu dostaw podmiotu i mieć negatywny wpływ na realizację wielu misji i procesów biznesowych.

2.3. WIELOPOZIOMOWE ZARZĄDZANIE RYZYKIEM[21]

Aby zintegrować zarządzanie ryzykiem w całym podmiocie, dokument [NSC800-39] opisuje trzy poziomy, przedstawione na rys. 2-3, które służą ocenie ryzyka z różnych perspektyw: 1) poziom podmiotu, 2) poziom misji i procesów biznesowych oraz 3) poziom operacyjny. Działania w zakresie C-SCRM wymagają zaangażowania na każdym z trzech poziomów.



Rysunek 2-3: Wielopoziomowe zarządzanie ryzykiem w skali całego podmiotu[22]

[21] Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

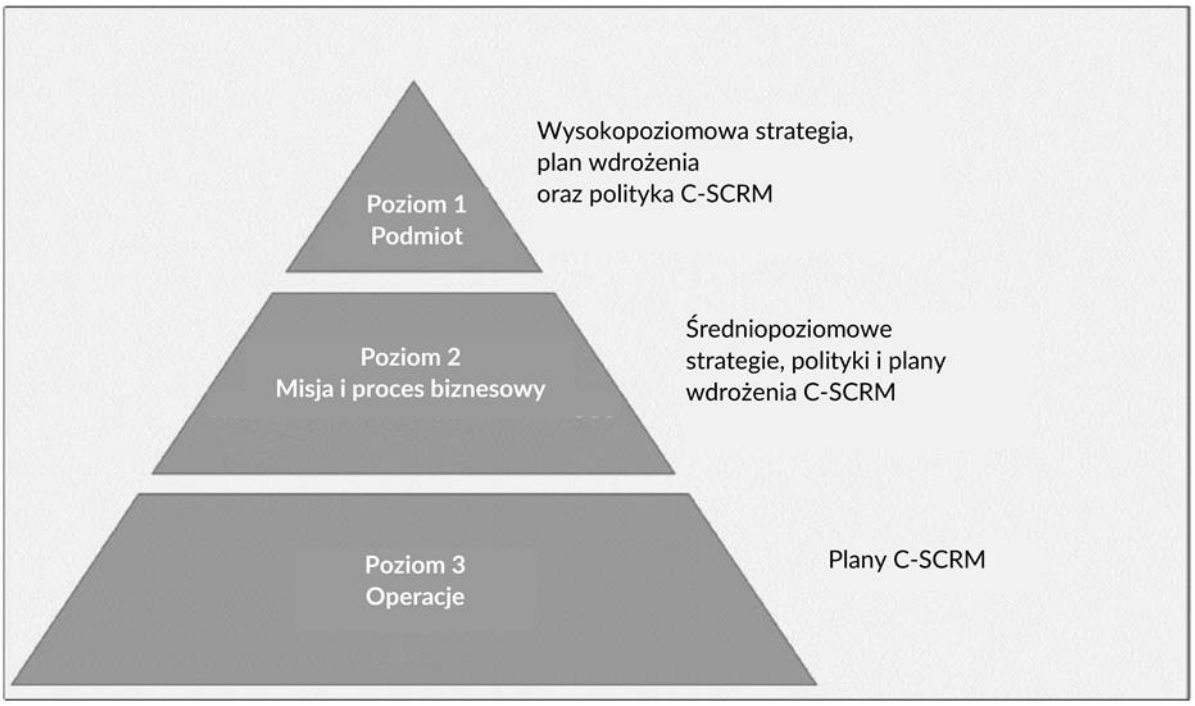
[22] Dodatkowe informacje na temat koncepcji przedstawionych na rys. 2-2 można znaleźć w dokumencie [NSC 800-39].

W wielopoziomowym zarządzaniu ryzykiem proces C-SCRM jest płynnie realizowany na trzech poziomach, a jego ogólnym celem jest ciągłe doskonalenie działań podmiotu związanych z ryzykiem oraz skuteczna komunikacja międzypoziomowa i wewnątrzpoziomowa wśród interesariuszy zainteresowanych działaniami w tym zakresie.

Działania C-SCRM mogą być realizowane przez różne osoby lub grupy w ramach podmiotu, począwszy od pojedynczej osoby, poprzez zespoły, oddziały, scentralizowane biura programowe lub inne struktury. Działania C-SCRM są odmienne dla różnych podmiotów w zależności od ich struktury, kultury, misji i wielu innych czynników. Działania C-SCRM na każdym z trzech poziomów obejmują produkcję różnych wysokopoziomowych produktów C-SCRM.

- Na poziomie 1 ogólna strategia C-SCRM, polityka i plan wdrożenia ustalają ogólny kierunek, strukturę zarządzania i granice dotyczące zarządzania działaniami w ramach C-SCRM w całym podmiocie i kierują działaniami C-SCRM wykonywanymi na poziomie misji i procesów biznesowych.
- Na poziomie 2 strategie, polityki i plany wdrożeniowe C-SCRM średniego szczebla przyjmują kontekst i kierunek określony na poziomie podmiotu i dostosowują go do konkretnej misji i procesu biznesowego.
- Na poziomie 3 plany działań w zakresie C-SCRM stanowią podstawę do określenia, czy system informacyjny spełnia wymagania biznesowe, funkcjonalne i techniczne oraz czy zawiera odpowiednio dopasowane zabezpieczenia. Na plany te duży wpływ ma kontekst i kierunek nadany na poziomie 2.

Rysunek 2-4 przedstawia przegląd wielopoziomowej struktury zarządzania ryzykiem oraz powiązanych strategii, polityk i planów opracowanych na każdym poziomie. Bardziej szczegółowe omówienie poszczególnych działań na każdym poziomie znajduje się w podrozdziałach od 2.3.1 do 2.3.5.



Rysunek 2-4: Dokumenty C-SCRM w procesie wielopoziomowego zarządzania ryzykiem w podmiocie

2.3.1. Role i obowiązki na każdym z trzech poziomów

Wdrożenie działań w zakresie C-SCRM wymaga od podmiotów ustanowienia skoordynowanego podejścia opartego na zespole i modelu współodpowiedzialności w celu skutecznego zarządzania ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw. Podmioty powinny ustanowić polityki dotyczące C-SCRM i przestrzegać ich wytycznych, a także stosowne procesy – często obejmujące wiele podmiotów, a także stosować programowe i techniczne środki łagodzenia skutków. Skoordynowane podejście zespołowe, zarówno doraźne, jak i formalne, umożliwia podmiotom skuteczne przeprowadzenie kompleksowej analizy łańcucha dostaw oraz reagowanie na ryzyko, komunikację z zewnętrznymi partnerami/interesariuszami, a także osiągnięcie konsensusu dotyczącego przydziału odpowiednich zasobów na potrzeby działań C-SCRM. Zespół C-SCRM powinien współpracować przy podejmowaniu decyzji i działań wynikających z zaangażowania wielu punktów widzenia oraz wiedzy specjalistycznej. Zespół wykorzystuje procesy C-SCRM, które powinny być przypisane do poszczególnych podmiotów lub obszarów, jednak nie przejmuje ich realizacji. Skuteczne

wdrożenia działań w zakresie C-SCRM często obejmują przyjęcie modelu wspólnej odpowiedzialności, który rozdziela obowiązki i odpowiedzialność za działania i ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw na zróżnicowaną grupę interesariuszy. Przykłady działań C-SCRM, w których podmioty korzystają z podejścia multidyscyplinarnego, obejmują opracowanie strategii zaopatrzenia na poziomie strategicznym, włączenie wymogów C-SCRM do zamówień publicznych, a także ustalenie możliwości najlepszego sposobu ograniczenia określonych ryzyk dotyczących łańcucha dostaw, zwłaszcza takich, które zostały uznane za znaczące.

W skład zespołu C-SCRM powinna wejść zróżnicowana grupa osób zaangażowanych w różne obszary związane z kluczowymi procesami podmiotu, takich jak bezpieczeństwo informacji, zaopatrzenie, zarządzanie ryzykiem podmiotu, inżynieria, rozwój oprogramowania, IT, kwestie prawne czy kwestie kadrowe. Aby skutecznie pomóc w realizacji działań w zakresie C-SCRM, osoby te powinny zapewnić wiedzę specjalistyczną w zakresie procesów i praktyk podmiotu właściwych dla swojego obszaru wiedzy oraz zrozumienie aspektów technicznych i współzależności systemów lub informacji przepływających przez systemy. Zespół do spraw C-SCRM może być rozszerzeniem istniejącego pionu odpowiedzialnego za zarządzanie ryzykiem, stanowić część pionu zarządzania ryzykiem związanym z cyberbezpieczeństwem podmiotu lub działać w ramach innego działu.

Kluczem do stworzenia multidyscyplinarnych zespołów do spraw C-SCRM jest przełamanie barier pomiędzy różnymi pionami podmiotu, które dążą do rozbieżnych celów. Wiele podmiotów rozpoczyna ten proces odgórnie, powołując grupę roboczą lub radę złożoną z liderów wyższego szczebla, reprezentujących niezbędne i odpowiednie obszary. Należy opracować plan określający cele, zadania, zarząd, terminy spotkań i obowiązki grupy roboczej. Następnie można podjąć decyzje dotyczące sposobu operacjonalizacji podejścia interdyscyplinarnego na poziomie misji oraz procesów biznesowych i operacyjnych. Często przybiera to formę grup roboczych składających się z osób odpowiedzialnych za realizację misji oraz procesów biznesowych, które mogą spotykać się bardziej regularnie i zajmować się wyzwaniami związanymi z obszarem C-SCRM w zakresie operacji oraz taktyki.

W tabeli 2-1 przedstawiono zestawienie interesariuszy zajmujących się obszarem C-SCRM na każdym poziomie wraz z konkretnymi działaniami C-SCRM wykonywanymi w ramach stosownych poziomów. Działania te stanowią bezpośrednie działania w zakresie C-SCRM lub mają wpływ na ogół praktyk C-SCRM.

Tabela 2-1: Zarządzanie ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw – interesariusze[23]

Poziomy	Nazwa poziomu	Interesariusz	Działania
1	Podmiot	Zarząd podmiotu[24]: CEO, CIO, COO, CFO, CISO, Chief Technology Officer (CTO), Chief Acquisition Officer (CAO), Chief Privacy Officer (CPO), CRO i inni.	• Określenie strategii podmiotu w zakresie C-SCRM. • Opracowanie struktur zarządzania i modelu operacyjnego. • Określenie ram ryzyka dla podmiotu i nadanie kierunku sposobowi zarządzania ryzykiem (np. ustalenie apetytu na ryzyko). • Określenie wysokopoziomowego planu wdrożenia, polityki, celów i zadań. • Podejmowanie decyzji dotyczących obszaru C-SCRM na poziomie podmiotu. • Stworzenie PMO dotyczącego działań w zakresie C-SCRM.

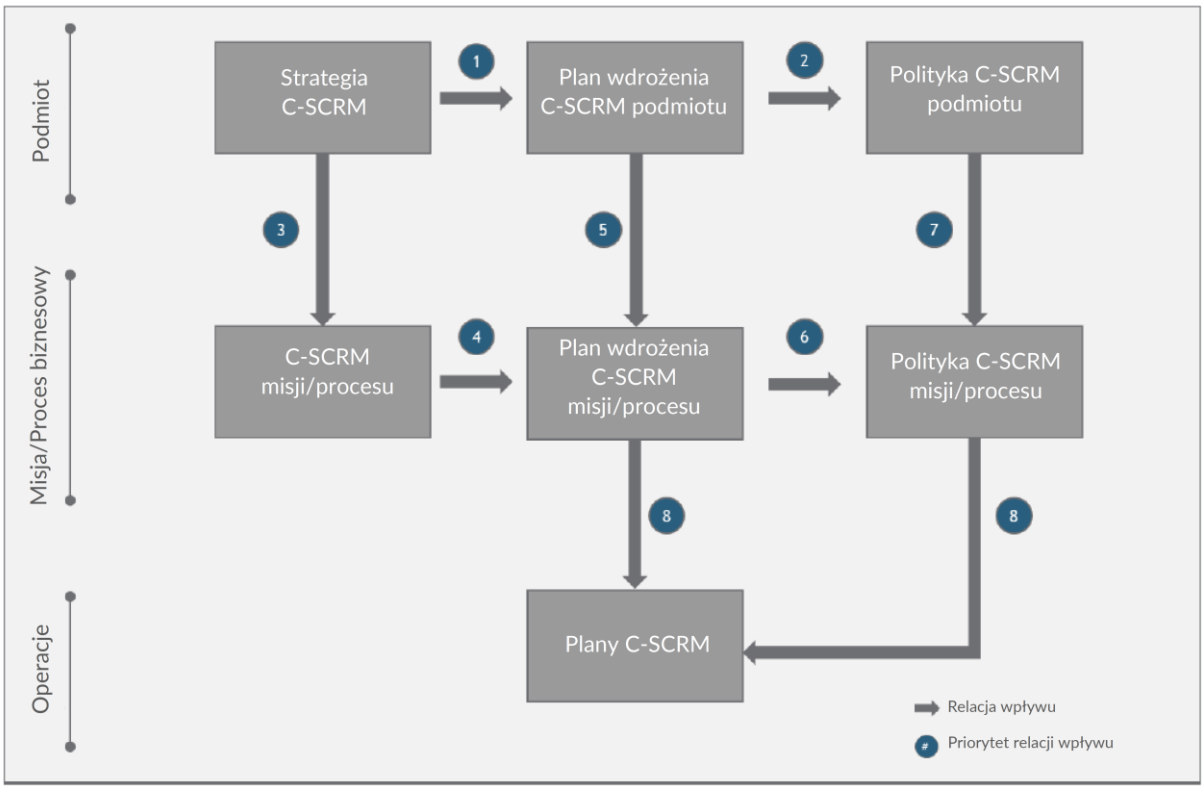
[23] W przypadku małych i średnich organizacji może nie występować tak znaczące zróżnicowanie wśród interesariuszy C-SCRM.

[24] Rozwinięcie skrótów – patrz NSC 7298.

Poziomy	Nazwa poziomu	Interesariusz	Działania
2	Misja i proces biznesowy	Kierownicy podmiotu: Kierownicy programów, kierownicy projektów, członkowie zintegrowanych zespołów projektowych, działy badawczo-rozwojowe, działy inżynieryjne (nadzór nad cyklem życia systemu), zarządzanie zaopatrzeniem oraz relacjami z dostawcami, rozliczanie kosztów, zarządzanie związane z niezawodnością, bezpieczeństwem, ochroną, jakością, PMO dotyczące działań w zakresie C-SCRM, itd.	• Opracowanie strategii związanej z misją i procesami biznesowymi. • Opracowanie polityki i procedur, wytycznych i ograniczeń. • Zmniejszanie podatności na zagrożenia na etapie rozpoczęcia nowych projektów informatycznych i/lub związanych z nimi procesów zaopatrzenia i zakupów. • Przegląd i ocena problemów systemowych, ludzkich lub organizacyjnych, które narażają środowiska biznesowe, techniczne i zaopatrzenia na zagrożenia i cyberataki. • Opracowanie planu (planów) wdrożenia działań w zakresie C SCRM. • Dostosowanie ram ryzyka podmiotu do misji i procesu biznesowego (np. ustalenie poziomu tolerowanego ryzyka). • Zarządzanie ryzykiem w ramach misji i procesów biznesowych.

Poziomy	Nazwa poziomu	Interesariusz	Działania
			• Utworzenie PMO dotyczącego działań w zakresie C-SCRM lub udział w jego pracach. • Składanie sprawozdań dotyczących działań w zakresie C-SCRM do przedstawicieli pierwszego poziomu oraz wdrażanie wniosków ze sprawozdań przesyłanych przez przedstawicieli trzeciego poziomu.
3	Operacje	Zarządzanie systemami: Architekci, deweloperzy, osoby odpowiedzialne za systemy, zespoły zapewnienia i kontroli jakości, testerzy, osoby odpowiedzialne za kontraktowanie, pracownicy PMO dotyczącego działań w zakresie C-SCRM, inżynier zabezpieczeń lub operator systemów zabezpieczeń, itd.	• Opracowanie planów w zakresie C-SCRM. • Wdrożenie polityki i wymagań w zakresie C-SCRM. • Przestrzeganie ograniczeń ustalonych na poziomach pierwszym i drugim. • Dostosowanie działań w zakresie C-SCRM do kontekstu danego systemu i wdrażanie ich w całym cyklu życia systemu. • Składanie sprawozdań dotyczących działań w zakresie C-SCRM przedstawicielom poziomu drugiego.

Proces C-SCRM powinien być realizowany na trzech poziomach zarządzania ryzykiem, a jego ogólnym celem jest ciągłe doskonalenie działań podmiotu związanych z ryzykiem oraz skuteczna komunikacja między poziomami oraz wewnątrzpoziomowa, a tym samym integracja działań zarówno strategicznych, jak i taktycznych wśród wszystkich interesariuszy, których celem jest realizacja misji oraz odniesienie sukcesu przez podmiot. Niezależnie od tego, czy chodzi o komponent, system, proces, dotyczący misji, czy politykę, kluczowe jest zaangażowanie odpowiednich interesariuszy C-SCRM na każdym poziomie, aby zapewnić, że działania w zakresie zarządzania ryzykiem są jak najbardziej świadome. Rysunek 2-5 ilustruje relacje pomiędzy kluczowymi dokumentami dotyczącymi działań w zakresie C SCRM na trzech poziomach.



Rysunek 2-5: Relacje między dokumentami dotyczącymi działań w zakresie C-SCRM

W kolejnych podrozdziałach przedstawiono przykładowe role i działania na każdym poziomie. Ze względu na to, że każdy podmiot jest inny, poszczególne działania mogą być realizowane na poziomach innych niż wymienione oraz zgodnie z wymogami indywidualnego kontekstu danego podmiotu.

Tłumaczenie

Załącznik A zawiera szereg zabezpieczeń związanych z obszarem C-SCRM dotyczących misji i działań biznesowych, które organizacje mogą wykorzystać w sposób dostosowany do swoich potrzeb, aby wspierać realizację działań C-SCRM na każdym z trzech poziomów. Należy pamiętać, że proces ich dostosowywania powinien uwzględniać potrzeby organizacji w zakresie zarządzania ryzykiem. Co więcej, organizacje powinny przeanalizować koszty niewdrożenia polityk, działań oraz zabezpieczeń związanych z C-SCRM podczas oceny alternatywnych sposobów reagowania na ryzyko. Koszty te mogą obejmować niską jakość lub pojawienie się na rynku podrobionych produktów, naruszenie zasad ochrony własności intelektualnej przez dostawców, manipulowanie przez dostawców kluczowymi informacjami lub ich kompromitacja, a także narażenie na cyberataki za pośrednictwem narażonych systemów informacyjnych dostawców.

2.3.2. Poziom 1 – Podmiot

Efektywne działania w zakresie C-SCRM wymagają zaangażowania, bezpośredniego udziału i stałego wsparcia ze strony liderów wyższego szczebla i zarządu. Podmioty powinny powierzyć odpowiedzialność za kierowanie działaniami w zakresie zarządzania ryzykiem w łańcuchu dostaw w skali całej organizacji osobie na stanowisku dyrektora, wybranemu biuru (wspieranemu przez zespół specjalistów) lub grupie (na przykład radzie ds. ryzyka, wykonawczemu komitetowi sterującemu lub radzie wykonawczej) niezależnie od struktury organizacyjnej agencji. Ponieważ zagrożenia dla cyberbezpieczeństwa w całym łańcuchu dostaw mogą występować w każdej głównej linii biznesowej, podmioty powinny zapewnić, że role i obowiązki C SCRM są zdefiniowane dla liderów wyższego szczebla, którzy uczestniczą w działaniach związanych z łańcuchem dostaw (np. pozyskiwanie i zaopatrzenie, bezpieczeństwo informacji, technologia informacyjna, prawo, zarządzanie programami oraz łańcuch dostaw i logistyka). Bez ustanowienia nadzoru wykonawczego nad działaniami C-SCRM, podmioty mają ograniczoną zdolność do podejmowania decyzji dotyczących ryzyka w całej organizacji w zakresie skutecznego zabezpieczania swoich produktów i usług.

Poziom 1 – poziom podmiotu – nadaje ton i kierunek działaniom C-SCRM w całym podmiocie poprzez opracowanie nadrzędnej strategii działań w zakresie C-SCRM, polityki C-SCRM oraz wysokopoziomowego planu wdrożenia, który kształtuje sposób

wdrażania działań w zakresie C-SCRM w całym podmiocie. W ramach poziomu 1 tworzone są struktury zarządzania, które umożliwiają dyrektorom i kierownictwu wyższego szczebla współpracę w zakresie C-SCRM z pionem zajmującym się zarządzaniem ryzykiem, podejmowanie decyzji dotyczących działań w zakresie C-SCRM, delegowanie decyzji do przedstawicieli poziomów 2 i 3 oraz ustalanie priorytetów w zakresie alokacji zasobów w całym podmiocie na potrzeby C SCRM. Działania na poziomie 1 pomagają zapewnić, że strategie łagodzenia skutków w ramach działań związanych z C-SCRM są zgodne ze strategicznymi celami i zadaniami podmiotu. Działania na poziomie 1 skutkują opracowaniem strategii C SCRM, polityki oraz planu wdrożeniowego wysokiego szczebla, które kształtują i ograniczają sposób realizacji działań związanych z C-SCRM na poziomach 2 i 3.

Odpowiedzialność za ryzyko związane z cyberbezpieczeństwem w łańcuchu dostaw spoczywa ostatecznie na kierowniku jednostki organizacyjnej.

- Decydenci czerpią wiedzę z profilu ryzyka organizacji, apetytu na ryzyko oraz poziomu tolerowania ryzyka. Procesy powinny uwzględniać informację na temat sposobu oraz czasu eskalacji decyzji dotyczących ryzyka.
- Odpowiedzialność za nie powinna być przekazana osobom autoryzującym w podmiocie w oparciu o ich władzę wykonawczą nad misją organizacji, operacjami biznesowymi lub systemami informacyjnymi.
- Osoby autoryzujące mogą delegować obowiązki do wybranych pracowników odpowiedzialnych za codzienne zarządzanie ryzykiem.

Efektywne działania w zakresie C-SCRM wymagają odpowiedzialności, zaangażowania, nadzoru, bezpośredniego udziału i stałego wsparcia ze strony liderów wyższego szczebla i zarządu. Podmioty powinny zapewnić, że role i obowiązki dotyczące C-SCRM są określone dla kierowników wyższego szczebla, którzy uczestniczą w działaniach związanych z łańcuchem dostaw (np. zakupy i zaopatrzenie, bezpieczeństwo informacji, technologia informacyjna, kwestie prawne, zarządzanie programem czy obsługa łańcucha dostaw i logistyka). Na poziomie 1 zarząd jest zazwyczaj odpowiedzialny za ocenę i ograniczanie wszystkich ryzyk podmiotu. Osiąga się to zazwyczaj dzięki

powołaniu rady ds. zarządzania ryzykiem w podmiocie. Efektywne działania w zakresie C-SCRM pozwalają na spojrzenie na to zagadnienie z perspektywy liderów skupionych w radzie ds. zarządzania ryzykiem, takich jak CEO, CRO, CIO, CLO, CISO oraz CAO – członkowie rady przekazują porady CIO i CISO zarządowi.

CIO bądź CISO mogą stworzyć organ zajmujący się zagadnieniami związanymi z C-SCRM, aby przeprowadzić dogłębne analizy w celu wsparcia działań rady ds. zarządzania ryzykiem w podmiocie. Rada ds. C-SCRM stanowi forum do ustalania priorytetów i zarządzania ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw dla podmiotu. Rada ds. C-SCRM lub inny organ zajmujący się zagadnieniami związanymi z C-SCRM jest odpowiedzialny za rozwój stosownej strategii dla całego podmiotu. Strategia działań w zakresie C-SCRM wyraźnie określa założenia podmiotu, ograniczenia, tolerancję ryzyka oraz priorytety i wybory ustalone przez radę ds. zarządzania ryzykiem w podmiocie. Działania w zakresie C-SCRM są związane z ogólnym zarządzaniem ryzykiem podmiotu – zapewnia się to przez udział CIO bądź CISO w radzie ds. zarządzania ryzykiem przy zarządzie.

Liderzy ci są również odpowiedzialni za opracowanie i rozpowszechnianie kompleksowego zestawu polityk, które obejmują misję podmiotu i procesy biznesowe, a także kierowanie procesem ustanawiania oraz dojrzewania działań w zakresie C-SCRM oraz wdrażaniem spójnego zestawu działań. Zadaniem liderów powinno być ustanowienie grupy roboczej do spraw C-SCRM lub inny dedykowany pion związany z C-SCRM, który będzie odpowiadał za realizację działań C-SCRM i służył jako punkt odniesienia dla realizacji skoordynowanych usług oraz wytycznych dla podmiotu w tym obszarze. Liderzy powinni również jasno określić kluczowe role na poziomie misji i procesu biznesowego – osoby odpowiedzialne za uszczegółowienie planów działania i realizację działań C-SCRM. Podmioty powinny wziąć pod uwagę, że bez ustanowienia nadzoru wykonawczego nad działaniami C-SCRM, podmioty mają ograniczoną zdolność do podejmowania decyzji dotyczących ryzyka w całej organizacji w zakresie skutecznego zabezpieczenia swoich produktów i usług.

Struktury zarządzania działaniami w zakresie C-SCRM i model operacyjny dyktują uprawnienia, odpowiedzialność i możliwość podejmowania decyzji dotyczących tego

obszaru oraz określają *sposób* realizacji procesów C-SCRM w podmiocie. Najlepszy model zarządzania i działania C-SCRM to takie, które spełniają wymagania biznesowe i funkcjonalne podmiotu. Na przykład, podmiot zmagający się ze ścisłymi ograniczeniami budżetowymi lub wysokimi wymaganiami w zakresie C-SCRM może rozważyć modele zarządzania i operacyjne, które centralizują władzę decyzyjną i opierają się na grupach roboczych do spraw C-SCRM w celu konsolidacji odpowiedzialności za zadania wymagające dużych zasobów, takie jak ocena ryzyka dostawcy. Z kolei podmioty, których misję i procesy biznesowe charakteryzuje duży stopień autonomii lub wysoce zróżnicowane wymagania w zakresie C-SCRM, mogą zdecydować się na zdecentralizowaną władzę, odpowiedzialność i podejmowanie decyzji.

Oprócz zdefiniowania struktur zarządzania C-SCRM i modeli operacyjnych, przedstawiciele poziomu 1 realizują działania niezbędne do stworzenia ram C-SCRM dla podmiotu. Opracowanie ram C-SCRM jest procesem, w którym podmiot ujawnia założenia dotyczące zagrożeń związanych z cyberbezpieczeństwem w całym łańcuchu dostaw (np. zagrożenia, podatności, wpływ ryzyka[25], prawdopodobieństwo wystąpienia ryzyka), a także apetytu oraz tolerowania ryzyka, priorytetów i kompromisów, na których opierają się decyzje dotyczące C-SCRM w całym podmiocie. Proces ujęcia ryzyka zapewnia dane wejściowe niezbędne do ustanowienia strategii C-SCRM, która dyktuje sposób, w jaki podmiot planuje oceniać i monitorować ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw, a także reagować na jego wystąpienie. Należy również opracować wysokopoziomowy plan wdrożenia, na którym oprze się realizacja strategii C-SCRM podmiotu. Proces ujmowania ryzyka został szczegółowo omówiony w Załączniku C.

Poziom 1, czerpiąc wnioski z procesu ujęcia ryzyka oraz strategii C-SCRM, opracowuje politykę podmiotu w zakresie C-SCRM. Polityka C-SCRM ustanawia cel programu działań związanych z C-SCRM, nakreśla obowiązki podmiotu w zakresie C-SCRM, definiuje i nadaje uprawnienia pracownikom odpowiedzialnym za C-SCRM w całym podmiocie

[25] Pojęcie wpływu ryzyka odnosi się do wpływu utraty poufności, integralności lub dostępności informacji lub systemu na działania organizacyjne, aktywa organizacyjne, osoby fizyczne, inne organizacje lub państwo – w tym interesy bezpieczeństwa narodowego. [NSC 800-53].

oraz nakreśla obowiązujące oczekiwania i procesy w zakresie zgodności i egzekwowania C-SCRM. Załącznik C zawiera przykładowe wzory strategii i polityki C-SCRM.

Działania w zakresie oceny ryzyka prowadzone na poziomie 1 koncentrują się na ocenie i monitorowaniu ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw, a także reagowaniu na ryzyko. Ocena ryzyka na poziomie 1 może opierać się na etapie ujęcia ryzyka zrealizowanym przez podmiot na poziomie 1 – na założeniach, ograniczeniach, podatności na ryzyko, tolerancji ryzyka, priorytetach i kompromisach, mogą być także zebranymi założeniami na poziomie podmiotu opartymi na ocenach ryzyka, które są przeprowadzane w odniesieniu do poszczególnych misji i procesów biznesowych. Na przykład ocena ryzyka na poziomie 1 może oceniać narażenie na zagrożenia dla celów podmiotu, które wynikają z produktów lub usług łańcucha dostaw. Celem oceny ryzyka na poziomie 1 może być również zebranie oraz ujęcie w nowym kontekście ocen ryzyka przeprowadzonych na poziomie 2 w celu opisania scenariuszy ryzyka w odniesieniu do głównych celów podmiotu.

Sprawozdawczość odgrywa ważną rolę w wyposażeniu decydentów poziomu 1 w kontekst niezbędny do podejmowania świadomych decyzji dotyczących zarządzania ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw. Sprawozdania powinny skupiać się na trendach dotyczących całego podmiotu i obejmować zakres, w jakim C-SCRM został wdrożony w całym podmiocie, skuteczność C-SCRM oraz warunki dotyczące ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw. Sprawozdania dotyczące C-SCRM powinny podkreślać wszelkie warunki, które wymagają pilnej uwagi lub działania ze strony kierownictwa, a także mogą opierać się na trendach ryzyka oraz wyników działań dotyczących działań w zakresie C-SCRM w danym okresie. Osoby odpowiedzialne za działania związane z C-SCRM w podmiocie powinny współpracować z liderami w celu określenia wymagań dotyczących sprawozdawczości, takich jak częstotliwość, zakres i format. Sprawozdawczość powinna obejmować mierniki omówione szerzej w podrozdziale 3.5.1.

Działania na poziomie 1 zapewniają nadrzędny kontekst i granice, w ramach których misja podmiotu i procesy biznesowe obejmują zagadnienia związane z zarządzaniem

ryzykiem dotyczącym cyberbezpieczeństwa w całym łańcuchu dostaw. Dane wyjściowe z poziomu 1, takie jak strategia C-SCRM, polityka C-SCRM, inne elementy zarządzania oraz modele operacyjne są dopracowywane i doskonalone w ramach poziomu 2, aby dopasować je do kontekstu każdej misji i każdego procesu biznesowego. Dane wyjściowe z poziomu 1 powinny być również aktualizowane na podstawie rezultatów prac w zakresie C-SCRM na niższych poziomach.

Należy zwrócić uwagę, że w złożonych podmiotach działania poziomu 1 mogą być realizowane na poziomie podmiotu oraz na poziomie poszczególnych organizacji. Działania na poziomie 1 podmiotu powinny kształtować działania na poziomie 1 organizacji.

Dodatkowe informacje można znaleźć w Załączniku A do niniejszego dokumentu oraz zabezpieczeniach SR-1, SR-3, PM-2, PM-6, PM-7, PM-9, PM-28, PM-29, PM-30 i PM-31 dokumentu /NSC 800-53.

2.3.3. Poziom 2 – Poziom misji i procesów biznesowych

Poziom 2 dotyczy sposobu, w jaki obszary odpowiedzialne za misję podmiotu oraz jego procesy biznesowe oceniają i monitorują ryzyko, a także reagują na ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw. Działania poziomu 2 są realizowane zgodnie ze strategią i polityką C-SCRM opracowaną na poziomie 1[26]. Na tym poziomie, strategie, polityki i plany wdrożeniowe działań związanych z C-SCRM dotyczące poszczególnych procesów wyznaczają sposób, w jaki cele i wymagania podmiotu w zakresie C-SCRM są realizowane w ramach każdej misji i każdego procesu biznesowego. Na tym poziomie określa się specyficzne wymagania działań w zakresie C-SCRM, które obejmują koszty, harmonogram, wydajność, bezpieczeństwo oraz szereg kluczowych wymagań niefunkcjonalnych. Wymagania niefunkcjonalne obejmują pojęcia takie jak niezawodność, bezpieczeństwo czy jakość.

Zespół poziomu 2 obejmuje przedstawicieli każdej misji i procesu biznesowego, takich jak kierownicy programów, badań i rozwoju oraz zaopatrzenia/zamówień. Działania dotyczące obszaru C-SCRM na poziomie 2 dotyczą C-SCRM w kontekście misji podmiotu i procesów biznesowych. Należy opracować konkretne strategie, polityki

[26] Więcej informacji można znaleźć w dokumencie [NIST SP 800-39, sekcja 2.2].

i procedury, aby dostosować wdrożenie C-SCRM do specyficznych wymagań każdej misji i poszczególnych procesów biznesowych. W celu dalszego rozwoju wysokopoziomowej Strategii Podmiotu i Planu Wdrożenia, różne obszary misji lub linie biznesowe podmiotu mogą wymagać opracowania własnych dostosowanych do misji oraz działalności strategii oraz planów wdrożenia. Muszą także zadbać o to, by realizacja działań w zakresie C-SCRM odbyła się w ramach ograniczeń określonych przez strategie C-SCRM wyższego poziomu oraz zgodnie z polityką C-SCRM. Aby ułatwić opracowanie i realizację planów strategicznych i wdrożeniowych na poziomie 2, podmioty mogą utworzyć komitet obejmujący przedstawicieli każdej misji i każdego procesu biznesowego. Koordynacja i współpraca między osobami odpowiedzialnymi za misję oraz procesy biznesowe może pomóc zwiększyć świadomość ryzyka, określić zagrożenia związane z cyberbezpieczeństwem w całym łańcuchu dostaw oraz wspierać rozwój architektury podmiotu oraz działań w zakresie C-SCRM. Biuro zarządzania projektami ds. C-SCRM może również pomagać we wdrażaniu działań związanych z C-SCRM na poziomie 2 poprzez świadczenie wsparcia – na przykład oferując szablony polityk, a także wsparcie ekspertów w zakresie C-SCRM.

Wiele zagrożeń *dotyczących* łańcucha dostaw i *występujących dzięki* łańcuchowi dostaw omawia się na poziomie 2 w zakresie zarządzania relacjami z dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych i innymi dostawcami usług związanych z ICT/OT. Ze względu na to, że działania związane z C-SCRM mogą zarówno bezpośrednio jak i pośrednio wpływać na procesy dotyczące realizacji misji, zrozumienie, integracja i koordynacja tych działań na tym poziomie nabierają kluczowego znaczenia. Działania na poziomie 2 skupiają się na dostosowaniu i zastosowaniu ram C-SCRM podmiotu w celu dopasowania ich do zagrożeń, podatności, skutków i prawdopodobieństwa ich wystąpienia w kontekście konkretnych misji oraz procesów biznesowych[27]. Na podstawie danych wyjściowych z poziomu 1 (np. strategii C-SCRM), osoby

[27] Pojęcie wpływu ryzyka odnosi się do wpływu utraty poufności, integralności lub dostępności informacji lub systemu na działania organizacyjne, aktywa organizacyjne, osoby fizyczne, inne organizacje lub państwo – w tym interesy bezpieczeństwa narodowego [NSC 800-53].

odpowiedzialne za misję oraz procesy biznesowe przyjmą strategię C-SCRM, która dostosowuje ogólną strategię podmiotu do konkretnej misji i konkretnego procesu biznesowego. Na poziomie 2 podmiot może również wydać polityki dotyczące misji i procesów biznesowych, które umieszczają politykę podmiotu w odpowiednim kontekście w odniesieniu do procesu.

Zgodnie ze strategią C-SCRM, liderzy odpowiedzialni za poszczególne misje oraz procesy biznesowe powinni opracować i zrealizować plan wdrożenia C-SCRM. Plan wdrożenia C-SCRM stanowi bardziej szczegółowy plan operacjonalizacji strategii C-SCRM w ramach misji i procesu biznesowego. W ramach planów wdrożenia C-SCRM, osoby odpowiedzialne za misje i procesy biznesowe określają role, obowiązki, kamienie milowe wdrożenia, daty oraz procesy monitorowania i sprawozdawczości dotyczące C-SCRM. Załącznik D do niniejszego dokumentu zawiera przykładowe wzory strategii C-SCRM, planu wdrożenia oraz polityki C-SCRM.

Działania związane z C-SCRM realizowane na poziomie 2 koncentrują się na ocenie ryzyka, reagowaniu i monitorowaniu ekspozycji na ryzyko wynikające z zależności misji i procesów biznesowych od dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT. Narażenie na ryzyko związane z łańcuchem dostaw może wystąpić w wyniku pierwotnych zależności od łańcucha dostaw lub wtórnych zależności od poszczególnych systemów informacyjnych lub innych misji i procesów biznesowych. Na przykład narażenie na ryzyko może wynikać z tego, że dostawca dostarcza kluczowe komponenty systemu lub usługi związane z wieloma systemami informacyjnymi, od których zależą krytyczne procesy. Ryzyko może również wynikać z produktów i usług pochodzących od dostawców niezwiązanych z systemami informacyjnymi, a także z roli, jaką te produkty i usługi odgrywają w realizacji ogólnej misji podmiotu i celów procesów biznesowych. Podmioty powinny wziąć pod uwagę nietypowe źródła zagrożeń cyberbezpieczeństwa w całym łańcuchu dostaw. Ryzyka te mogą wymykać się ramom procesów związanych z obszarem C-SCRM, na przykład w przypadku wykorzystania oprogramowania otwartoźródłowego (*ang. open source software*). Podmioty powinny ustanowić polityki i środki bezpieczeństwa w celu

zarządzania nietypowymi zagrożeniami związanymi z cyberbezpieczeństwem w całym łańcuchu dostaw.

Sprawozdawczość na poziomie 2 odgrywa ważną rolę w wyposażeniu liderów misji i procesów biznesowych w kontekst niezbędny do zarządzania C-SCRM w zakresie poszczególnych misji i procesów biznesowych. Tematy poruszane na poziomie 2 będą odzwierciedlać te poruszane na poziomie 1, ale powinny być przeformułowane w taki sposób, aby skupiały się na konkretnej misji i konkretnych procesach biznesowych, którym odpowiadają. Sprawozdawczość na poziomie 2 powinna zawierać wskaźniki, które pokazują realizację misji i procesów biznesowych w zestawieniu z określonymi przez podmiot deklaracjami apetytu na ryzyko i tolerancji ryzyka, zdefiniowanymi na poziomach 1 i 2. Wymagania dotyczące sprawozdawczości powinny być zdefiniowane w taki sposób, aby odpowiadały potrzebom liderów w zakresie misji i procesów biznesowych oraz na poziomie 1.

Dane wyjściowe z poziomu 2 będą miały znaczący wpływ na sposób prowadzenia działań dotyczących działań w zakresie C-SCRM na poziomie 3. Na przykład na poziomie 2 można określić tolerancję ryzyka oraz wspólne decyzje dotyczące podstawowych standardów zabezpieczeń, a następnie dostosować je i zastosować w kontekście poszczególnych systemów informacyjnych na poziomie 3. Dane wyjściowe poziomu 2 powinny być również wykorzystywane do iteracyjnego wpływania na dane wyjściowe poziomu 1 i dalszego ich udoskonalania.

Dodatkowe informacje można znaleźć w Załączniku A do niniejszego dokumentu oraz zabezpieczeniach SR-1, SR-3, SR-6, PM- 2, PM-6, PM-7, PM-30, PM-31 i PM-32 dokumentu NSC 800-53.

2.3.4. Poziom 3 – Poziom operacji

W skład zespołu poziomu 3 wchodzi personel odpowiedzialny za działania operacyjne, w tym przeprowadzanie zamówień i wykonywanie działań C-SCRM związanych z systemem w ramach cyklu życia systemu, który obejmuje badania i rozwój, projektowanie, produkcję, dostarczanie, integrację, eksploatację i utrzymanie oraz utylizację systemów. Do personelu tego należą osoby odpowiedzialne za systemy,

osoby odpowiedzialne za zamówienia i umowy, przedstawiciele tych osób, architekci, inżynierowie systemów, specjaliści ds. bezpieczeństwa informacji, integratorzy systemów oraz deweloperzy. Personel ten jest odpowiedzialny za opracowanie planów C-SCRM, które dotyczą zarządzania, zapewnienia wdrożenia i monitorowania zabezpieczeń C-SCRM (w tym tych mających zastosowanie do podmiotów zewnętrznych, takich jak wykonawcy) oraz nabywania, rozwijania i utrzymywania systemów i komponentów w całym cyklu życia systemu w celu wspierania misji i procesów biznesowych. W podmiotach, w których utworzono grupę roboczą ds. C-SCRM, działania takie jak ocena ryzyka związanego z produktem, mogą być świadczone jako scentralizowana, wspólna usługa.

W ramach działań na poziomie 3, rezultaty prac przeprowadzonych na poziomach 1 oraz 2 przygotowują podmiot do realizacji działań związanych z C-SCRM na poziomie operacyjnym zgodnie z ramami zarządzania ryzykiem [NSC 800-37]. Działania w zakresie C-SCRM stosuje się do systemów informacyjnych poprzez opracowanie i wdrożenie planów C-SCRM. Na plany te duży wpływ mają założenia, ograniczenia, apetyt na ryzyko i tolerowanie ryzyka, a także priorytety i kompromisy określone na poziomach 1 i 2. Plany C-SCRM dyktują, w jaki sposób działania C-SCRM są włączane w cały cykl życia systemu – od nabycia, zarówno rozwiązań na zamówienie, jak i rozwiązań komercyjnych, wymagania, projekt architektury, rozwój, dostarczanie, instalację, integrację, utrzymanie i utylizację lub wycofanie. Plany C-SCRM dotyczą konkretnych wdrożeń i zapewniają realizację polityki, określają także wymagania, ograniczenia i implikacje dla systemów, które wspierają realizację misji oraz procesów biznesowych.

Działania na poziomie 3 koncentrują się na zarządzaniu ryzykiem na poziomie operacyjnym wynikającym z wszelkich produktów i usług związanych z ICT/OT dostarczanych poprzez łańcuch dostaw, które są wykorzystywane przez podmiot lub wchodzą w zakres granicy autoryzacji systemów. Działania C-SCRM na poziomie 3 rozpoczynają się od analizy prawdopodobieństwa i wpływu potencjalnych zagrożeń związanych z cyberbezpieczeństwem w łańcuchu dostaw wykorzystujących podatność na poziomie operacyjnym (np. w systemie lub komponencie systemu). W stosownych przypadkach te oceny ryzyka powinny być oparte na ocenach ryzyka przeprowadzonych

na poziomie 1 i 2. W odpowiedzi na określenie ryzyka, podmioty powinny ocenić alternatywne sposoby działania w celu zmniejszenia narażenia na ryzyko, takie jak między innymi akceptację ryzyka, jego unikanie, złagodzenie, dystrybucję lub przeniesienie. Reakcja na ryzyko jest osiągana poprzez wybór, dostosowanie, wdrożenie i monitorowanie zabezpieczeń C-SCRM w całym cyklu życia systemu zgodnie z ramami zarządzania ryzykiem [NSC 800-37]. Wybrane środki bezpieczeństwa C-SCRM często składają się z kombinacji zabezpieczeń z poziomu 1 i poziomu 2 oraz zabezpieczeń specyficznych dla systemu informacyjnego na poziomie 3.

Sprawozdawczość na poziomie 3 powinna skupiać się na wdrożeniu C-SCRM, skuteczności, efektywności oraz ogólnym poziomie narażenia na ryzyko związane z cyberbezpieczeństwem w łańcuchu dostaw dla danego systemu. Sprawozdawczość na poziomie konkretnych systemów powinna zapewnić osobom odpowiedzialnym za systemy wgląd na poziomie taktycznym, który umożliwi im szybkie wprowadzanie zmian i reagowanie na warunki ryzyka. Sprawozdawczość na poziomie 3 powinna obejmować wskaźniki określające wyniki w odniesieniu do oświadczeń dotyczących gotowości podmiotu do podejmowania ryzyka oraz tolerancji ryzyka określonych na poziomach 1, 2 i 3.

Kluczowym działaniem poziomu 3 jest opracowanie planu C-SCRM. Wraz z mającymi zastosowanie informacjami o środkach bezpieczeństwa, plan C-SCRM zawiera informacje o systemie, jego kategoryzacji, statusie operacyjnym, powiązanych umowach, architekturze, kluczowych osobach, powiązanych prawach, regulacjach, politykach i planie awaryjnym. Jednym z kluczowych aspektów tego obszaru jest ciągłe przestrzeganie wytycznych, natomiast plan C-SCRM jest żywym dokumentem, który powinien być utrzymywany i używany jako punkt odniesienia do ciągłego monitorowania wdrożonych zabezpieczeń związanych z obszarem C-SCRM. Plany C-SCRM są dokumentami, które powinny być regularnie używane, w związku z czym powinny być okresowo przeglądane i odświeżane. Nie są to dokumenty opracowane w celu spełnienia wymogu zgodności. Podmioty powinny raczej być w stanie wykazać, jak stosowały i skutecznie stosują swoje plany w celu kształtowania, dopasowywania, informowania i podejmowania działań i decyzji w zakresie C-SCRM na wszystkich trzech poziomach.

Informacje zebrane w ramach działań C-SCRM poziomu 3 powinny wpływać na działania w zakresie C-SCRM realizowane na poziomach 1 oraz 2 w celu dalszego doskonalenia strategii i planów wdrażania C-SCRM.

Dodatkowe informacje można znaleźć w Załączniku A do niniejszego dokumentu oraz w zabezpieczeniach SR-1, SR-2, SR-6, PL-2, PM-31 i PM-32 dokumentu NSC 800-53.

2.3.5. Biuro zarządzania projektami ds. C-SCRM

Różnorodne modele operacyjne (np. scentralizowany, zdecentralizowany, hybrydowy) ułatwiają realizację działań w zakresie C-SCRM w całym podmiocie, a także misji oraz procesów biznesowych. Jeden z takich modeli zakłada koncentrację i przypisanie odpowiedzialności za określone działania C-SCRM scentralizowanej grupie roboczej ds. C-SCRM. W tym modelu biuro zarządzania projektami (*ang. Program Management Office – PMO*) ds. C-SCRM działa jako dostawca usług dla innych misji i procesów biznesowych. Osoby odpowiedzialne za misję oraz procesy biznesowe są następnie odpowiedzialne za wybór i żądanie usług od biura zarządzania projektami ds. C-SCRM w ramach swoich obowiązków związanych z realizacją celów i zadań C-SCRM. Istnieje wiele korzystnych usług, które może świadczyć biuro:

- usługi doradcze i wsparcie merytoryczne,
- kierowanie wewnętrznymi grupami roboczymi, radami lub innymi organami koordynującymi działania w zakresie C-SCRM,
- oferowanie narzędzi, pomocy, działań uświadamiających oraz szablonów szkoleń,
- dokonywanie ocen ryzyka dostawców i produktów,
- utrzymywanie kontaktów z zewnętrznymi interesariuszami,
- zarządzanie wymianą informacji (np. w obrębie departamentu/podmiotu oraz w kontaktach z FASC),
- zarządzanie rejestrem ryzyka związanego z C-SCRM,
- prowadzenie działań sekretariatu do spraw zarządzania C-SCRM w podmiocie,
- zarządzanie projektami i wynikami działań C-SCRM,
- omówienia, prezentacje i sprawozdania dotyczące C-SCRM.

Biuro zarządzania projektami ds. C-SCRM zazwyczaj składa się z ekspertów zajmujących się obszarem C-SCRM, którzy pomagają w realizacji strategii i wdrażaniu C-SCRM w całym podmiocie, a także w poszczególnych jednostkach zajmujących się realizacją misji i procesów biznesowych. Biuro zarządzania projektami ds. C-SCRM może obejmować lub podlegać wyznaczonemu dyrektorowi odpowiedzialnemu za nadzorowanie działań C-SCRM w całym podmiocie. Biuro zarządzania projektami ds. C-SCRM powinno obejmować dedykowanych pracowników lub wyznaczonych przedstawicieli odpowiedzialnych za działania dotyczące C-SCRM w ramach szeregu procesów realizowanych przez podmiot, w tym z obszarów takich jak bezpieczeństwo informacji, zaopatrzenie, zarządzanie ryzykiem, inżynieria, rozwój oprogramowania, IT, dział prawny oraz dział kadr. Bez względu na to, czy biuro zarządzania projektami ds. C-SCRM jest częścią poziomu 1 lub 2, kluczowe jest, aby biuro zarządzania projektami ds. C-SCRM obejmowało przedstawicieli wielu dyscyplin i obszarów.

Obowiązki biura zarządzania projektami ds. C-SCRM mogą obejmować świadczenie usług na rzecz liderów podmiotu, które pomagają nadać ogólny ton wdrażaniu praktyk dotyczących działań w zakresie C-SCRM w całym podmiocie. Biuro zarządzania projektami ds. C-SCRM może zapewnić wsparcie specjalistom i ekspertom w celu przeprowadzenia interesariuszy poziomu 1 przez proces określania ryzyka, który obejmuje ustalenie apetytu podmiotu na ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw oraz jego tolerancji. Osoby odpowiedzialne za zarządzanie ryzykiem mogą przekazać biuru odpowiedzialność za opracowanie strategii i polityki C-SCRM podmiotu. Biuro zarządzania projektami ds. C-SCRM może również koordynować wymianę informacji wewnętrznie lub z podmiotami zewnętrznymi. Wreszcie, biuro może przeprowadzać prezentacje dla zarządu dotyczące zagadnienia C-SCRM (np. dla pionu zajmującego się ryzykiem, rady nadzorczej), aby pomóc interesariuszom poziomu 1 w opracowaniu kompleksowego obrazu ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw.

Na poziomie 2 biuro zarządzania projektami ds. C-SCRM może opracować zestawy startowe C-SCRM, które zawierają strategię bazową oraz zestaw polityk, procedur i wytycznych, które mogą być dalej dostosowywane do konkretnych misji i procesów

biznesowych. Biuro może również zapewnić eksperckie wsparcie dla interesariuszy w ramach misji i procesów biznesowych, ponieważ tworzą oni strategie C-SCRM specyficzne dla danego procesu i opracowują plany wdrożenia C-SCRM. W ramach tej odpowiedzialności biuro zarządzania projektami ds. C-SCRM może doradzać lub rozwijać wspólne podstawy zabezpieczeń C-SCRM w ramach misji podmiotu i procesów biznesowych. Biuro zarządzania projektami ds. C-SCRM może również przeprowadzać oceny ryzyka związanego z obszarem C-SCRM skoncentrowane na dostawcach, deweloperach, integratorach systemów, dostawcach zewnętrznych usług systemowych oraz innych dostawcach usług związanych z ICT/OT, zarówno produktów i usług związanych z technologią, jak i niezwiązanych z technologią.

Odpowiedzialność biura zarządzania projektami ds. C-SCRM na poziomie 1 i 2 ostatecznie wpływa na działania C-SCRM na poziomie 3. Biuro zarządzania projektami ds. C-SCRM może doradzać zespołom w całym cyklu życia systemów w zakresie wyboru, dopasowania i monitorowania zabezpieczeń C-SCRM. Co więcej, biuro zarządzania projektami ds. C-SCRM może być odpowiedzialne za działania, które skutkują opracowaniem rezultatów dotyczących działań w zakresie C-SCRM na wszystkich poziomach zarządzania ryzykiem. Centralizacja usług C-SCRM daje podmiotom możliwość wykorzystania specjalistycznych umiejętności w ramach skonsolidowanego zespołu, który oferuje wysokiej jakości usługi C-SCRM dla całego podmiotu. Poprzez centralizację usług oceny ryzyka podmioty mogą osiągnąć poziom standaryzacji, który w innym przypadku – np. w modelu zdecentralizowanym – nie byłby możliwy do osiągnięcia. Podmioty mogą również uzyskać oszczędności w przypadku, gdy zasoby biura zarządzania projektami będą skupione na działaniach w zakresie C-SCRM w przeciwieństwie do modeli zdecentralizowanych, w których pracownicy mogą pełnić wiele ról oprócz obowiązków związanych z C-SCRM.

Model oparty na biurze zarządzania projektami ds. C-SCRM będzie zazwyczaj wybierany przez większe, bardziej złożone podmioty, które wymagają standaryzacji praktyk C-SCRM w ramach zróżnicowanego zestawu misji i procesów biznesowych. Podmioty powinny wybrać model operacyjny C-SCRM, który będzie odpowiedni w odniesieniu do ich dostępnych zasobów i kontekstu.

Najważniejsze wnioski[28]

Uzasadnienie biznesowe dotyczące praktyk C-SCRM. Działania w zakresie C-SCRM zapewniają podmiotom szereg korzyści, takich jak zrozumienie krytycznych systemów, zmniejszenie prawdopodobieństwa kompromitacji w łańcuchu dostaw, efektywność operacyjną, ograniczenie problemów z jakością i bezpieczeństwem produktów oraz większą niezawodność i pewność dostarczanych usług.

Ryzyko związane z cyberbezpieczeństwem w łańcuchach dostaw. Potencjalne szkody lub kompromitacja wynikające z relacji z dostawcami, ich łańcuchami dostaw oraz dostarczanymi przez nich produktami lub usługami materializują się, gdy zagrożenie ze strony człowieka lub innych podmiotów skutecznie wykorzystuje podatność związaną z systemem, produktem, usługą lub ekosystemem łańcucha dostaw.

Wielopoziomowe, multidyscyplinarne podejście do C-SCRM. Jak wynika z opisu w dokumencie [NSC 800-39], wielopoziomowe zarządzanie ryzykiem obejmuje celową realizację oraz ciągłe doskonalenie działań w zakresie zarządzania ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw na poziomach podmiotu (np. CEO, COO), misji i procesu biznesowego (np. kierownicy biznesowi, dział badań i rozwoju) oraz operacyjnym (np. zarządzanie systemami). Każdy poziom obejmuje interesariuszy zajmujących się wieloma dziedzinami, takimi jak m.in. bezpieczeństwo informacji, zaopatrzenie, zarządzanie ryzykiem w podmiocie, inżynieria, rozwój oprogramowania, IT, kwestie prawne, czy kwestie kadrowe, którzy wspólnie realizują i stale doskonalą działania w zakresie C-SCRM

Biuro zarządzania projektami ds. C-SCRM. Specjalne biuro, określane mianem biura zarządzania projektami ds. C-SCRM, może wspierać działania podmiotu w zakresie C-SCRM poprzez dostarczanie produktów (np. szablonów polityk) i usług (np. oceny ryzyka dostawców) pozostałym jednostkom działającym w ramach podmiotu. Biuro zarządzania projektami ds. C-SCRM może zapewnić wsparcie na wszystkich trzech poziomach i działać się na poziomie 1 lub 2, w zależności od podmiotu.

[28] Najważniejsze wnioski opisują kluczowe informacje zawarte w tekście rozdziału. Definicje znajdują się w glosariuszu, który stanowi Załącznik H do niniejszego dokumentu.

C-SCRM jest procesem dotyczącym całego cyklu życia. Działania C-SCRM powinny być zintegrowane i realizowane w ramach odpowiednich procesów dotyczących cyklu życia realizowanych przez podmiot, takich jak na przykład cykl życia systemu. Na przykład w przypadku systemów ryzyko dotyczące cyberbezpieczeństwa związane z łańcuchem dostaw może się urzeczywistnić i urzeczywistnia się na etapie eksploatacji i konserwacji. Organizacje powinny zapewnić wprowadzenie odpowiednich działań w zakresie C-SCRM w celu ciągłej oceny i monitorowania ryzyka dotyczącego cyberbezpieczeństwa w łańcuchu dostaw, a także reagowania na to ryzyko.

3. KLUCZOWE CZYNNIKI SUKCESU

Aby skutecznie przeciwdziałać zmieniającym się zagrożeniom cyberbezpieczeństwa w całym łańcuchu dostaw, podmioty muszą realizować wiele wewnętrznych procesów i działań, komunikować się i współpracować na różnych poziomach oraz w różnych obszarach, a także dołożyć wszelkich starań, by zagwarantować, że wszyscy interesariusze rozumieją swoją rolę w zarządzaniu zagrożeniami dotyczącymi cyberbezpieczeństwa w całym łańcuchu dostaw. Podmioty potrzebują strategii komunikowania się, określania najlepszych sposobów wdrażania i monitorowania skuteczności zabezpieczeń i praktyk w zakresie cyberbezpieczeństwa w łańcuchach dostaw. Oprócz wewnętrznego rozpowszechniania zabezpieczeń dotyczących zarządzania ryzykiem dotyczącego cyberbezpieczeństwa w łańcuchu dostaw, podmioty powinny angażować się w wymianę spostrzeżeń dotyczących działań w zakresie C-SCRM. Te spostrzeżenia pomogą podmiotom w ciągłej ocenie swoich postępów w tym zakresie oraz w określeniu obszarów do poprawy oraz kroków prowadzących do zwiększenia dojrzałości realizowanych programów działań w zakresie C-SCRM. W tym rozdziale omówiono procesy i działania podmiotu niezbędne do skutecznego wdrożenia działań w zakresie C-SCRM. Chociaż w niniejszej publikacji zdecydowano się na wyszczególnienie kluczowych czynników sukcesu, lista nie jest wyczerpująca i nie opisuje wszystkich czynników, które mogą przyczynić się do skutecznego wdrożenia praktyk w zakresie C-SCRM przez podmiot. Kluczowe czynniki sukcesu są zmienne i z czasem będą ulegać zmianom wraz z rozwojem środowiska i możliwości podmiotu.

3.1. PRAKTYKI C-SCRM W ZAMÓWIENIACH[29]

Włączenie rozważań dotyczących zagadnień w zakresie C-SCRM do działań związanych z zamawianiem oraz nabywaniem towarów na każdym etapie procesu cyklu życia zamówienia i zarządzania umową ma zasadnicze znaczenie dla poprawy zarządzania ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw. Wspomniany cykl życia rozpoczyna się od określenia przez nabywcę potrzeby

[29] Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

i obejmuje procesy planowania i określania wymagań, prowadzenia badań w celu zidentyfikowania i oceny możliwych źródeł dostaw, pozyskiwania ofert, oceny ofert w celu zapewnienia zgodności z wymogami w zakresie C-SCRM oraz oceny ryzyka związanego z obszarem C-SCRM związanego z oferentem, a także z oferowanymi produktami lub usługami. Po udzieleniu zamówienia należy zapewnić, że dostawca spełnia warunki określone w umowie oraz że produkty i usługi są zgodne z oczekiwaniami i wymaganiami. Monitorowanie zmian, które mogą mieć wpływ na ryzyko związane z cyberbezpieczeństwem w łańcuchu dostaw, powinno odbywać się przez cały cykl życia umowy i może wymagać ponownej oceny lub reakcji na ryzyko.

Podmioty polegają w dużej mierze na produktach komercyjnych i usługach zewnętrznych, które umożliwiają im prowadzenie działalności oraz realizację misji i celów biznesowych. Należy jednak podkreślić fakt, że wybrane produkty i usługi są również dostępne poza tradycyjnym procesem zamówień i zaopatrzenia – mowa tu na przykład o oprogramowaniu otwartoźródłowym, wykorzystaniu rozwiązań zapewnianych przez wewnętrznego dostawcę usług wspólnych lub ponownym wykorzystaniu istniejącego produktu w celu zaspokojenia nowej potrzeby. Działania dotyczące obszaru C-SCRM muszą dotyczyć także wszelkich alternatywnych procesów pozyskiwania rozwiązań.

Oprócz uwzględnienia ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw i prowadzenia działań C-SCRM na każdym etapie procesu zamówień, podmioty powinny opracować i realizować strategię zamówień i zaopatrzenia, która prowadzi do zmniejszenia ogólnej ekspozycji na ryzyko. Stosując takie strategie, podmioty mogą zmniejszyć ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw w ramach poszczególnych procesów zamówień oraz w skali całego podmiotu. Podmioty będą wspierać wysiłki mające na celu osiągnięcie zamierzonych rezultatów w zakresie ograniczania ryzyka poprzez wdrażanie polityk i procesów dotyczących zamówień, które włączają działania dotyczące obszaru C-SCRM do działań związanych z zamówieniami.

Wdrażając środki bezpieczeństwa C-SCRM zgodne z uznanymi w branży normami i wytycznymi, na przykład opisanymi w dokumentach NSC 800-53 lub NIST CSF,

podmiot może zapewnić kompleksowe podejście do zagrożeń związanych z cyberbezpieczeństwem w całym łańcuchu dostaw oraz wdrożyć stosowne praktyki C-SCRM. Środki bezpieczeństwa C-SCRM mogą dotyczyć różnych uczestników łańcucha dostaw, w tym samego podmiotu, wykonawców i podwykonawców. Ponieważ podmioty w dużym stopniu opierają się na głównych wykonawcach i ich podwykonawcach w zakresie opracowywania i wdrażania produktów i usług ICT/OT, środki bezpieczeństwa wdrożone w ramach cyklu życia systemu będą z dużym prawdopodobieństwem dotyczyć między innymi podwykonawców.

Ustanowienie środków zabezpieczających C-SCRM mających zastosowanie w całym łańcuchu dostaw i całym cyklu życia systemu pomoże podmiotom w opracowaniu wspólnych zasad oraz zestawu oczekiwań wobec dostawców i poddostawców, aby pomóc wszystkim interesariuszom w zarządzaniu ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw.

3.1.1. Zamówienia w strategii i planie wdrażania C-SCRM

Strategia i plan wdrożenia C-SCRM podmiotu prowadzi podmiot w kierunku osiągnięcia długoterminowego, trwałego zmniejszenia narażenia na ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw. Jako kluczową część strategii C-SCRM i planu wdrożenia, podmioty powinny przyjrzeć się bliżej zagadnieniu zarządzania ryzykiem w całym procesie zamówień i zaopatrzenia.

Ryzyka związane z cyberbezpieczeństwem w łańcuchu dostaw obejmują ryzyka związane z dostawcą, produktami, usługami, a także dostawcami i łańcuchami dostaw dostawców. Biuro zarządzania projektami ds. C-SCRM może być pomocne w opracowaniu konkretnych strategii i planów wdrożeniowych w celu włączenia kwestii dotyczących obszaru C-SCRM do obszaru zamówień. Działania związane z zamówieniami istotne z punktu widzenia C-SCRM to:

- zwiększanie świadomości i komunikowanie oczekiwań dotyczących obszaru C-SCRM w ramach działań związanych z zarządzaniem relacjami z dostawcami;
- ustanowienie listy kontrolnej wymogów bezpieczeństwa zamówień, którą należy wypełnić w ramach wniosków o udzielenie zamówienia, aby zapewnić wprowadzenie niezbędnych zasad i zabezpieczeń;

- wykorzystanie zewnętrznego dostawcy usług wspólnych lub wdrożenie biura zarządzania projektami ds. C-SCRM w celu zapewnienia oceny dostawców, produktów lub usług w formie usługi wspólnej dla innych procesów wewnętrznych, w tym procesów związanych z zamówieniami i zaopatrzeniem;
- prowadzenie analiz due diligence w celu pozyskiwania informacji na temat odpowiedzialności oferenta oraz identyfikacji i oceny postawy oferentów w zakresie ryzyka związanego z danym produktem lub usługą;
- pozyskiwanie oprogramowania otwartoźródłowego ze zweryfikowanych i sprawdzonych bibliotek;
- włączenie kryteriów dotyczących obszaru C-SCRM do ocen wyboru źródła produktu;
- opracowanie listy zakazanych dostawców, jeśli jest ona wymagana, zgodnie z obowiązującymi przepisami i dyrektywami;
- opracowanie i wykorzystywanie zatwierdzonej listy produktów lub listy preferowanych lub kwalifikowanych dostawców, którzy wykazali zgodność z wymogami bezpieczeństwa podmiotu na podstawie rygorystycznego procesu przeprowadzonego przez podmiot bądź innego rozwiązania. [CISA SCRM WG3];
- zapewnienie, że produkty – w tym oprogramowanie lub produkty logiczne obejmujące sprzęt – są dostarczane z listą komponentów, zgodną z odpowiednimi protokołami zatwierdzonymi przez organizację.

Strategia i plan wdrożenia działań w zakresie C-SCRM powinny dotyczyć istotnych z punktu widzenia bezpieczeństwa procesów zamówień komponentów niezbędnych do wdrożenia programu C-SCRM. W celu wsparcia strategii liderzy podmiotów powinni promować wartość i znaczenie praktyk C-SCRM w ramach procesów zaopatrzenia oraz zapewnić wystarczające finansowanie niezbędnych działań. Takie postępowanie pomoże podmiotom zapewnić odpowiedzialność za programy i procesy biznesowe, a także odpowiedzialność za postępy w osiąganiu wyników. Podmioty powinny założyć odpowiednią ilość czasu na działania związane z zapatrzeniem oraz projektami, aby umożliwić realizację działań w zakresie C-SCRM. Podmioty powinny

również przypisać role i obowiązki – niektóre z nich będą dotyczyły wielu podmiotów oraz zespołów, z kolei inne skupią się wyłącznie na procesach zaopatrzenia. Należy także zapewnić odpowiednie szkolenie członkom personelu odpowiedzialnego za zamówienia i zaopatrzenie, aby zapewnić, że role i obowiązki są zrozumiałe i wykonywane zgodnie z oczekiwaniami lidera.

Możliwości podmiotu, jego zasoby, ograniczenia operacyjne oraz istniejące relacje z dostawcami, umowy, nabyte usługi i produkty stanowią podstawowy kontekst niezbędny do opracowania strategii, która jest zarówno realistyczna, jak i osiągalna. Ten wyjściowy punkt odniesienia pełni także rolę znacznika, na podstawie którego można śledzić i oceniać postępy w realizacji i wyniki.

Pierwszym krytycznym krokiem jest zapewnienie, że istnieje aktualny i dokładny spis relacji z dostawcami podmiotu, a także umów oraz wszelkich produktów i usług dostarczanych przez tych dostawców. Informacja ta pozwala na przypisanie tych dostawców do strategicznie istotnych grup określonych przez organizację. Na przykład ocena tych dostawców może doprowadzić do podziału na szereg kategorii – takich jak produkty strategiczne i innowacyjne, produkty krytyczne, produkty wymagane do utrzymania działalności oraz produkty standardowe i niezbędne. Taka segmentacja ułatwia dalszą analizę i zrozumienie narażenia na ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw oraz pomaga dostrzec i nadać priorytet kluczowym dostawcom, którzy mają największe znaczenie strategiczne lub operacyjne dla podmiotu i jego misji oraz procesów biznesowych. Ważne jest także określenie, które produkty i usługi wymagają wyższego poziomu zaufania w zakresie ograniczania ryzyka oraz obszarów ryzyka, takich jak nadmierne poleganie na jednym dostawcy. Taka inwentaryzacja oraz analiza ułatwiają również wybór i dostosowanie zapisów umów w zakresie C-SCRM i kryteriów oceny.

Dodatkowe informacje można znaleźć w Załączniku A do niniejszego dokumentu, a także w dokumencie [NISTIR 8179] oraz zabezpieczeniach SA-1, SA-2, SA-4, SR-5, SR-13 dokumentu NSC800-53.

3.1.2. Znaczenie działań w zakresie C-SCRM w procesie zamówień

Realizując zamówienia, podmioty powinny wyznaczyć ekspertów zajmujących się różnymi obszarami tematycznymi do udziału w procesie pozyskiwania w roli członków zespołu zamówień lub zintegrowanego zespołu projektowego[30]. Obejmuje to kierowników programów, pracowników posiadających wiedzę techniczną oraz dotyczącą bezpieczeństwa, a także przedstawicieli środowisk związanych z dostawami i zaopatrzeniem. Choć wymogi dotyczące zamówień dotyczą konkretnych celów oraz są do nich dostosowane, a także gwarantują zaspokojenie wymogów dotyczących zgodności z przepisami, skuteczne przeciwdziałanie ryzykom związanym z cyberbezpieczeństwem w łańcuchach dostaw wymaga uwzględnienia kontekstu, który obejmuje znaczenie dla podmiotu, wrażliwość danych i środowisko operacyjne.

Określenie kontekstu pozwala zespołowi ds. zamówień i zaopatrzenia skuteczną ocenę tolerancji ryzyka w odniesieniu do konkretnego wymogu zamówienia i określić, które z zabezpieczeń C-SCRM opisanych w niniejszym dokumencie i dokumencie [NSC 800-53] są istotne i konieczne do wdrożenia w przypadku konkretnych zakupów. Biuro programowe lub osoba odpowiedzialna za zamówienie powinna skonsultować się z pracownikami ds. bezpieczeństwa informacji, aby przeprowadzić proces wyboru zabezpieczeń, a także współpracować z osobą odpowiedzialną za zamówienia, aby uwzględnić te zabezpieczenia w dokumentach określających wymagania i w umowach. Bezpieczeństwo powinno być kluczowym czynnikiem przy podejmowaniu decyzji o zamówieniu. Z tego powodu przy zakupie produktów lub usług związanych z ICT/OT podmioty powinny unikać stosowania kryteriów najniższej ceny za produkt spełniający minimalne wymogi techniczne.

Zasady oraz procesy dotyczące zamówień muszą uwzględniać kwestie dotyczące C-SCRM na każdym etapie procesu zarządzania cyklem życia zamówienia i umowy, obejmujących planowanie zamówienia, określanie i opracowywanie wymagań, przeprowadzanie analizy rynku, realizację zamówienia, zapewnienie zgodności oraz monitorowanie pod kątem zmian, które mają wpływ na status ryzyka związanego z cyberbezpieczeństwem

[30] Zintegrowany zespół projektowy jest odpowiednikiem zespołu do spraw zamówień.

w łańcuchu dostaw, zgodnie z dokumentem [NISTIR 7622]. Obejmuje to zapewnienie uwzględnienia zagrożeń związanych z cyberbezpieczeństwem w całym łańcuchu dostaw przy dokonywaniu zamówień związanych z ICT/OT płatnych kartą.

Na etapie planowania zamówienia należy określić zapotrzebowanie i znaczenie zamawianego produktu lub usługi wraz z opisem czynników wpływających na określenie zapotrzebowania i poziomu krytyczności – na tej podstawie ustalany jest poziom tolerowanego ryzyka, osoby zaangażowane w planowanie oraz opracowanie konkretnych wymagań, które będzie musiał spełnić dostawca. Działania te są zwykle realizowane przez osoby odpowiedzialne za misję oraz proces biznesowy jednostki nabywającej lub osoby przez nie wyznaczone we współpracy z kierownikiem do spraw zamówień i zaopatrzenia lub jego przedstawicielem.

Podczas fazy planowania podmiot powinien opracować i określić wymagania dotyczące ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw, a także określić cele w zakresie wydajności, harmonogramu i kosztów. Proces ten jest zazwyczaj inicjowany przez osobę odpowiedzialną za misję oraz osobę odpowiedzialną za proces biznesowy jednostki nabywającej lub osobę wyznaczoną we współpracy z osobą odpowiedzialną za zamówienia i innymi członkami zespołu C-SCRM.

Po określeniu wymagań podmioty zwykle przeprowadzają analizę rynku w celu poszukiwania potencjalnych dostawców. Działania w zakresie badania i analizy rynku badają dostępność potencjalnych lub wstępnie zakwalifikowanych dostawców. Ten krok jest zwykle inicjowany przez osobę odpowiedzialną za misję oraz proces biznesowy lub wyznaczonego przedstawiciela. Podmioty powinny wykorzystać ten etap do przeprowadzenia bardziej szczegółowych analiz due diligence potencjalnych dostawców bądź produktów w celu wygenerowania profilu ryzyka dostawcy.
W ramach analizy due diligence podmiot może rozważyć koncentrację rynku dla poszukiwanego produktu lub usługi jako sposób na identyfikację współzależności w ramach łańcucha dostaw. Podmiot może również wykorzystać prośbę o informacje (*ang. request for information - RFI*), zawiadomienie o poszukiwaniu dostawcy (*ang. sources sought notice - SSN*) oraz kwestionariusze należytej staranności do wstępnego sprawdzenia i zebrania informacji od potencjalnych dostawców. Podmioty nie

powinny traktować wstępnej oceny ryzyka związanego z obszarem C-SCRM jako wyczerpującej. Wyniki tych analiz mogą być również pomocne w kształtowaniu podejścia do zamówień oraz dopracowaniu wymagań.

Na koniec podmiot zakończy etap udzielania zamówienia poprzez opracowanie zakresu prac (*ang. statement of work - SOW)*, oświadczenia o wykonaniu prac (*ang. performance work statement - PWS*) lub oświadczenia o celu (*ang. statement of objective - SOO*) w celu opublikowania zapytania ofertowego (*ang. request for proposal - RFP*) lub zapytania o wycenę (*ang. request for quotes - RFQ*). Każdy oferent odpowiadający na zapytania powinien zostać oceniony według odpowiednich kryteriów C-SCRM. Proces przeglądu ofert powinien również obejmować wszelkie oceny ryzyka dostawcy dotyczące danego zamówienia. Kryteria oceny będą w znacznym stopniu oparte na zdefiniowanych wymaganiach dotyczących C-SCRM i będą obejmowały m.in. informacje o podmiocie, jego procesach bezpieczeństwa i dotychczasowej historii dotyczącej bezpieczeństwa. Proces przeglądu ofert obejmuje wielu interesariuszy procesów C-SCRM, w tym dział zamówień, osobę odpowiedzialną za misję i proces biznesowy, odpowiednie osoby odpowiedzialne za działanie systemów informacyjnych oraz ekspertów technicznych. Przed dokonaniem zakupu podmioty powinny określić i ocenić jakość komponentów produktu lub systemu, autentyczność, podatności oraz inne istotne czynniki ryzyka związanego z cyberbezpieczeństwem w łańcuchu dostaw. Ocena powinna zostać przeprowadzona przed wdrożeniem produktu.

Po zawarciu umowy podmiot powinien śledzić zmiany, które mają wpływ na jego narażenie na ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw. Takie zmiany mogą obejmować wewnętrzne zmiany w podmiocie lub systemie, zmiany operacyjne lub strukturalne po stronie dostawców, aktualizacje produktów oraz zmiany geopolityczne lub środowiskowe. Umowy powinny zawierać postanowienia dające podstawę do ich rozwiązania w przypadku zmian w zakresie ryzyka związanego z cyberbezpieczeństwem w łańcuchu dostaw, którego nie można odpowiednio ograniczyć do dopuszczalnego poziomu. Ponadto podmioty powinny wyciągać wnioski z procesu zamówień, aby stale zwiększać możliwości oceny i monitorowania zagrożeń związanych z cyberbezpieczeństwem w całym łańcuchu dostaw, a także ich oceny.

Tabela 3-1 przedstawia zestawienie etapów procesu zamówień, w których mogą odbywać się analizy C-SCRM.

Tabela 3-1: Działania związane z C-SCRM w procesie zamówień

Proces udzielania zamówień	Ocena ryzyka związanego z usługami	Ocena ryzyka dostawcy	Ocena ryzyka związanego z produktem
Planowanie zamówienia	Ocena ryzyka w zakresie usługi Znaczenie usługi Inny kontekst (realizowane funkcje; dostęp do systemów/danych itp.) Odpowiednie do celu	Odpowiednie do celu	Znaczenie wymaganego produktu Inny kontekst (środowisko operacyjne, dane, użytkownicy, itp.) Odpowiednie do celu
Określenie lub opracowanie wymagań	Określenie odpowiednich zabezpieczeń lub wymagań w zakresie C-SCRM	Określenie odpowiednich zabezpieczeń lub wymagań w zakresie C-SCRM	Określenie odpowiednich zabezpieczeń lub wymagań w zakresie C-SCRM
Przeprowadzenie analizy rynku	Wstępna ocena ryzyka (np. kwestionariusze due diligence)	Wstępna ocena ryzyka (np. kwestionariusze due diligence)	Analiza różnych opcji oraz czynników ryzyka
Zaproszenie do składania ofert/realizacja zamówienia	Potwierdzenie spełnienia wymagań w zakresie C-SCRM Pełna ocena ryzyka	Potwierdzenie spełnienia wymagań w zakresie C-SCRM Pełna ocena ryzyka	Ocena ryzyka przed wdrożeniem
Eksploatacja i konserwacja	Ciągłe monitorowanie ryzyka	Ciągłe monitorowanie ryzyka	Ciągłe monitorowanie ryzyka

Oprócz działań procesowych istnieje wiele użytecznych narzędzi i technik zwiększających bezpieczeństwo zamówień, w tym ukrywanie końcowego zastosowania systemu lub jego komponentu, stosowanie ślepych lub filtrowanych

zakupów, wymóg stosowania opakowań uniemożliwiających manipulację lub stosowanie zaufanych bądź kontrolowanych dystrybutorów. Wyniki oceny ryzyka cyberbezpieczeństwa łańcucha dostaw mogą stanowić źródło wiedzy dotyczącej strategii, narzędzi i metod, które będą najlepszym rozwiązaniem w danej sytuacji. Narzędzia, techniki i praktyki mogą zapewnić ochronę przed nieautoryzowaną produkcją, kradzieżą, manipulacją, wprowadzaniem do obrotu podróbek, wprowadzaniem złośliwego oprogramowania lub tylnych drzwi (*ang. backdoor*) oraz złymi praktykami rozwojowymi w całym cyklu życia systemu.

Aby zapewnić skuteczne i ciągłe zarządzanie ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw i w całym cyklu życia zamówienia, porozumienia umowne i zarządzanie umowami powinny obejmować:

- spełnienie obowiązujących wymogów bezpieczeństwa w zamówieniach i mechanizmach jako warunek udzielenia zamówienia;
- wymagania dotyczące zabezpieczeń dla podwykonawców, obejmujące warunki ich stosowania, w tym cele działań w zakresie C-SCRM powiązane z metodą zabezpieczeń w planie nadzoru zapewnienia jakości lub równoważną metodą monitorowania wydajności;
- okresowa ocena przestrzegania przez dostawców wymogów bezpieczeństwa w celu zapewnienia ciągłej zgodności;
- procesy i protokoły dotyczące komunikacji i zgłaszania informacji o podatnościach, incydentach i innych zakłóceniach działalności, obejmujące dopuszczalne odchylenia, jeśli zakłócenie działalności zostanie uznane za poważne, oraz podstawowe kryteria pozwalające określić, czy zakłócenie kwalifikuje się jako poważne, a także
- warunki, które dotyczą ról, odpowiedzialności i działań rządu, dostawcy i innych podmiotów zewnętrznych w zakresie reagowania na zidentyfikowane ryzyka łańcucha dostaw lub incydenty związane z ryzykiem w celu zmniejszenia narażenia na ryzyko, zminimalizowania szkód i wspierania terminowych działań naprawczych lub usuwania skutków incydentu.

Istnieje wiele dopuszczalnych metod walidacji i rewalidacji, takich jak wymagane certyfikaty, wizyty na miejscu, oceny podmiotów lub samooceny. Rodzaj i zakres

wymaganych metod powinien być współmierny do krytyczności nabywanej usługi lub produktu oraz odpowiadających im wymagań dotyczących zapewnienia bezpieczeństwa.

Dodatkowe wytyczne dotyczące integracji działań w zakresie C-SCRM z procesem nabycia znajdują się w Załączniku C, który opisuje rozszerzone uwzględnienie działań w zakresie C-SCRM w procesie zarządzania ryzykiem [NSC 800-39]. Ponadto, podmioty powinny zapoznać się z zasadami, przepisami oraz najlepszymi praktykami w zakresie nabywania i zamówień, które dotyczą danego sektora (np. sektor infrastruktury krytycznej, samorząd itp.)

Dodatkowe informacje można znaleźć w Załączniku A do niniejszego dokumentu oraz zabezpieczeniach SA-1, SA-2, SA-3, SA-4, SA-9, SA-19, SA-20, SA-22, SR-5, SR-6, SR-10 i SR-11 dokumentu NSC800-53.

3.2. WYMIANA INFORMACJI O ŁAŃCUCHU DOSTAW

Podmioty są stale narażone na ryzyko związane z łańcuchami dostaw. Skuteczny proces wymiany informacji pomaga zagwarantować, że podmioty mogą uzyskać dostęp do informacji, które mają kluczowe znaczenie dla zrozumienia i ograniczenia ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw, a także dzielić się odpowiednimi informacjami z innymi podmiotami, które mogą skorzystać z wiedzy na temat tego ryzyka lub wymagają jej.

Aby pomóc w identyfikacji, szacowaniu, monitorowaniu i reagowaniu na ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw, podmioty powinny włączyć procesy i działania związane z wymianą informacji do swoich programów C-SCRM. Może to obejmować zawieranie umów o wymianie informacji z innymi podmiotami, partnerami biznesowymi i dostawcami. Poprzez wymianę informacji o ryzyku związanym z łańcuchem dostaw (*ang. Supply Chain Risk Information - SCRI*) w ramach społeczności, podmioty mogą wykorzystać zbiorową wiedzę, doświadczenie i możliwości wszystkich interesariuszy, aby uzyskać pełniejsze zrozumienie zagrożeń, z jakimi mogą mieć do czynienia. Dodatkowo, udostępnianie takich informacji pozwala podmiotom na skuteczniejsze wykrywanie kampanii skierowanych do konkretnych sektorów przemysłu i organizacji. Podmiot powinien jednak mieć pewność, że wymiana informacji odbywa się poprzez formalne struktury wymiany informacji, takie

jak Centra Wymiany Informacji i Analiz (*ang. Information Sharing and Analysis Centers - ISAC*). Nieformalne lub nieodpowiednie udostępnianie informacji może narazić podmiot na potencjalne ryzyko prawne.

Dokument NIST SP 800-150 opisuje kluczowe praktyki dotyczące ustanawiania i uczestnictwa współdzielenia informacji, które obejmują:

- ustanowienie celów i zadań w zakresie wymiany informacji, które wspierają procesy biznesowe i polityki bezpieczeństwa,
- określenie istniejących wewnętrznych źródeł informacji,
- określenie zakresu działań związanych z wymianą informacji[31],
- ustanowienie zasad wymiany informacji,
- dołączenie do działań związanych z wymianą informacji i uczestniczenie w nich,
- aktywne dążenie do rozwoju wskaźników poprzez dostarczenie dodatkowego kontekstu, poprawek lub sugerowanych ulepszeń,
- korzystanie z bezpiecznych, zautomatyzowanych przepływów pracy do publikowania, konsumowania, analizowania i wykorzystywania informacji,
- proaktywne zawieranie umów o udostępnianiu informacji,
- ochronę bezpieczeństwa i prywatności informacji wrażliwych,
- zapewnienie stałego wsparcia dla działań związanych z wymianą informacji.

Jak przedstawiono w Tabeli 3-2 poniżej, proces wymiany informacji związanych z łańcuchami dostaw opisuje lub identyfikuje istotne charakterystyki związane z cyberbezpieczeństwem w łańcuchu dostaw oraz czynniki ryzyka związane z produktem, usługą lub źródłem dostaw. Mogą one występować w różnych formach (np. surowe dane, mapa sieci łańcucha dostaw, sprawozdanie z oceny ryzyka itp.) i powinny im towarzyszyć metadane, które ułatwią ocenę poziomu zaufania do informacji i jej wiarygodności. Podmioty powinny stosować się do ustalonych procesów i procedur, które opisują, czy i kiedy udostępnianie lub zgłaszanie

[31] Zakres działań związanych z wymianą informacji powinien obejmować poziom klasyfikacji danych, który został zatwierdzony podczas ostatniej oceny ryzyka dla dostawcy oraz typy danych, które zostały zatwierdzone dla tego dostawcy. Na przykład, jeśli ocena została przeprowadzona dla danych o określonym poziomie klasyfikacji (np. Business Confidential – poufne dane biznesowe podmiotu), a zakres zlecenia zmienia się tak, że obejmuje dane o nowym poziomie klasyfikacji (np. restricted – zastrzeżone dane o ograniczonym dostępie), ocena ryzyka wymaga aktualizacji.

określonych informacji jest obowiązkowe lub dobrowolne oraz czy istnieją jakiekolwiek niezbędne wymagania, których należy przestrzegać w zakresie przetwarzania, ochrony i klasyfikacji informacji.

Tabela 3-2: Charakterystyka łańcucha dostaw i czynniki ryzyka w zakresie cyberbezpieczeństwa związane z produktem, usługą lub źródłem dostaw[32]

Źródło dostaw, charakterystyka produktu lub usługi	Wskaźniki ryzyka, analiza i ustalenia
• Cechy i funkcjonalność • Dostęp do danych i informacji, w tym przywileje systemowe • Środowisko instalacji lub pracy • Bezpieczeństwo, autentyczność i integralność danego produktu lub usługi oraz związanego z nimi łańcucha dostaw i kompilacji • Możliwości dostawcy w zakresie wytworzenia i dostarczenia produktu lub usługi zgodnie z oczekiwaniami • Kontrola podmiotów zagranicznych nad dostawcą (np. struktura własności, osobiste i zawodowe powiązania między dostawcą i jakimkolwiek podmiotem zagranicznym, system prawny jakiegokolwiek obcego kraju, w którym źródło ma siedzibę lub prowadzi działalność)[33] • Rynkowe alternatywy dla dostawcy • Pochodzenie i rodowód komponentów • Relacje i lokalizacje w łańcuchu dostaw • Potencjalne czynniki ryzyka, takie jak czynniki geopolityczne, prawne, środki	• Informacje o zagrożeniach obejmują wskaźniki (artefakty systemowe lub obserwowalne czynniki związane z atakiem), taktyki, techniki i procedury. • Alerty bezpieczeństwa lub raporty o zagrożeniach • Wpływ na bezpieczeństwo narodowe, bezpieczeństwo wewnętrzne, krajową infrastrukturę krytyczną lub procesy związane z wykorzystaniem produktu lub usługi • Podatność systemów, programów lub obiektów na zagrożenia • Ocena poziomu zagrożenia i poziomu podatności na zagrożenia • Potencjalny wpływ lub szkody spowodowane przez możliwą utratę, uszkodzenie lub narażenie produktu, materiału lub usługi na szwank operacji lub misji podmiotu oraz prawdopodobieństwo potencjalnego wpływu, szkody lub możliwości wykorzystania systemu

[32] Charakterystyka łańcucha dostaw i czynniki ryzyka w zakresie cyberbezpieczeństwa związane z produktem, usługą lub źródłem dostaw nie są wyczerpujące.

[33] Dokument Special 301 Report, prepared annually by the Office of the United States Trade Representative (USTR) określa dodatkowe wytyczne dotyczące własności intelektualnej (https://ustr.gov/issue-areas/intellectual-property/special-301).

Tłumaczenie

Źródło dostaw, charakterystyka produktu lub usługi	Wskaźniki ryzyka, analiza i ustalenia
bezpieczeństwa na poziomie zarządu oraz wewnętrzne, stabilność finansowa, incydenty związane z cyberbezpieczeństwem, bezpieczeństwo osobowe i fizyczne lub wszelkie inne informacje, które mogą wpłynąć na analizę bezpieczeństwa, ochrony, integralności, odporności, niezawodności, jakości, wiarygodności lub autentyczności produktu, usługi lub źródła	• Określenie możliwości ograniczania ryzyka

3.3. SZKOLENIE I ŚWIADOMOŚĆ W ZAKRESIE C-SCRM

Do sukcesu działań C-SCRM przyczynia się wiele osób w podmiocie. Mogą to być osoby zajmujące się bezpieczeństwem informacji, zamówieniami, zarządzaniem ryzykiem, inżynierią, tworzeniem oprogramowania, informatyką, zagadnieniami prawnymi i kadrowymi, a także menedżerowie programów. Każda z tych grup przyczynia się do realizacji tych działań na wiele sposobów. Na przykład:

- Osoby odpowiedzialne za systemy ponoszą odpowiedzialność za wiele aspektów działań C-SCRM na poziomie operacyjnym w ramach ich odpowiedzialności za rozwój, zamówienia, integrację, modyfikację, eksploatację, utrzymanie oraz utylizację systemu informacyjnego.
- Dział kadr określa i wdraża politykę weryfikacji pracowników i szkoleń, która pomaga zapewnić, że osoby są przeszkolone w zakresie odpowiednich procesów i procedur dotyczących C-SCRM.
- Dział prawny pomaga w przygotowaniu lub przeglądzie zapisów umów w zakresie C-SCRM, które są włączane do umów z dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych i innymi dostawcami usług związanych z ICT/OT.
- Zespoły zamówień i zaopatrzenia określają proces wdrażania praktyk weryfikacji dostawców będących częścią procesu zamówień.

- Zespoły inżynieryjne projektują produkty i rozumieją obowiązujące wymagania dotyczące korzystania z komponentów otwartoźródłowych.
- Deweloperzy oprogramowania zapewniają, że słabe punkty i podatności w oprogramowaniu są identyfikowane i usuwane na jak najwcześniejszym etapie, między innymi poprzez testowanie i naprawianie kodu.
- Dział logistyki dba o to, by opakowania zawierające krytyczne komponenty nie zostały naruszone w drodze lub w magazynie.
- Kierownicy projektów zapewniają, że plany projektów są opracowywane i uwzględniają kwestie C-SCRM w ramach planów oraz strategii realizacji projektów.

Każdy pracownik podmiotu, w tym użytkownicy końcowi systemów informacyjnych, odgrywa rolę w zarządzaniu ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw. Podmiot powinien promować kulturę bezpieczeństwa, której integralną częścią jest C-SCRM. Podmiot może stosować różne metody komunikacji w celu promowania kultury, z których tradycyjne uświadamianie i szkolenia oparte na rolach są tylko jednym z elementów.

Każdy pracownik podmiotu powinien przejść odpowiednie szkolenie, które umożliwi zrozumienie znaczenia działań w zakresie C-SCRM dla podmiotu, specyficznych zadań i obowiązków oraz tego, jak działania te przekładają się na procesy i procedury zgłaszania incydentów. Szkolenie to może być zintegrowane z ogólnym szkoleniem uświadamiającym w zakresie cyberbezpieczeństwa. Podmioty powinny określić podstawowe wymagania szkoleniowe w szerokim zakresie na poziomie 1, a wymagania te powinny następnie być dostosowane i udoskonalone w oparciu o konkretny kontekst na poziomie 2 i 3.

Osoby pełniące bardziej znaczące role w zarządzaniu ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw powinny odbyć dostosowane do ich potrzeb szkolenie C-SCRM, które pomoże im zrozumieć zakres ich obowiązków, konkretne procesy i wdrożenia procedur, za które są odpowiedzialne, oraz działania, które należy podjąć w przypadku incydentu, zakłócenia lub innego zdarzenia

związanego z C-SCRM. Podmioty powinny ustanowić konkretne kryteria szkoleniowe oparte na rolach i opracować szkolenie C-SCRM dla poszczególnych ról i obowiązków. Podmiot może również rozważyć dodanie treści C-SCRM do istniejących wcześniej szkoleń opartych na rolach dla niektórych konkretnych ról. Więcej szczegółów można znaleźć w rozdziale dotyczącym zabezpieczeń świadomości i szkolenia.

Podmioty są zachęcane do korzystania z ram National Initiative for Cybersecurity Education (NICE) opracowanych przez Narodowy Instytut Standaryzacji i Technologii[34] w celu stworzenie wspólnego leksykonu dotyczącego tematyki C-SCRM dla pracowników. Pomoże to podmiotom w opracowaniu szkoleń związanych z obowiązkami w zakresie C-SCRM dla poszczególnych ról oraz w przekazywaniu pracownikom informacji dotyczących tematów związanych z cyberbezpieczeństwem. Ramy NICE określają kategorie, obszary specjalizacji, role robocze, wiedzę, umiejętności i zdolności oraz zadania, które opisują zagadnienia związane z cyberbezpieczeństwem.

3.4. KLUCZOWE PRAKTYKI W ZAKRESIE C-SCRM[35]

Zarządzanie ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw opiera się na istniejących standardowych praktykach w wielu obszarach i stale rozwijającym się zestawie działań w zakresie C-SCRM. Kluczowe praktyki C-SCRM mają na celu szczególne podkreślenie i zwrócenie uwagi na podzbiór praktyk C-SCRM opisanych w niniejszej publikacji. Podmioty powinny w pierwszej kolejności osiągnąć podstawowy poziom dojrzałości w zakresie tych kluczowych praktyk przed przejściem do wdrażania dodatkowych działań w zakresie C-SCRM. Podmioty powinny dostosować wdrożenie tych praktyk w taki sposób, by uwzględnić tylko najważniejsze obszary zainteresowania w specyficznym kontekście, na przykład w oparciu o dostępne zasoby i profil ryzyka. Kluczowe praktyki w zakresie C-SCRM są opisane w normach i wytycznych NIST, takich jak [NISTIR 8276] oraz innych normach krajowych i międzynarodowych, jeżeli obowiązują. Praktyki w zakresie C-SCRM

[34] Patrz: NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*.

[35] Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

obejmują integrację zagadnień związanych z obszarem C-SCRM w całym podmiocie i obejmują ustanowienie formalnego programu; identyfikację krytycznych produktów, usługi i dostawców oraz zarządzanie nimi, analizę łańcucha dostaw podmiotu; ścisłą współpracę z kluczowymi dostawcami; włączenie kluczowych dostawców w działania związane z odpornością i doskonaleniem; ocenę i monitorowanie w całym okresie relacji z dostawcą; a także kompleksowe planowanie cyklu życia systemów.

3.4.1. Podstawowe praktyki i działania

Wdrożenie podstawowych praktyk jest kluczowe dla udanej i produktywnej współpracy z integratorami systemów. Dostawcy mogą stosować standardowe praktyki w różnym stopniu. Poniżej przedstawiono konkretne przykłady zalecanych wielodyscyplinarnych praktyk podstawowych, które mogą być stopniowo wdrażane w celu poprawy zdolności podmiotu do opracowania i realizacji bardziej zaawansowanych praktyk C-SCRM:

- utworzenie głównego, wyspecjalizowanego, multidyscyplinarnego biura zarządzania programem C-SCRM bądź zespołu do spraw C-SCRM;
- uzyskanie wsparcia kierownictwa wyższego szczebla dla ustanowienia bądź intensyfikacji działań dotyczących obszaru C-SCRM;
- wdrożenie hierarchii zarządzania ryzykiem oraz procesu zarządzania ryzykiem (zgodnie z dokumentem [NSC 800-39]), w tym procesu oceny ryzyka w skali całego podmiotu zgodnie z [NSC 800-30]);
- ustanowienie struktury zarządzania podmiotem, która integruje wymagania C-SCRM i włącza te wymagania do jego zasad i polityk;
- opracowanie procesu identyfikacji kluczowych dostawców, produktów i usług podmiotu oraz oceny stopnia zależności;
- zwiększanie świadomości zagadnień związanych z obszarem C-SCRM oraz ich znaczenia;
- ustanowienie spójnych, dobrze udokumentowanych, powtarzalnych procesów określania poziomów wpływu na przetwarzane informacje (NSC 199);

- ustanowienie i rozpoczęcie stosowania procesów oceny ryzyka dostawcy w trybie priorytetowym – w tym analizy krytyczności, analizy zagrożeń i analizy podatności – po określeniu poziomu wpływu [NSC 199];
- wdrożenie programu jakości i niezawodności, który obejmuje proces i praktyki zapewniania jakości i kontroli jakości;
- ustanowienie jasnych, opartych na współpracy i specyficznych dla danej dyscypliny ról, zakresów odpowiedzialności, struktur i procesów dotyczących łańcucha dostaw, cyberbezpieczeństwa, bezpieczeństwa produktów, bezpieczeństwa fizycznego i innych istotnych procesów (np. w działach prawnych, zespołach ds. zarządzania ryzykiem, dziale kadr, działach finansów, działach IT, wśród menedżerów programów, w zespołach ds. inżynierii systemów, bezpieczeństwa informacji, zamówień i zaopatrzenia, zespołach ds. logistyki i łańcucha dostaw itd.);
- zapewnienie, że odpowiednie zasoby zostały wyznaczone i są wykorzystywane w związku z obszarami bezpieczeństwa informacji i C-SCRM, aby zapewnić właściwe wdrożenie polityk, wytycznych i zabezpieczeń;
- zapewnienie wystarczającej liczby sprawdzonych pracowników pełniących kluczowe role w procesach związanych z C-SCRM i wykonujących obowiązki związane z dostępem do informacji niejawnych związanych z C-SCRM oraz ich udostępnianiem;
- wdrożenie odpowiedniego i dostosowanego zestawu podstawowych środków bezpieczeństwa informacji, które można znaleźć w dokumencie [NSC 800-53];
- ustanowienie wewnętrznych mechanizmów równowagi i kontroli w celu zapewnienia zgodności z wymogami bezpieczeństwa i jakości;
- ustanowienie programu zarządzania dostawcami, który obejmuje między innymi wytyczne dotyczące zamówień od zakwalifikowanych producentów oryginalnego sprzętu (OEM)[36] lub ich autoryzowanych dystrybutorów i sprzedawców;

[36] Na potrzeby niniejszej publikacji termin producenci oryginalnego sprzętu obejmuje także producentów oryginalnych części i komponentów.

- wdrożenie skutecznego programu zarządzania incydentami w celu zapewnienia sprawnego identyfikowania incydentów bezpieczeństwa, reagowania na ich wystąpienie oraz ograniczania ich skutków. Program ten powinien być w stanie doprowadzić do określenia podstawowej przyczyny incydentów bezpieczeństwa, w tym incydentów, których źródłem jest łańcuch dostaw;
- ustanowienie wewnętrznych procesów w celu weryfikacji, czy dostawcy i usługodawcy aktywnie identyfikują i ujawniają podatności w swoich produktach;
- stworzenie możliwości zarządzania i monitorowania składników oprogramowania wbudowanego w celu zarządzania ryzykiem w całym podmiocie (np. SBOM[37] połączone z krytycznością, podatnością, zagrożeniem i możliwością wykorzystania w celu większej automatyzacji).

3.4.2. Działania podtrzymujące

W celu zwiększenia skuteczności zarządzania ryzykiem dotyczącego cyberbezpieczeństwa w łańcuchu dostaw należy wdrażać i stosować działania podtrzymujące. Obejmują one podstawowe praktyki i działania, a także opierają się na nich. Podmioty, które w szerokim zakresie znormalizowały i wdrożyły podstawowe praktyki, powinny rozważyć wdrożenie działań podtrzymujących, które stanowią kolejny etap rozwoju możliwości zarządzania ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw:

- utworzenie programu bezpieczeństwa opartym na informacjach o zagrożeniach oraz wykorzystywanie go w praktyce;
- wykorzystanie mechanizmów budowania zaufania, takich jak badania oceniające prowadzone przez podmioty zewnętrzne, lokalne wizyty oraz formalne certyfikaty (np. ISO 27001) do oceny najważniejszych możliwości i praktyk dostawców w zakresie bezpieczeństwa;
- ustanowienie formalnych procesów i częstotliwości ciągłego monitorowania i ponownej oceny dostawców, dostarczanych produktów i usług oraz samego łańcucha dostaw pod kątem potencjalnych zmian w profilu ryzyka;

[37] *Ang. Software Bill of Materials - SBOM.*

- wykorzystanie zrozumienia przez podmiot profilu ryzyka związanego z obszarem C-SCRM (lub profili ryzyka dotyczących poszczególnych misji i obszarów biznesowych) w celu określenia apetytu na ryzyko oraz tolerancji ryzyka, aby umożliwić liderom podmiotu podejmowanie decyzji dotyczących działań w zakresie C-SCRM zgodnie z założeniami misji podmiotu oraz celami i zadaniami strategicznymi;
- wykorzystanie działu lub pionu wymiany informacji w celu nawiązania współpracy z ISAC, i innymi organizacjami publicznymi[38], co pozwoli rozszerzyć wiedzę podmiotu na temat zagrożeń i ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw oraz pomóc w zapewnieniu skoordynowanego i holistycznego podejścia do zagrożeń związanych z cyberbezpieczeństwem w całym łańcuchu dostaw, które mogą mieć wpływ na wiele organizacji państwowych, sektor prywatny lub bezpieczeństwo narodowe;
- koordynacja z kierownictwem programu cyberbezpieczeństwa podmiotu w celu przekazania informacji na temat profilu ryzyka związanego z obszarem C-SCRM komitetom najwyższego szczebla zajmującym się ryzykiem w podmiocie;
- włączenie szkoleń dotyczących działań w zakresie C-SCRM do programów szkoleniowych dla odpowiednich ról w procesach podmiotu związanych z C-SCRM, w tym bezpieczeństwa informacji, zaopatrzenia, zarządzania ryzykiem, inżynierii, rozwoju oprogramowania, IT, zagadnień prawnych oraz kadrowych;
- włączenie zagadnień związanych z obszarem C-SCRM do każdego aspektu cyklu życia systemu i produktu oraz wdrożenie spójnych, dobrze udokumentowanych, powtarzalnych procesów dla inżynierii systemów, praktyk w zakresie cyberbezpieczeństwa i zamówień;
- włączenie zdefiniowanych przez podmiot wymagań w zakresie C-SCRM do treści umów z dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych oraz innymi dostawcami usług związanych z ICT/OT;

[38] Instytucje publiczne (dalej w publikacji: organizacje) to różne organy i jednostki, które zapewniają obywatelom dostęp do świadczeń i usług związanych z ochroną, edukacją, zdrowiem, prawem, finansami i innymi dziedzinami życia. Instytucje publiczne finansowane są ze środków publicznych.

- uwzględnienie kluczowych dostawców w planowaniu awaryjnym, reagowaniu na incydenty oraz planowaniu odtworzenia po katastrofie i testach;
- współpraca z dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych i innymi dostawcami usług związanych z ICT/OT w celu poprawy ich praktyk w zakresie cyberbezpieczeństwa;
- określanie, gromadzenie i raportowanie wskaźników związanych z obszarem C-SCRM w celu zapewnienia świadomości ryzyka, umożliwienia aktywnego zarządzania wdrożeniami działań w zakresie C-SCRM oraz zwiększania skuteczności procesów i praktyk C-SCRM wdrażanych w podmiocie.

3.4.3. Praktyki i działania udoskonalające

Praktyki i działania udoskonalające powinny być wdrażane przez podmiot w celu osiągania adaptacyjnych i predykcyjnych możliwości związanych z obszarem C-SCRM. Podmioty powinny stosować te praktyki, gdy działania podtrzymujące zostaną wdrożone i znormalizowane w całym podmiocie:

- Automatyzacja procesów związanych z obszarem C-SCRM wszędzie tam, gdzie jest to możliwe w celu zapewnienia spójności realizacji, wydajności i możliwości wykorzystania najważniejszych zasobów wymaganych do innych kluczowych działań w tym obszarze.
- Przeprowadzanie ilościowych analiz ryzyka, w których stosuje się podejścia probabilistyczne (np. analizę bayesowską) w celu zmniejszenia niepewności co do prawdopodobieństwa wystąpienia i wpływu zagrożeń związanych z cyberbezpieczeństwem w całym łańcuchu dostaw, optymalizacji alokacji zasobów na potrzeby reakcji na ryzyko, a także określenie stopy zwrotu z inwestycji (tj. skuteczności reagowania).
- Wdrożenie wniosków zebranych na podstawie najważniejszych wskaźników związanych z obszarem C-SCRM (tj. wskaźników perspektywicznych), aby przejść do realizacji predykcyjnych strategii i planów dotyczących C-SCRM, które dostosowują się do zmian profilu ryzyka, zanim one wystąpią.
- Stworzenie lub uczestnictwo w społeczności praktyków (np. Centrum Doskonałości) w celu wzmocnienia i usprawnienia praktyk i działań w zakresie C-SCRM.

Wytyczne oraz zabezpieczenia opisane w niniejszej publikacji opierają się na istniejących praktykach multidyscyplinarnych i mają na celu zwiększenie zdolności podmiotów do strategicznego zarządzania ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw przez cały cykl życia systemów, produktów i usług. Podsumowanie kluczowych praktyk i działań w zakresie C-SCRM znajduje się w tabeli 3-3.

3.5. POMIAR WDROŻENIA MOŻLIWOŚCI ORAZ DZIAŁAŃ W ZAKRESIE C-SCRM

Podmioty powinny aktywnie zarządzać efektywnością i skutecznością swoich programów C-SCRM w ramach ciągłych analiz samych programów. Podmioty mogą wykorzystać kilka metod do pomiaru i zarządzania efektywnością swojego programu C-SCRM:

- wykorzystanie istniejących ram takich jak NIST CSF do oceny możliwości oraz zdolności w obszarze C-SCRM,
- analiza postępów realizacji inicjatyw C-SCRM,
- analiza skuteczności C-SCRM w zakresie osiągania pożądanych celów.

Wszystkie metody opierają się na różnych działaniach związanych z gromadzeniem, analizą, kontekstualizacją i raportowaniem danych. Metody te powinny być wykorzystywane do śledzenia i raportowania postępów i wyników, które wskazują na zmniejszenie narażenia na ryzyko i poprawę wyników podmiotu w zakresie bezpieczeństwa.

Zarządzanie skutecznością praktyk i działań w zakresie C-SCRM zapewnia wiele korzyści biznesowych i finansowych. Główne korzyści obejmują zwiększenie odpowiedzialności interesariuszy za rezultaty działań w zakresie C-SCRM; poprawę skuteczności działań C-SCRM; wykazanie zgodności z przepisami, zasadami i dyrektywami; gromadzenie danych usprawniających proces alokacji zasobów; oraz unikanie kosztów związanych z ograniczeniem wpływu lub prawdopodobieństwa wystąpienia incydentu związanego z cyberbezpieczeństwem w łańcuchu dostaw.

Podmioty mogą wykorzystać istniejące ramy w celu określenia bazowego poziomu swoich możliwości dotyczących obszaru C-SCRM – to między innymi NIST CSF Implementation Tiers, które pozwalają podmiotowi obserwować i mierzyć rozwój swoich praktyk i działań w obszarze C-SCRM. Postępy oceniane na podstawie ram są mierzone przy pomocy skali ocen (1-5), które pozwalają na uwidocznienie postępów prac na poszczególnych poziomach. Poniżej przedstawiono przykłady, w jaki sposób może przebiegać ocena możliwości podmiotu w zakresie C-SCRM poprzez zastosowanie poszczególnych poziomów NIST CSF Tiers na podstawie opublikowanej normy:

- CSF Tier 1: Podmiot nie rozumie swojej ekspozycji na ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw ani swojej roli w szeroko pojętym ekosystemie. Podmiot nie współpracuje z innymi podmiotami ani nie wdrożył procesów mających na celu określenie, ocenę i ograniczanie ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw.
- CSF Tier 2: Podmiot rozumie ryzyka związane z cyberbezpieczeństwem w całym łańcuchu dostaw oraz swoją rolę w szeroko pojętym ekosystemie. Podmiot nie sformalizował swoich działań w zakresie zarządzania ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw ani zdolności do nawiązywania kontaktów i wymiany informacji z podmiotami w ramach szeroko pojętego ekosystemu.
- CSF Tier 3: Obejmujące cały podmiot podejście do zarządzania ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw jest realizowane poprzez polityki, procesy i procedury zarządzania ryzykiem. Obejmuje to także strukturę zarządzania (np. komitet ds. ryzyka), która uwzględnia zarządzanie ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw na równi z innymi ryzykami podmiotu. Polityki, procesy i procedury są konsekwentnie wdrażane zgodnie z założeniami oraz stale monitorowane i poddawane przeglądom. Pracownicy posiadają wiedzę i umiejętności pozwalające na wykonywanie wyznaczonych obowiązków w zakresie zarządzania ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw. Podmiot zawarł formalne umowy informujące o podstawowych wymaganiach

w tym zakresie dostawców i partnerów. Podmiot rozumie swoje zależności od innych podmiotów na rynku i współpracuje z partnerami w celu wymiany informacji, aby umożliwić podejmowanie decyzji dotyczących zarządzania opartego na ryzyku w odpowiedzi na zdarzenia.

- CSF Tier 4: Podmiot aktywnie wykorzystuje informacje oraz przekazuje je partnerom, a także wykorzystuje informacje przekazywane w czasie rzeczywistym lub zbliżonym do rzeczywistego w celu poprawy cyberbezpieczeństwa i bezpieczeństwa łańcucha dostaw zanim wystąpią zdarzenia. Podmiot wykorzystuje wiedzę na temat zarządzania ryzykiem dotyczącego cyberbezpieczeństwa w łańcuchu dostaw u swoich zewnętrznych dostawców i partnerów, wewnętrznie w powiązanych obszarach funkcjonalnych oraz na wszystkich szczeblach własnej działalności. Podmiot podejmuje proaktywną komunikację przy pomocy mechanizmów formalnych (np. umów) oraz nieformalnych, aby rozwijać i utrzymywać relacje ze swoimi dostawcami, nabywcami i innymi partnerami.

Budowanie zdolności zaczyna się od stworzenia solidnych podstaw programowych, które obejmują strategie i plany, ustanowienie polityk i wytycznych, inwestycje w szkolenia, a także przydział odpowiednich zasobów. Po ustanowieniu tych podstaw, podmiot może wykorzystać plany rozwoju zawarte w ramach, aby wyznaczyć strategiczny kierunek swoich programów oraz rozwijać swoje możliwości w zakresie C-SCRM w różnych obszarach programu. W tabeli 3-3 przedstawiono przykładowy model wdrożenia C-SCRM w podmiocie.

Tabela 3-3: Przykładowy model wdrożenia praktyk w zakresie C-SCRM w podmiocie[39]

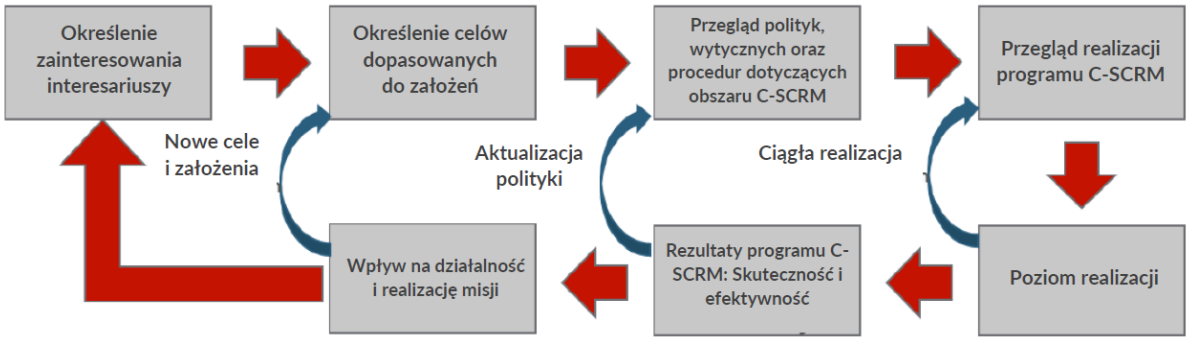
Poziom wdrożenia	Powiązane praktyki w zakresie C-SCRM
Podstawowy	• Utworzenie biura zarządzania projektami ds. C-SCRM • Uzyskanie wsparcia kierownictwa dotyczącego działań w zakresie C-SCRM

[39] Więcej informacji na temat możliwości C-SCRM znajduje się w rozdziale 3.4 – Kluczowe praktyki w zakresie C-SCRM.

Poziom wdrożenia	Powiązane praktyki w zakresie C-SCRM
	• Ustanowienie polityk w zakresie C-SCRM na wszystkich szczeblach podmiotu • Określenie hierarchii C-SCRM • Stworzenie struktury zarządzania obszarem C-SCRM • Dobrze udokumentowane, spójne procesy dotyczące C-SCRM • Wprowadzenie w podmiocie kultury uwzględniającej obszar C-SCRM • Wprowadzenie programu jakości i niezawodności • Włączenie zagadnień dotyczących obszaru C-SCRM do polityk zamówień i zaopatrzenia • Określenie poziomów wpływu na podstawie dokumentu NSC 199 • Określenie wyraźnych ról w obszarze C-SCRM • Przydział odpowiednich zasobów na potrzeby działań w obszarze C-SCRM • Określenie podstawowych zabezpieczeń dotyczących obszaru C-SCRM • Ustanowienie wewnętrznych mechanizmów równowagi i kontroli w obszarze C-SCRM w celu zapewnienia zgodności • Opracowanie programu zarządzania dostawcami • Włączenie praktyk C-SCRM do istniejącego programu zarządzania incydentami • Wprowadzenie procesów zapewniających ujawnianie przez dostawców podatności
Utrzymanie	• Program bezpieczeństwa wykorzystujący informacje o zagrożeniach • Wykorzystywanie ocen podmiotów zewnętrznych, wizyt na miejscu i formalnej certyfikacji • Opracowanie formalnego programu monitorowania dostawców • Określenie apetytu na ryzyko w zakresie C-SCRM i tolerancji ryzyka w tym obszarze • Formalizacja procesów wymiany informacji (np. współpraca z FASC)

Poziom wdrożenia	Powiązane praktyki w zakresie C-SCRM
	• Regularne raportowanie zagrożeń związanych z obszarem C-SCRM kierownictwu bądź komitetom ds. ryzyka • Wdrożenie formalnego programu szkoleń dotyczących obszaru C-SCRM • Integracja działań w zakresie C-SCRM z cyklem życia systemu • Włączenie zagadnień związanych z C-SCRM do treści umów • Zaangażowanie dostawców w proces reagowania na incydenty, przywracania danych po katastrofie oraz planowania awaryjnego • Współpraca z dostawcami w celu poprawy ich praktyk w zakresie cyberbezpieczeństwa • Formalne określenie, gromadzenie oraz raportowanie wskaźników i danych dotyczących obszaru C-SCRM
Udoskonalanie	• Automatyzacja procesów C-SCRM • Wykorzystywanie ilościowej analizy ryzyka • Wdrożenie predykcyjnych i adaptacyjnych strategii i procesów w obszarze C-SCRM • Utworzenie społeczności praktyków lub uczestnictwo w istniejącej społeczności

3.5.1. Pomiar działań w obszarze C-SCRM na podstawie wskaźników efektywności



Rysunek 3-1: Proces rozwoju wskaźników dotyczących obszaru C-SCRM

Podmioty zazwyczaj opierają się na wskaźnikach dotyczących bezpieczeństwa informacji wykorzystywanych w celu podejmowania decyzji oraz poprawy osiągów i dbania o odpowiedzialność za swoje programy bezpieczeństwa informacji. Podmioty mogą

osiągnąć podobne korzyści w ramach swoich programów działań w zakresie C-SCRM. Dodatkowo, podmioty powinny przekazywać informacje na temat wskaźników C-SCRM do zarządu w ramach procesu zarządzania ryzykiem w podmiocie.

Rysunek 3-1 ilustruje proces opracowywania wskaźników na podstawie dokumentu [NIST SP 800-55, Rev. 1], który obejmuje:

- **Określenie zainteresowania interesariuszy:** Określenie głównych (np. CISO, CIO, CTO) i drugorzędnych interesariuszy związanych z obszarem C-SCRM (np. kierownik jednostki organizacyjnej/dyrektor generalny, COO, CFO) oraz określenie/pomiar wymagań w oparciu o kontekst wymagany przez każdego interesariusza lub grupy interesariuszy.
- **Określenie celów i zadań:** Określenie i udokumentowanie celów strategicznych podmiotu oraz celów dotyczących obszaru C-SCRM. Cele te mogą być wyrażone w postaci planów strategicznych podmiotu, polityk C-SCRM, wymagań, przepisów prawa, rozporządzeń itd.
- **Przegląd polityk, wytycznych oraz procedur dotyczących obszaru C-SCRM:** Określenie praktyk w zakresie C-SCRM, środków bezpieczeństwa i oczekiwań zawartych w tych dokumentach oraz wykorzystanie ich do przeprowadzenia wdrożenia działań związanych z obszarem C-SCRM w całym podmiocie.
- **Przegląd realizacji programu C-SCRM:** Zebranie wszystkich dostępnych danych, wskaźników i dowodów, które mogą stanowić podstawy do opracowania nowych wskaźników i działań. Można je znaleźć w planach C-SCRM, planach działań i kamieni milowych. ocenach dostawców itp.
- **Poziom realizacji:** Opracowanie i przyporządkowanie wskaźników do określonych standardów, polityk i procedur dotyczących obszaru C-SCRM w celu wykazania postępów we wdrażaniu programu. Wskaźniki te powinny być brane pod uwagę przy podejmowaniu decyzji o ustalaniu priorytetów i inwestowaniu w rozwój możliwości w zakresie C-SCRM.
- **Rezultaty programu C-SCRM w zakresie skuteczności i efektywności:** Opracowanie i przyporządkowanie wskaźników C-SCRM do określonych celów strategii i polityk

w celu weryfikacji, czy udało się osiągnąć pożądane rezultaty działań. Wskaźniki te powinny być rozpatrywane w ramach przeglądów działań i polityk.

- **Wpływ na działalność i realizację misji:** Opracowanie i przyporządkowywanie wskaźników dotyczących określonych celów strategicznych podmiotu oraz celów związanych z działaniami w zakresie C-SCRM w celu zapewnienia przeglądu wpływu praktyk w obszarze C-SCRM (np. wpływ na oszczędności w obrębie procesów biznesowych; wpływ na bezpieczeństwo narodowe). Wskaźniki te powinny być rozpatrywane w ramach przeglądów celów oraz założeń.

Podobnie jak w przypadku wskaźników dotyczących bezpieczeństwa informacji, także wskaźniki dotyczące C-SCRM mogą być gromadzone na różnych szczeblach działalności podmiotu. Tabela 3-4 przedstawia przykładowe zagadnienia, które mogą być określane przy pomocy wskaźników na każdym z trzech poziomów zarządzania ryzykiem.

Tabela 3-4: Przykładowe mierzalne zagadnienia na poszczególnych poziomach zarządzania ryzykiem

Poziom zarządzania ryzykiem	Przykładowe mierzalne zagadnienia
Poziom 1	• wdrożenie polityk na niższych poziomach • terminowość wdrażania polityk na niższych poziomach • realizacja założeń w zakresie apetytu na ryzyko i tolerowania ryzyka • zróżnicowane poziomy narażenia na ryzyko na poziomie 2 • zgodność z przepisami, dyrektywami i normami • zgodność z wymogami klienta
Poziom 2	• skuteczność strategii mających na celu ograniczanie ryzyka • przeznaczanie czasu na działania w zakresie C-SCRM • narażenie na ryzyko na poziomie misji i procesu biznesowego • zakres oraz jakość wdrożenia wymogów dotyczących C-SCRM w ramach misji i procesów biznesowych • korzystanie z usług biura zarządzania projektami ds. C-SCRM przez poziom 3

Poziom zarządzania ryzykiem	Przykładowe mierzalne zagadnienia
Poziom 3	• skuteczność projektowa zabezpieczeń • skuteczność operacyjna zabezpieczeń • efektywność kosztowa zabezpieczeń

Podmioty powinny potwierdzić określone cele oraz założenia w zakresie C-SCRM z docelowymi grupami interesariuszy przed podjęciem wysiłków w celu opracowania konkretnych działań i wskaźników. Opracowując wskaźniki C-SCRM, podmioty powinny skoncentrować się na kluczowych priorytetach interesariuszy i wyznaczyć je w oparciu o dane, które można realistycznie pozyskać i zgromadzić. Każdy ustalony wskaźnik powinien mieć określony cel wykorzystywany do oceny, czy założenia oraz cele związane z danym wskaźnikiem są realizowane. Podmioty powinny rozważyć zastosowanie szablonów w celu formalizacji wskaźników oraz wykorzystania ich w roli punktu odniesienia dla wszystkich informacji dotyczących danego wskaźnika. Co więcej, podmioty powinny wypracować mechanizmy wymiany informacji zwrotnych z interesariuszami, aby zagwarantować, że wskaźniki stanowią źródło pożądanych informacji i są dostosowane do ogólnych celów strategicznych podmiotu w zakresie C-SCRM.

3.6. FINANSOWANIE DZIAŁAŃ W ZAKRESIE C-SCRM

Aby odpowiednio zarządzać ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw, podmioty powinny przeznaczyć określone środki na ten cel. Określenie zapotrzebowania na zasoby oraz podjęcie działań w celu zapewnienia stosownego, powtarzalnego i dedykowanego finansowania to kluczowe działania, które muszą stanowić część strategii C-SCRM oraz zostać uwzględnione w obszarach planowania i wdrożenia, a także włączone do procesów ustalania budżetu, przeglądu inwestycji i zarządzania funduszami w podmiocie. Dostęp do odpowiednich zasobów jest kluczowym czynnikiem umożliwiającym ustanowienie i utrzymanie programu C-SCRM. Jeśli jest to możliwe, należy zachęcać podmioty do wykorzystania istniejących źródeł finansowania w celu zwiększania zdolności w zakresie C-SCRM. Stała dostępność funduszy celowych pozwoli podmiotom na utrzymanie i rozszerzanie tych możliwości w czasie.

Zabezpieczenie i przydział środków na działania w zakresie C-SCRM jest wyrazem świadomości znaczenia C-SCRM wśród liderów, a także wpływu tego obszaru dla bezpieczeństwa narodowego i gospodarczego oraz zapewnienie ochrony, ciągłości i odporności procesów biznesowych i misji podmiotu, a także jego majątku.

Odpowiednie finansowanie umożliwia planowanie zorientowane na cele i działania. Badanie potrzeb w zakresie zasobów i przydzielanie środków finansowych wymaga stosownego procesu budżetowania i planowania strategicznego. Skuteczne podmioty zaczynają te wysiłki od określenia zestawu celów i zadań, które będą stanowić elementy planu strategicznego określającego drogę do ich osiągnięcia poprzez przydzielenie i alokację ograniczonych zasobów. Przydział środków na realizację celów programu C-SCRM pozwala na przypisanie odpowiedzialności za jego rezultaty oraz stanowi motywator dla pracowników odpowiedzialnych za jego realizację do efektywności, skuteczności oraz ciągłego doskonalenia możliwości w zakresie C-SCRM i osiągania wyników zwiększających bezpieczeństwo.

Pozyskanie nowych lub większych środków może stanowić wyzwanie, ponieważ zasoby są często ograniczone i niezbędne do realizacji wielu konkurencyjnych celów. Ograniczone środki finansowe wymuszają z kolei ustalanie priorytetów. Liderzy działań w zakresie C-SCRM muszą najpierw przeanalizować, jakie rezultaty mogą osiągnąć wykorzystując dostępne zasoby, a także opracować argumenty, ustalić priorytety oraz skutecznie uzasadniać swoje prośby o dodatkowe zasoby. W przypadku nowych inwestycji wymaga to uzgodnienia planowanych inicjatyw z misją podmiotu i celami biznesowymi. Dobrze przeprowadzony i systematyczny proces planowania może przyczynić się do lepszego dopasowania procesów C-SCRM do tych celów.

Wiele procesów C-SCRM może stanowić element istniejących programów i działań operacyjnych, mogą być także realizowane przy wykorzystaniu dostępnych środków. Może jednak zaistnieć potrzeba uzyskania jednorazowo dodatkowych środków na potrzeby zapoczątkowania programu C-SCRM oraz wprowadzenia pierwszych działań z nim związanych. Może to obejmować na przykład potrzebę zatrudnienia nowych pracowników posiadających stosowne doświadczenie w zakresie praktyk C-SCRM,

uzyskanie wsparcia ze strony podmiotu zewnętrznego w celu opracowania wytycznych dla programu C-SCRM, a także konieczność opracowania treści szkolenia C-SCRM dla poszczególnych grup. W niektórych sytuacjach może brakować zasobów do zaspokojenia wszystkich potrzeb związanych z realizacją programu C-SCRM. Może zaistnieć potrzeba przesunięcia istniejących funduszy w kierunku działań związanych z obszarem C-SCRM lub wystąpienia o nowe lub dodatkowe fundusze. Podmioty powinny również szukać możliwości wykorzystania usług wspólnych, gdy tylko jest to możliwe.

Wykorzystanie usług wspólnych pozwoli na optymalizację wykorzystania ograniczonych zasobów i skupianie wszystkich działań w ramach centrów doskonałości, które zapewniają efektywny kosztowo dostęp do usług, systemów lub narzędzi. Podmioty mogą wykorzystać mechanizmy podziału kosztów w swoich jednostkach niższego szczebla, które umożliwiają efektywny kosztowo dostęp do zasobów i możliwości C-SCRM. Podmioty, które realizują modele usług wspólnych w zakresie C-SCRM, powinny być również świadome wyzwań związanych z takimi modelami. Usługi wspólne (np. biuro zarządzania projektami ds. C-SCRM) są najbardziej efektywne, gdy działania w całym podmiocie opierają na dość jednolitym zestawie strategii, polityk i procesów C-SCRM. W wielu przypadkach scentralizowana realizacja usług dotyczących obszaru C-SCRM wymaga sprawnej infrastruktury technologicznej. Systemy podmiotu powinny wspierać automatyzację procesów i scentralizowane dostawy, aby w pełni wykorzystać korzyści płynące z modelu usług wspólnych.

Konsultacje z kierownikami odpowiedzialnymi za budżet oraz finansowanie są kluczem do ustalenia, jakie możliwości są dostępne i wykonalne w najbliższym czasie i w kolejnych latach. Osoby te mogą również doradzić, w jaki sposób najlepiej uzasadnić potrzeby, a także jakie są ramy czasowe i procesy związane z wnioskowaniem o przydział dodatkowych środków. W wielu przypadkach istnieją różne procesy, których wymogów należy przestrzegać w celu uzyskania stałego dofinansowania oraz w ramach ubiegania się o jednorazowe dofinansowanie. Na przykład uzyskanie środków na zakup nowego systemu informacyjnego w celu wsparcia działań w zakresie C-SCRM może wiązać się z koniecznością opracowania

formalnego uzasadnienia biznesowego przedstawionego do zatwierdzenia przez jednostkę odpowiedzialną za ocenę inwestycji podmiotu. Organizacje mogą uznać, że pomocnym rozwiązaniem będzie rozłożenie zapotrzebowania na środki na koszty bieżące i jednorazowe lub ich podział na kategorie kosztów zgodne z założeniami budżetu, procesem podejmowania decyzji dotyczących alokacji zasobów oraz zarządzania dostępnymi środkami.

Zaleca się, aby biuro zarządzania projektami ds. C-SCRM było odpowiedzialne za koordynację z osobami odpowiedzialnymi za misję, procesy biznesowe oraz ustalanie budżetu, aby wspólnie opracować i utrzymywać wieloletni budżet na potrzeby programu C-SCRM, który uwzględnia zarówno powtarzalne, jak i jednorazowe zapotrzebowania na środki oraz łączy je z dostępnymi źródłami finansowania. Aby zrozumieć zakres wymaganego finansowania, a także potrzeby i cele, podmioty powinny określić i ocenić jaki rodzaj i zakres zasobów (środków, materiałów lub pracowników) jest wymagany do wdrożenia programu C-SCRM i bieżącej realizacji wymaganych procesów C-SCRM. Koszt związany z każdą z tych potrzeb może zostać następnie ujęty w budżecie, który będzie zawierał pozycje dotyczące odpowiednich kategorii kosztów, takich jak koszty zatrudnienia, umów, szkoleń, delegacji, narzędzi lub systemów. Zapewni to podmiotowi podstawowy wgląd w możliwości realizacji programu w ramach dostępnych środków oraz luki, które należy wypełnić. Rzeczywisty podział środków może być ujęty w ramach jednego budżetu programu C-SCRM lub rozproszony w ramach całego podmiotu i odzwierciedlony w budżetach poszczególnych biur, a także jednostek odpowiedzialnych za misje i procesy biznesowe. Niezależnie od sposobu przydziału środków, opracowanie głównego budżetu programu C-SCRM oraz analiza stanu jego finansowania stanowi cenne źródło informacji, które pozwoli na uzasadnienie nowych wniosków, ustalanie priorytetów oraz dostosowanie oczekiwań dotyczących pewnych działań i czasu, w którym mogą być one zrealizowane.

Zapewnienie ujęcia finansowania programu C-SCRM w budżecie podmiotu, a także opracowanie wskaźników efektywności powiązanych z finansowaniem, pozwoli na zwiększenie odpowiedzialności pracowników za osiągane rezultaty. Dodatkowo jasne i czytelne ujęcie przeznaczenia środków we wnioskach o finansowanie oraz planach

realizacji i sprawozdaniach skłoni kierownictwo do zwrócenia uwagi na procesy C-SCRM i realizację celów. Należy okresowo występować o budżety i opatrywać wnioski stosownymi uzasadnieniami. Proces ten umożliwia kierownikom oraz liderom obserwowanie oraz mierzenie skuteczności oraz wykorzystania przydzielonych środków. Takie działanie stanowi z kolei motywator dla pracowników odpowiedzialnych za realizację programu i działań C-SCRM do obserwacji wyników oraz odpowiedniego zarządzania rezultatami działań.

Najważniejsze wnioski[40]

Praktyki C-SCRM w zamówieniach. Włączenie zagadnień dotyczących obszaru C-SCRM do działań związanych z zamówieniami i zakupami jest kluczem do zapewnienia skuteczności programu C-SCRM. Wymagania dotyczące obszaru C-SCRM powinny zostać uwzględnione w całym cyklu życia zamówień. Działania związane z obszarem C-SCRM obejmują przeprowadzanie oceny ryzyka usług, dostawców i produktów; określanie odpowiednich zabezpieczeń w zakresie C-SCRM; przeprowadzanie analiz due diligence, a także stałe monitorowanie dostawców.

Wymiana informacji o łańcuchu dostaw. Podmioty uzyskają dostęp do kluczowych informacji pozwalających na zrozumienie ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw dzięki wykorzystaniu procesów i działań związanych z wymianą informacji w ramach programów C-SCRM. Podmioty powinny współpracować z innymi podmiotami, partnerami biznesowymi, dostawcami i społecznościami zajmującymi się wymianą informacji (np. ISAC), aby uzyskiwać informacje na temat ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw i korzystać z doświadczeń całej społeczności.

Świadomość i szkolenie w zakresie C-SCRM. Podmioty powinny wdrożyć programy szkoleniowe obejmujące całe jednostki oraz poszczególne grupy, aby edukować użytkowników na temat potencjalnego wpływu zagrożeń związanych z cyberbezpieczeństwem w całym łańcuchu dostaw oraz najlepszych praktyk

[40] Najważniejsze wnioski opisują kluczowe informacje zawarte w tekście rozdziału. Definicje znajdują się w glosariuszu, który stanowi Załącznik H do niniejszego dokumentu.

dotyczących ograniczania tego ryzyka. Stosowne przeszkolenie pracowników w zakresie C-SCRM jest kluczowym czynnikiem umożliwiającym podmiotom wdrożenie w swoich strukturach kultury zakładającej znajomość tego zagadnienia.

Kluczowe praktyki w zakresie C-SCRM. Niniejsza publikacja przedstawia szereg podstawowych, podtrzymujących i usprawniających praktyk i działań związanych z zarządzaniem ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw, które podmioty powinny wdrożyć i przystosować do swoich kontekstów. Podmioty powinny w pierwszej kolejności osiągnąć podstawowy poziom dojrzałości w zakresie tych kluczowych praktyk przed przejściem do wdrażania bardziej zaawansowanych działań w zakresie C-SCRM.

Pomiar wdrożenia możliwości oraz działań w zakresie C-SCRM. Podmioty powinny aktywnie zarządzać efektywnością i skutecznością swoich programów C-SCRM. W tym celu powinny przede wszystkim wdrożyć ramy programu C-SCRM, które będą stanowiły podstawę analizy postępów w realizacji celów związanych z tym obszarem. W drugiej kolejności podmioty powinny opracować oraz wdrożyć ilościowe wskaźniki efektywności oraz określić cele w zakresie tolerancji ryzyka, które pozwolą na ocenę postępów podmiotu przez pryzmat konkretnych celów operacyjnych.

Finansowanie działań w zakresie C-SCRM Jeśli jest to możliwe i stosowne, podmioty powinny dokonać alokacji środków z myślą o realizacji działań związanych z obszarem C-SCRM. Korzyści z takiego rozwiązania obejmują usprawnienie planowania strategicznego i zorientowanego na cele, zwiększanie poczucia odpowiedzialności wewnętrznych interesariuszy za realizację i rozwój praktyk C-SCRM w podmiocie oraz stałe monitorowanie postępów przez kierownictwo podmiotu.

REFERENCJE

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[41]	
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 oceny ryzyka w podmiotach realizujących zadania publiczne – na podstawie NIST SP 800-30
NSC 800-34	Poradnik planowania awaryjnego – na podstawie NIST SP 800-34
NSC 800-37	Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu – na podstawie NIST SP 800-37
NSC 800-39	Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego – na podstawie NIST SP 800-39
NSC 800-53	Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53
NSC 800-53A	Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informacyjnych oraz organizacji. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A
NSC 800-53B	Zabezpieczenia bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B

[41] Narodowe Standardy Cyberbezpieczeństwa

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[41]	
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[42]	
[CISA SCRM WG3]	Cybersecurity and Infrastructure Agency - Working Group 3 (2021) Miti National Institute of Standards and Technology National Institute of Standards and Technology gating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists (Arlington, Virginia). Do pobrania: https://www.cisa.gov/sites/default/files/publications/ICTSCRMTF_Qualified-Bidders- Lists_508.pdf
[COSO 2011]	Rittenberg L, Martens F (2012) Enterprise Risk Management: Understanding and Communicating Risk Appetite. (Committee of Sponsoring Organizations of the Treadway Commission), Thought Leadership in ERM. Do pobrania: https://www.coso.org/Documents/ERM-Understanding-and-Communicating-Risk- Appetite.pdf
[COSO 2020]	Martens F, Rittenberg L (2020) Risk Appetite - Critical to Success: Using Risk Appetite To Thrive in a Changing World. (Committee of Sponsoring Organization of the Treadway Commission), Thought Leadership in ERM. Do pobrania: https://www.coso.org/Documents/COSO-Guidance-Risk-Appetite-Critical-to-Success.pdf
[Defense Industrial Base Assessment: Counterfeit Electronics]	Bureau of Industry and Security, Office of Technology Evaluation (2010) Defense Industrial Base Assessment: Counterfeit Electronics. (U.S. Department of Commerce, Washington, D.C.). Do pobrania: https://www.bis.doc.gov/index.php/documents/technology-evaluation/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010/file

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

Tłumaczenie

PUBLIKACJE ANGLOJĘZYCZNE[42]	
[FEDRAMP]	General Services Administration (2022) FedRAMP. Do pobrania: http://www.fedramp.gov/
[GAO]	Government Accountability Office (2020) Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks. (U.S. Government Accountability Office, Washington D.C.), Report to Congressional Requesters GAO-21171. Do pobrania: https://www.gao.gov/assets/gao-21-171.pdf
[CNSSI 4009]	Committee on National Security Systems (2015) Committee on National Security Systems (CNSS) Glossary (CNSS, Ft. Meade, Md.), CNSSI 4009-2015. Do pobrania: https://www.cnss.gov/CNSS/issuances/Instructions.cfm
[EO 14028]	Executive Order 14028 (2021) Improving the Nation's Cybersecurity. (The White House, Washington, DC), DCPD-202100401, May 12, 2021. https://www.govinfo.gov/app/details/DCPD-202100401
[FASCA]	Federal Acquisition Supply Chain Security Act of 2018 (FASCA), Title II of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE) Technology Act of 2018, Pub. L. 115-390, 132 Stat. 5173. Do pobrania: https://www.congress.gov/115/plaws/publ390/PLAW-115publ390.pdf
[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

PUBLIKACJE ANGLOJĘZYCZNE[42]	
[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
[FSP]	Cyber Risk Institute (2020) *Financial Services Cybersecurity Framework Profile Version 1.0*. Do pobrania: https://cyberriskinstitute.org/the-profile/
[ISO 9000]	International Organization for Standardization (2015) ISO 9000:2015 — Quality management — Fundamentals and vocabulary (ISO, Geneva). Do pobrania: https://www.iso.org/standard/45481.html
[ISO 28001]	International Organization for Standardization (2007) ISO 28001:2007 — Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance (ISO, Geneva). Do pobrania: https://www.iso.org/standard/45654.html.
[ISO GUIDE 73]	International Organization for Standardization (2009) ISO Guide 73:2009 — Risk management — Vocabulary (ISO, Geneva). Do pobrania: https://www.iso.org/standard/44651.html
[ISO/IEC 2382]	International Organization for Standardization/International Electrotechnical Commission (2015) ISO/IEC 2382:2015 — Information technology — Vocabulary (ISO, Geneva). Do pobrania: https://www.iso.org/standard/63598.html

PUBLIKACJE ANGLOJĘZYCZNE[42]	
[ISO/IEC 20243]	International Organization for Standardization/International Electrotechnical Commission (2018) ISO/IEC 20243-1:2018 - Information technology — Open Trusted Technology ProviderTM Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products Part 1: Requirements and recommendations (ISO, Geneva). Do pobrania: https://www.iso.org/standard/74399.html
[ISO/IEC 27000]	International Organization for Standardization/International Electrotechnical Commission (2018) ISO/IEC 27000:2018 - Information technology - Security techniques - Information security management systems - Overview and vocabulary (ISO, Geneva). Do pobrania: https://www.iso.org/standard/73906.html
[ISO/IEC 27002]	International Organization for Standardization/International Electrotechnical Commission (2022) ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection - Information security controls (ISO, Geneva). Do pobrania: https://www.iso.org/standard/75652.html
[ISO/IEC 27036]	International Organization for Standardization/International Electrotechnical Commission (2014) ISO/IEC 27036-2:2014 - Information technology - Security techniques - Information security for supplier relationships - Part 2: Requirements (ISO, Geneva). Do pobrania: https://www.iso.org/standard/59680.html
[ISO/IEC/IEEE 15288]	International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (2015) ISO/IEC/IEEE 15288:2015 — Systems and software engineering — System life cycle processes (ISO, Geneva). Do pobrania: https://www.iso.org/standard/63711.html

Tłumaczenie

PUBLIKACJE ANGLOJĘZYCZNE[42]	
[ITIL SERVICE STRATEGY]	Cannon D (2011) ITIL Service Strategy (The Stationary Office, London), 2nd Ed.
[NDIA]	National Defense Industrial Association System Assurance Committee (2008) Engineeringfor System Assurance. (NDIA, Arlington, VA). Do pobrania: https://www.ndia.org/-/media/sites/ndia/meetings-and-events/divisions/systems-engineering/sse-committee/systems-assurance-guidebook.ashx.
[NIST CSF]	National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018
[NIST SCRM PROCEEDINGS 2012]	National Institute of Standards and Technology (2012) Summary of the Workshop on Information and Communication Technologies Supply Chain Risk Management. Do pobrania: https://tsapps.nist.gov/publication/get pdf.cfm?pub id=913338
[NIST SP 800-16]	deZafra DE, Pitcher SI, Tressler JD, Ippolito JB (1998) Information Technology Security Training Requirements: a Role- and Performance-Based Model. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-16. https://doi.org/10.6028/NIST.SP.800-16
[NIST SP 800-30 REV. 1]	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

PUBLIKACJE ANGLOJĘZYCZNE[42]	
[NIST SP 800-32]	Kuhn DR, Hu VC, Polk WT, 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
[NIST SP 800-34 REV. 1]	Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D (2010) Contingency Planning Guide for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-34, Rev. 1, Includes updates as of November 11, 2010. https://doi.org/10.6028/NIST.SP.800- 34r1
[NIST 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
[NIST 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
[NIST SP 800-53 REV. 5]	Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

PUBLIKACJE ANGLOJĘZYCZNE[42]	
[NIST SP 800-53A REV. 5]	Joint Task Force (2022) Assessing Security and Privacy Controls in Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53Ar5
[NIST SP 800-53B]	Joint Task Force (2020) Control Baselines for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53B, Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53B
[NIST SP 800-55 REV. 1]	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
[NIST SP 800-64]	Kissel R, Stine KM, Scholl MA, Rossman H, Fahlsing J, Gulick, J (2008) Security Considerations in the System Development Life Cycle. (National Institute of Standards and Technology, Gaithersburg, MD), (Withdrawn) NIST Special Publication (SP) 800-64 Rev. 2. https://doi.org/10.6028/NIST.SP.800-64r2
[NIST SP 800-100]	Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007. https://doi.org/10.6028/NIST.SP.800-100

PUBLIKACJE ANGLOJĘZYCZNE[42]	
[NIST 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
[NIST SP 800-160 VOL. 1]	Ross RS, Oren JC, McEvilley M (2016) Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Includes updates as of March 21, 2018. https://doi.org/10.6028/NIST.SP.800-160v1
[NIST SP 800-160 VOL. 2]	Ross RS, Pillitteri VY, Graubart R, Bodeau D, McQuaid R (2021) Developing Cyber Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-160v2r1
[NIST SP 800-171 REV. 2]	Ross RS, Pillitteri VY, Dempsey KL, Riddle M, Guissanie G (2020) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171, Rev. 2, Includes updates as of January 28, 2021. https://doi.org/10.6028/NIST.SP.800-171r2
[NIST SP 800-172]	Ross RS, Pillitteri VY, Guissanie G, Wagner R, Graubart R, Bodeau D (2021) Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-172. https://doi.org/10.6028/NIST.SP.800-172

PUBLIKACJE ANGLOJĘZYCZNE[42]	
[NIST SP 800-181 REV. 1]	Petersen R, Santos D, Wetzel KA, Smith MC, Witte GA (2017) Workforce Framework for Cybersecurity (NICE Framework). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181, Rev. 1. https://doi.org/10.6028/NIST.SP.800-181r1
[NIST SSDF]	National Institute of Standards and Technology (2022) NIST Secure Software Development Framework. Do pobrania: https://csrc.nist.gov/projects/ssdf
[NISTIR 7622]	Boyens JM, Paulsen C, Bartol N, Shankles S, Moorthy R (2012) Notional Supply Chain Risk Management Practices for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7622. https://doi.org/10.6028/NIST.IR.7622
[NISTIR 8179]	Paulsen C, Boyens JM, Bartol N, Winkler K (2018) Criticality Analysis Process Model: Prioritizing Systems and Components. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8179. https://doi.org/10.6028/NIST.IR.8179
[NISTIR 8276]	Boyens J, Paulsen C, Bartol N, Winkler K, Gimbi J (2021) Key Practices in Cyber Supply Chain Risk Management: Observations from Industry. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8276. https://doi.org/10.6028/NIST.IR.8276
[NISTIR 8286]	Stine KM, Quinn SD, Witte GA, Gardner RK (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8286. https://doi.org/10.6028/NIST.IR.8286

PUBLIKACJE ANGLOJĘZYCZNE[42]	
[NTIA SBOM]	The Minimum Elements For a Software Bill of Materials (SBOM), NTIA and Department of Commerce, 2021 https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf
[OMB A-123]	Office of Management and Budget (2004) Management's Responsibility for Internal Control. (The White House, Washington, DC), OMB Circular A-123, December 21, 2004. Do pobrania: https://georgewbush-whitehouse.archives.gov/omb/circulars/a123/a123_rev.html
[OMB A-130]	Office of Management and Budget (2016) anaging Information as a Strategic Resource. (The White House, Washington, DC), OMB Circular A-130, July 28, 2016. Do pobrania: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a 130revised.pdf
[SAFECODE 1]	Software Assurance Forum for Excellence in Code (2010) Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain. Do pobrania: http://www.safecode.org/publications/SAFECode_Software_Integrity_Controls0610.pdf
[SAFECODE 2]	Software Assurance Forum for Excellence in Code (2009) The Software Supply Chain Integrity Framework: Defining Risks and Responsibilities for Securing Software in the Global Supply Chain. http://www.safecode.org/publication/SAFECode Supply Chain0709.pdf
[SWA]	Polydys ML, Wisseman S (2008) Software Assurance in Acquisition: Mitigating Risks to the Enterprise. A Reference Guide for Security-Enhanced Software Acquisition and Outsourcing. (National Defense University Press, Washington, D.C.) Information Resources Management College Occasional Paper. Do pobrania: https://apps.dtic.mil/dtic/tr/fulltext/u2/a495389.pdf

Tłumaczenie

ZAŁĄCZNIK A ŚRODKI BEZPIECZEŃSTWA ZWIĄZANE Z OBSZAREM C-SCRM[43]

WPROWADZENIE DO ŚRODKÓW BEZPIECZEŃSTWA ZWIĄZANYCH Z OBSZAREM C-SCRM

Narodowy Instytut Standaryzacji i Technologii definiuje środki bezpieczeństwa jako:

> *Metody zarządzania, zabezpieczenia operacyjne i techniczne (środki bezpieczeństwa lub środki przeciwdziałania) przewidziane dla systemu informacyjnego w celu ochrony poufności, integralności i dostępności systemu i przechowywanych danych* [FIPS 199][44].

Dokument [NSC 800-53] w ramach katalogu zabezpieczeń informacji określa liczne środki bezpieczeństwa związane z cyberbezpieczeństwem łańcucha dostaw. Niniejszy rozdział ma strukturę rozszerzonego uzupełnienia dokumentu [NSC 800-53]. Określa i uzupełnia środki bezpieczeństwa związane z zagadnieniem C-SCRM o dodatkowe wytyczne rozszerzające oraz w stosownych przypadkach opisuje nowe środki bezpieczeństwa. Środki bezpieczeństwa dotyczące obszaru C-SCRM są podzielone na 20 rodzin zabezpieczeń opisanych w dokumencie [NSC 800-53]. Takie podejście ułatwia wykorzystanie technik oceny środków bezpieczeństwa przedstawionych w dokumencie [NSC SP 800-53A] do oceny wdrożenia zabezpieczeń C-SCRM.

Środki bezpieczeństwa przedstawione w niniejszej publikacji są przeznaczone do wdrożenia wewnętrznego przez podmioty oraz wykorzystania do opracowania wymagań dotyczących wykonawców i podwykonawców, jeśli mają zastosowanie i są określone w umowie. Podobnie jak w przypadku dokumentu [NSC 800-53], środki bezpieczeństwa i zabezpieczenia rozszerzone stanowią punkt wyjścia, który pozwala na dodawanie, usuwanie lub dalsze dostosowywanie zabezpieczeń w zależności od potrzeb podmiotu. Każdy środek bezpieczeństwa uwzględniony w niniejszym rozdziale został opisany pod kątem możliwości jego zastosowania w obszarze C SCRM. Środki bezpieczeństwa zawarte w dokumencie [NSC 800-53], które nie zostały wymienione, nie zostały uznane za możliwe do uwzględnienia w związku

[43] Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

[44] Wersja polskojęzyczna: NSC 199.

z obszarem C-SCRM, a zatem nie zostały zawarte w niniejszej publikacji. Szczegóły i dodatkowe wskazówki dotyczące różnych środków bezpieczeństwa dotyczących obszaru C-SCRM w niniejszej publikacji znajdują się w Załączniku A.

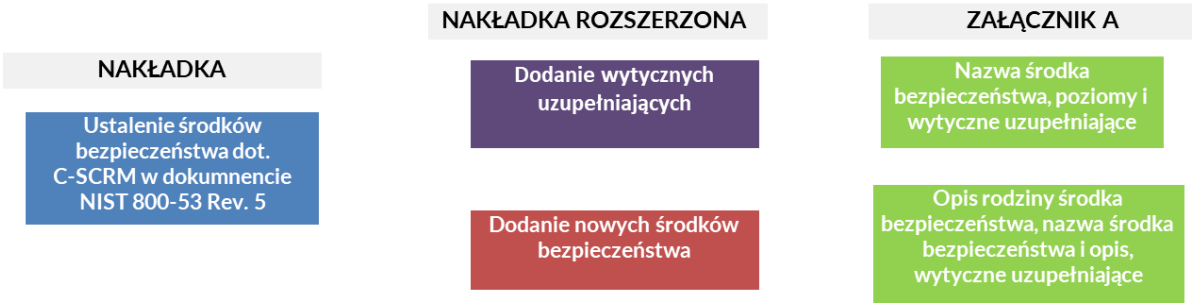
PODSUMOWANIE ŚRODKÓW BEZPIECZEŃSTWA ZWIĄZANYCH Z OBSZAREM C-SCRM

W ramach etapu reagowania procesu zarządzania ryzykiem opisanym w rozdziale 2, podmioty wybierają, dostosowują i wdrażają mechanizmy zabezpieczeń w celu ograniczenia ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw. Dokument [NSC 800-53B] wymienia zestaw środków bezpieczeństwa informacji o wysokim, umiarkowanym i niskim potencjalnym poziomie wpływu na organizację kategoryzowanych według [NSC 199]. W tym rozdziale opisano, w jaki sposób rzeczone środki bezpieczeństwa pomagają ograniczyć ryzyko odnoszące się do systemów informacyjnych i ich komponentów, a także infrastruktury łańcucha dostaw. Rozdział zawiera 20 kategorii (rodzin) zabezpieczeń w zakresie C-SCRM, które obejmują odpowiednie środki bezpieczeństwa i wytyczne uzupełniające.

Rysunek A-1 przedstawia proces zastosowany w celu określenia, dopracowania i dodania wytycznych uzupełniających C-SCRM do zabezpieczeń związanych z obszarem C-SCRM opisanych w dokumencie [NSC 800-53] i przedstawia następujące kroki:

1. Wybór i wyodrębnienie poszczególnych środków bezpieczeństwa i rozszerzeń tych zabezpieczeń z dokumentu [NSC 800-53] mających zastosowanie do obszaru C-SCRM.
2. Analizę wybranych środków bezpieczeństwa, aby określić, w jaki sposób mają one zastosowanie do obszaru C-SCRM.
3. Ocenę wyodrębnionego zestawu zabezpieczeń oraz zabezpieczeń rozszerzonych w celu ustalenia, czy uwzględniają one wszelkie zagadnienia związane z obszarem C-SCRM.
4. Opracowanie dodatkowych środków bezpieczeństwa, które nie zostały określone w treści dokumentu [NSC 800-53].
5. Określenie zabezpieczeń, które powinny zostać wykorzystane przez odpowiednich wykonawców niższego szczebla.

6. Przypisanie odpowiednich poziomów kategoryzacji do poszczególnych zabezpieczeń C-SCRM.
7. Opracowanie wytycznych uzupełniających dla poszczególnych zabezpieczeń C-SCRM.



Rysunek Błąd! W dokumencie nie ma tekstu o podanym stylu.**-1: Środki bezpieczeństwa związane z C-SCRM według NSC 800-161.**

Należy zauważyć, że dokument [NSC 800-53] przedstawia szereg środków bezpieczeństwa i rodzin zabezpieczeń związanych z C-SCRM. Rzeczone środki bezpieczeństwa mogą zostać omówione w niniejszej publikacji wraz z podsumowaniem lub dodatkowymi wytycznymi oraz odniesieniem do oryginalnej treści dokumentu [NSC 800-53] dotyczącej zabezpieczeń i szczegółowych wytycznych uzupełniających.

ŚRODKI BEZPIECZEŃSTWA ZWIĄZANE Z C-SCRM W CAŁYM PODMIOCIE

Jak pokazuje tabela A-1, środki bezpieczeństwa związane z C-SCRM zawarte w niniejszej publikacji opierają się na trzech poziomach zarządzania ryzykiem w podmiocie. Ma to na celu ułatwienie wyboru zabezpieczeń związanych z C-SCRM odpowiednich dla danego podmiotu, realizowanej misji oraz wykorzystywanych przezeń systemów, zgodnie z informacjami zawartymi Załączniku C na temat etapu reagowania procesu zarządzania ryzykiem. Podczas wyboru zabezpieczeń podmioty powinny wykorzystać listę środków bezpieczeństwa uwzględnionych w niniejszym rozdziale, aby określić odpowiednie środki bezpieczeństwa związane z obszarem C-SCRM na podstawie własnej oceny ryzyka. Poprzez wybór i wdrożenie odpowiednich zabezpieczeń C-SCRM dla każdego poziomu, podmioty zapewniają skuteczne wdrożenie rozwiązań w zakresie C-SCRM w swoich strukturach.

ZASTOSOWANIE ŚRODKÓW BEZPIECZEŃSTWA ZWIĄZANE Z OBSZAREM C-SCRM DO PROCESÓW ZAMÓWIEŃ PRODUKTÓW I USŁUG

Podmioty nabywające mogą wykorzystywać środki bezpieczeństwa związane z obszarem C-SCRM jako punkt wyjścia i podstawę wymogów w tym obszarze przekazywanych różnym podmiotom dostarczającym produkty i usługi, w tym dostawcom, deweloperom, integratorom systemów, dostawcom zewnętrznych usług systemowych oraz innym dostawcom usług związanych z ICT/OT. Podmioty nabywające powinny unikać stosowania uogólnionych stwierdzeń dotyczących wymagań, takich jak „zapewnienie zgodności z wymogami w zakresie środków bezpieczeństwa zgodnie z dokumentem NSC 800-161, Rev. 1". Zadaniem podmiotów nabywających jest dobór środków bezpieczeństwa odpowiednich dla konkretnego przypadku użycia nabywanej usługi lub produktu. Podmioty nabywające powinny włączać zagadnienie C-SCRM do wszystkich działań związanych z zamówieniami i zaopatrzeniem. Więcej szczegółów na temat roli C-SCRM w procesach zamówień i zaopatrzenia znajduje się w rozdziale 3.1 niniejszego dokumentu.

Ważne jest, aby zdawać sobie sprawę, że środki bezpieczeństwa opisane w niniejszym rozdziale nie są przeznaczone do bezpośredniego uwzględnienia w treści zawieranych umów i kontraktów. Podmioty nabywające powinny wykorzystać niniejszą publikację jako zbiór wskazówek pozwalających na opracowanie własnych umów zawierających konkretne wymagania dotyczące C-SCRM. W kolejnych rozdziałach omówiono role dostawcy, dewelopera, integratora systemów, dostawcy zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT w odniesieniu do oczekiwań podmiotów nabywających w zakresie C-SCRM.

Aby upewnić się, czy stosowne środki bezpieczeństwa zostały wdrożone, podmioty mogą korzystać z wielu technik, takich jak: samoocena dostawcy, ocena przez podmiot nabywający lub audyt przeprowadzony przez podmiot zewnętrzny pod kątem zgodności z wymogami podmiotu. Podmioty powinny najpierw przeanalizować dostępne oceny podmiotów zewnętrznych, aby sprawdzić, czy spełniają one ich potrzeby. Kiedy podmiot określa swoje wymagania w zakresie C-SCRM, może odkryć, że dostępne oceny przeprowadzone przez podmioty zewnętrzne mogą nie

uwzględniać wszystkich specyficznych wymagań. W takim przypadku mogą być potrzebne dodatkowe informacje dotyczące nieuwzględnionych wymagań. Należy pamiętać, że uzyskane w tym celu dane powinny być odpowiednio zabezpieczone.

DOSTAWCY

Dostawcy mogą dostarczać nabywcy rozwiązania komercyjne, a w kontekście rządowym także rozwiązania rządowe. Rozwiązania komercyjne obejmują elementy nierozwijane przez dostawców, takie jak rozwiązania/produkty licencjonowane na zasadach komercyjnych. Rozwiązania rządowe są rozwiązaniami licencjonowanymi wyłącznie przez rządy. Dostawcy stanowią zróżnicowaną grupę, która obejmuje zarówno bardzo małe jak i duże podmioty, które mogą być wyspecjalizowane lub zróżnicowane, a także mogą posiadać siedziby w jednym lub wielu krajach. Dostawcy różnią się również znacząco pod względem poziomu zaawansowania, zasobów oraz przejrzystości i widoczności swoich procesów i rozwiązań.

Dostawcy stosują różne poziomy i rodzaje praktyk w obszarze C-SCRM. Praktyki te oraz powiązane z nimi działania mogą stanowić podstawę oceny zarządzania ryzykiem w łańcuchu dostaw. W stosownych przypadkach należy umożliwić dostawcom ponowne wykorzystanie wszelkich istniejących danych i dokumentów, które mogą potwierdzić wdrożenie praktyk i rozwiązań w zakresie C-SCRM.

Podmioty powinny rozważyć, czy na koszt współpracy z dostawcami może mieć bezpośredni wpływ zakres wymogów dotyczących cyberbezpieczeństwa łańcucha dostaw nałożonych na dostawców, a także chęć lub zdolność dostawców do umożliwienia wglądu w sposób opracowywania lub wytwarzania ich produktów oraz sposób stosowania przez nich praktyk w zakresie bezpieczeństwa i łańcucha dostaw w odniesieniu do ich rozwiązań. Gdy podmioty lub integratorzy systemów wymagają od dostawców większej przejrzystości, muszą rozważyć ewentualne koszty takich wymagań. Dostawcy mogą zdecydować się na nieuczestniczenie w procesach zamówień, aby uniknąć zwiększonych kosztów lub zagrożenia dla ich własności intelektualnej, ograniczając tym samym możliwości wyboru dostaw lub technologii przez podmiot. Ponadto dostawcy mogą być narażeni na ryzyko związane

z nakładaniem przez klientów wielu różnych zestawów wymogów dotyczących cyberbezpieczeństwa łańcucha dostaw, które dostawca musi spełnić w zależności od klienta. Zakres przejrzystości wymaganej od dostawców powinien być współmierny do krytyczności dostawców, która jest wystarczająca do uwzględnienia ryzyka.

DEWELOPERZY I PRODUCENCI

Deweloperzy i producenci to podmioty, które opracowują lub wytwarzają systemy, komponenty systemu (np. oprogramowanie) lub usługi systemowe (np. Interfejsy API]). Ich opracowywanie może odbywać się wewnętrznie w podmiotach lub za pośrednictwem podwykonawców zewnętrznych. Deweloperzy zazwyczaj posiadają uprzywilejowane prawa dostępu i odgrywają istotną rolę w całym cyklu życia systemu. Czynności, które wykonują i rezultaty ich pracy mogą wzmocnić bezpieczeństwo lub wprowadzić nowe podatności. Dlatego też istotne jest, aby deweloperzy podlegali wymogom i środkom bezpieczeństwa w zakresie C-SCRM oraz byli z nimi dobrze zaznajomieni.

INTEGRATORZY SYSTEMÓW

Integratorzy systemów świadczą na rzecz podmiotów nabywających usługi dostosowane do jego potrzeb, w tym opracowywanie rozwiązań na zamówienie, testowanie, obsługę i konserwację. Podmioty należące do tej grupy zwykle odpowiadają na zapytania ofertowe od podmiotów nabywających, oferując rozwiązanie lub usługę dostosowaną do wymagań. Takie propozycje dostarczane przez integratorów systemów mogą obejmować produkty wielu dostawców oraz współpracę z innymi dostawcami lub podwykonawcami. Integrator systemu powinien zapewnić, że te podmioty są sprawdzone i zweryfikowane pod kątem wymogów C-SCRM podmiotu nabywającego. Ze względu na poziom widoczności, jaki można uzyskać w relacjach z integratorem systemu, podmiot nabywający może według własnego uznania wymagać rygorystycznych kryteriów akceptacji dostawcy oraz wszelkich odpowiednich środków przeciwdziałania w celu wyeliminowania zidentyfikowanego lub potencjalnego ryzyka.

DOSTAWCY ZEWNĘTRZNYCH USŁUG SYSTEMOWYCH LUB SYSTEMÓW INFORMACYJNYCH

Podmioty wykorzystują dostawców zewnętrznych usług do realizacji lub wspierania niektórych swoich misji i funkcji biznesowych [NSC 800-53]. Outsourcing systemów i usług powoduje powstanie szeregu problemów w zakresie cyberbezpieczeństwa związanych z łańcuchem dostaw, które ograniczają widoczność i kontrolę podmiotu nabywającego nad działaniami zleconymi na zewnątrz. Dlatego wymaga to od podmiotów zwiększonego rygoru w zakresie definiowania wymogów C-SCRM, określania ich w umowach zamówień, monitorowania dostarczanych usług oraz ich oceny pod kątem zgodności z określonymi wymogami. Niezależnie od tego, kto świadczy usługi, podmiot nabywający ponosi ostateczną odpowiedzialność za ryzyko dla systemów i danych podmiotu, które wynika z korzystania z tych usług. Podmioty powinny wdrożyć zestaw środków bezpieczeństwa w zakresie C-SCRM w celu ograniczenia tego ryzyka i współpracować z osobami odpowiedzialnymi za realizację misji oraz procesy biznesowe lub osobę odpowiedzialną za zarządzanie ryzykiem w celu akceptacji tego ryzyka. Do przekazywania informacji, a następnie weryfikacji i monitorowania wymagań dotyczących C-SCRM można wykorzystać różne metody, takie jak kontrakty, umowy międzyorganizacyjne, uzgodnienia dotyczące linii biznesowych, umowy licencyjne lub transakcje w ramach łańcucha dostaw.

INNI DOSTAWCY USŁUG ZWIĄZANYCH Z ICT/OT

Dostawcy usług mogą pełnić wiele różnych funkcji, począwszy od doradztwa, poprzez publikowanie treści stron internetowych, aż po usługi konserwacji i utrzymania. Kategoria innych dostawców usług związanych z ICT/OT obejmuje tych usługodawców, którzy wymagają fizycznego lub logicznego dostępu do systemów ICT/OT lub wykorzystania technologii (np. fotograf wykorzystujący drona do wykonywania zdjęć/filmów lub firma ochroniarska zdalnie monitorująca obiekt za pomocą systemu monitoringu wideo w chmurze) w ramach świadczenia swoich usług. W wyniku dostępu lub korzystania z usług dostawcy wzrasta potencjał wystąpienia ryzyka związanego z cyberbezpieczeństwem w łańcuchu dostaw podmiotu.

Technologie operacyjne posiadają unikalne charakterystyki operacyjne i bezpieczeństwa, które wymagają zastosowania specjalistycznych umiejętności i zdolności w celu ich skutecznej

ochrony. Podmioty, które posiadają szeroki zakres komponentów OT w swojej architekturze, często zwracają się do wyspecjalizowanych usługodawców w celu bezpiecznego wdrożenia i utrzymania tych urządzeń, systemów lub sprzętu. Każdy podmiot lub osoba fizyczna świadczący usługi, które mogą obejmować autoryzowany dostęp do systemu ICT lub OT, powinni stosować się do wymagań C-SCRM podmiotu nabywającego. Podmioty powinny zwracać szczególną uwagę na dostawców usług związanych z ICT/OT, którzy zarządzają zasobami o kluczowym znaczeniu dla podmiotu lub związanymi z bezpieczeństwem.

WYBÓR, DOSTOSOWANIE I WDROŻENIE ŚRODKÓW BEZPIECZEŃSTWA ZWIĄZANYCH Z OBSZAREM C-SCRM

Środki bezpieczeństwa związane z obszarem C-SCRM zdefiniowane w niniejszym rozdziale powinny zostać dobrane i dostosowane do indywidualnych potrzeb i środowisk podmiotu z wykorzystaniem wytycznych zawartych w dokumencie [NSC 800-53] w celu zapewnienia efektywnego kosztowo, opartego na ryzyku podejścia do wdrożenia programu C-SCRM w całym podmiocie. Określony w niniejszej publikacji poziom podstawowy C-SCRM odpowiada na podstawowe potrzeby szerokiego i zróżnicowanego zbioru podmiotów. Podmioty muszą wybrać, dopasować i wdrożyć środki bezpieczeństwa w oparciu o: (I) środowiska, w których systemy informacyjne podmiotów są nabywane i działają; (II) charakter operacji prowadzonych przez podmioty; (III) rodzaje zagrożeń, na które narażone są podmioty, realizowane przez nie misje oraz procesy biznesowe, łańcuchy dostaw i systemy informacyjne; oraz (IV) rodzaje informacji przetwarzanych, przechowywanych lub przesyłanych przez systemy informacyjne i infrastrukturę łańcucha dostaw.

Po wybraniu wstępnego zestawu środków bezpieczeństwa, podmiot nabywający powinien rozpocząć proces dostosowywania wymogów zgodnie z dokumentem NSC 800-53B, aby odpowiednio zmodyfikować i lepiej dostosować wybrane środki bezpieczeństwa do konkretnych warunków dotyczących danego podmiotu. Przed wdrożeniem środków bezpieczeństwa związanych z obszarem C-SCRM należy przeprowadzić proces dostosowania, który powinien być skoordynowany z odpowiednim personelem wyższego szczebla podmiotu, na przykład z osobami autoryzującymi, pełnomocnikami takich osób, personelem odpowiedzialnym za ryzyko, CIO lub SISO. Ponadto podmioty mogą elastycznie dostosowywać wymogi na szczeblu całego

podmiotu (w celu opracowania podstawowego poziomu lub punktu wyjścia na potrzeby dostosowania polityk, programów lub systemów) na potrzeby wsparcia określonych programów lub poszczególnych systemów informacyjnych lub stosując kombinację podejść na poziomie podmiotu, programu/misji i systemów.

Decyzje dotyczące wyboru i dostosowania, w tym konkretne uzasadnienie tych decyzji, powinny być zawarte w dokumentacji C-SCRM na poziomach 1, 2 i 3 oraz w Załączniku C i zatwierdzone przez odpowiednich kierowników i dyrektorów podmiotu w ramach procesu zatwierdzania planu działań w zakresie C-SCRM.

FORMAT ŚRODKÓW BEZPIECZEŃSTWA ZWIĄZANYCH Z OBSZAREM C-SCRM

W tabeli A-1 przedstawiono format stosowany w niniejszej publikacji dla środków bezpieczeństwa, a także dodatkowych wytycznych związanych z obszarem C-SCRM dotyczących wybranych środków uwzględnionych w dokumencie [NSC 800-53] lub zabezpieczeń rozszerzonych.

Środki bezpieczeństwa związane z obszarem C-SCRM, które nie opierają się na dokumencie [NSC 800-53], są w większości przypadków zgodne z formatem ogólnym opisanym w dokumencie [NSC SP 800-53] z dodaniem odpowiednich poziomów. Nowe środki bezpieczeństwa otrzymują identyfikatory zgodne z dokumentem [NSC 800-53], jednak nie powielają istniejących identyfikatorów zabezpieczeń.

Tabela A-1: Format środków bezpieczeństwa związanych z obszarem C-SCRM

IDENTYFIKATOR ŚRODKA BEZPIECZEŃSTWA	NAZWA ŚRODKA BEZPIECZEŃSTWA
	Dodatkowe wytyczne dotyczące obszaru C-SCRM: Poziom(y): Powiązane środki bezpieczeństwa: Zabezpieczenia rozszerzone:
(1)	*NAZWA ŚRODKA BEZPIECZEŃSTWA | NAZWA ZABEZPIECZENIA ROZSZERZONEGO* Dodatkowe wytyczne dotyczące obszaru C-SCRM: Poziom(y): Powiązane środki bezpieczeństwa:

Poniżej przedstawiono przykład formatu środka bezpieczeństwa związanego z obszarem C-SCRM na przykładzie środka bezpieczeństwa SCRM AC-3 oraz zabezpieczenia rozszerzonego SCRM AC-3(8):

AC-3 EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Zapewnienie, że systemy informacyjne i łańcuch dostaw są wyposażone w stosowne mechanizmy egzekwowania dostępu. Obejmuje to zarówno fizyczne, jak i logiczne mechanizmy egzekwowania dostępu, skoordynowane z myślą o potrzebach łańcucha dostaw. Podmioty powinny opracować szczegółową definicję egzekwowania dostępu.

Poziom(y): 2, 3

Powiązane środki bezpieczeństwa: AC-4

Zabezpieczenia rozszerzone:

(8) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | WYCOFANIE UPRAWNIEŃ DOSTĘPU

1. Dodatkowe wytyczne dotyczące obszaru C-SCRM: Szybkie wycofanie uprawnień ma kluczowe znaczenie dla zapewnienia, że dostawcy,

deweloperzy, integratorzy systemów, dostawcy zewnętrznych usług systemowych i inni dostawcy usług związanych z ICT/OT, którzy nie potrzebują już dostępu lub którzy nadużywają swoich przywilejów dostępu, tracą możliwość dostępu do systemu podmiotu. Przykładem takiej sytuacji może być przeniesienie umowy pomiędzy dwoma integratorami systemów, choć obsługą umowy nadal zajmują się ci sami pracownicy. W takiej sytuacji podmiot powinien wyłączyć istniejące konta, wycofać stare dane uwierzytelniające, założyć nowe konta i wydać nowe dane uwierzytelniające.

Poziom(y): 2, 3

STOSOWANIE ZABEZPIECZEŃ DOTYCZĄCYCH C-SCRM ZAWARTYCH W NINIEJSZEJ PUBLIKACJI

Pozostała część Załącznika A stanowi uzupełnienie dokumentu NSC 800-53 dotyczące zagadnień związanych z obszarem C-SCRM. Znajdują się w nim informacje na temat związku między środkami bezpieczeństwa zawartymi w dokumencie NSC 800-53 i środkami bezpieczeństwa dotyczącymi obszaru C-SCRM przedstawione w jeden z następujących sposobów:

- Jeśli dany środek bezpieczeństwa lub dane zabezpieczenie rozszerzone określone w dokumencie [NSC 800-53] zostały uznane jako środki bezpieczeństwa informacji, które mogą stanowić fundamentalne zabezpieczenie związane z obszarem C-SCRM, jednak nie odnoszą się wyłącznie do tego obszaru, nie zostały one uwzględnione w niniejszej publikacji.
- Jeśli dany środek bezpieczeństwa lub dane zabezpieczenie rozszerzone określone w dokumencie [NSC 800-53] zostały uznane za istotne z punktu widzenia obszaru C-SCRM, zostały wskazane poziomy, do których mają zastosowanie.
- Jeśli zabezpieczenie rozszerzone opisane w dokumencie [NSC 800-53] zostało uznane za istotne z punktu widzenia obszaru C-SCRM, jednak nadrzędny środek bezpieczeństwa nie został za taki uznany, wówczas numer i nazwa zabezpieczenia zostały uwzględnione, jednak nie zostały opracowane dodatkowe wytyczne dotyczące obszaru C-SCRM.

- Środki bezpieczeństwa oraz zabezpieczenia rozszerzone dotyczące obszaru C-SCRM, które nie mają powiązanego środka bezpieczeństwa lub zabezpieczenia rozszerzonego w dokumencie [NSC 800-53] są wymienione wraz z nazwami oraz pełnym opisem.
- Wszystkie środki bezpieczeństwa związane z obszarem C-SCRM obejmują poziomy, dla których dany środek ma zastosowanie oraz dodatkowe wytyczne C-SCRM, jeśli są wymagane.
- Jeżeli zabezpieczenie rozszerzone obejmuje mechanizm wdrożenia środka bezpieczeństwa związanego z obszarem C-SCRM, takie zabezpieczenie rozszerzone jest wymienione w ramach dodatkowych wytycznych dotyczących obszaru C-SCRM i nie jest opisywane oddzielnie.
- Jeśli dokument [NSC 800-53] uwzględnia wycofanie lub reorganizację istniejących środków bezpieczeństwa wynikających z dokumentu [NSC 800-161], nie zostały one uwzględnione w niniejszym dokumencie.

Dodano następujące nowe zabezpieczenia oraz zabezpieczenia rozszerzone:

- Do rodziny zabezpieczeń C-SCRM dotyczącej utrzymania dodano środek bezpieczeństwa MA-8 – Monitorowanie utrzymania i wymiana informacji
- Środek bezpieczeństwa związany z obszarem C-SCRM, SR-13 – Wykaz dostawców, został dodany do rodziny środków bezpieczeństwa w kategorii: Zarządzanie ryzykiem w łańcuchu dostaw.

ŚRODKI BEZPIECZEŃSTWA ZWIĄZANE Z OBSZAREM C-SCRM

KATEGORIA AC: KONTROLA DOSTĘPU

Dokument [NSC 200] określa minimalne wymagania bezpieczeństwa w zakresie kontroli dostępu w następujący sposób:

> *Organizacje powinny ograniczyć dostęp do systemu informacyjnego do autoryzowanych użytkowników, procesów działających w imieniu autoryzowanych użytkowników lub urządzeń (w tym innych systemów informacyjnych) oraz do typów transakcji i funkcji, które upoważnieni użytkownicy mogą wykonywać.*

Do systemów i komponentów, które przemieszczają się w łańcuchu dostaw, dostęp mają różne osoby i podmioty, w tym dostawcy, deweloperzy, integratorzy systemów, dostawcy zewnętrznych usług systemowych oraz inni dostawcy usług związanych z ICT/OT. Zasady takiego dostępu powinny być określone i zarządzane w taki sposób, by zapewnić, że nie spowoduje on niezamierzonego ujawnienia, modyfikacji lub zniszczenia informacji. Dostęp ten powinien być ograniczony wyłącznie do niezbędnego rodzaju, czasu trwania i poziomu dostępu dla upoważnionych podmiotów (i upoważnionych osób w ramach tych podmiotów) oraz monitorowany pod kątem wpływu na łańcuch dostaw w zakresie cyberbezpieczeństwa.

AC-1 POLITYKA I PROCEDURY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny określić i zawrzeć w umowach w zasady i polityki dotyczące kontroli dostępu dotyczące dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT, którzy posiadają polityki kontroli dostępu. Powinny one obejmować zarówno fizyczny, jak i logiczny dostęp do łańcucha dostaw i systemu informacyjnego. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom.

Poziom(y): 1, 2, 3

AC-2 ZARZĄDZANIE KONTAMI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Stosowanie tego środka bezpieczeństwa pomaga w zapewnieniu identyfikowalności działań i podmiotów w łańcuchu dostaw. Ten środek bezpieczeństwa pomaga również na bieżąco zapewniać, że uprawnienia dostępu uczestników łańcucha dostaw są zawsze na odpowiednim poziomie. Podmiot może zdecydować się na określenie zestawu ról i powiązanie poziomu uprawnień w celu zapewnienia właściwego wdrożenia tego zabezpieczenia. Podmioty muszą zapewnić, że konta dla pracowników wykonawcy nie będą aktywne po zakończeniu obowiązywania umowy. Konta uprzywilejowane powinny być tworzone wyłącznie dla zweryfikowanych pracowników wykonawcy. Podmioty powinny również wdrożyć procesy dotyczące zakładania oraz zarządzania kontami tymczasowymi lub awaryjnymi dla pracowników wykonawców, którzy wymagają dostępu do systemu o znaczeniu krytycznym lub umożliwiającego realizację misji podczas zdarzenia związanego z ciągłością działalności lub sytuacją awaryjną. Na przykład podczas pandemii może zaistnieć potrzeba tymczasowego zastąpienia pracowników wykonawcy, którzy nie są w stanie pracować z powodu choroby. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

AC-3 EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Zapewnienie, że systemy informacyjne i łańcuch dostaw są wyposażone w stosowne mechanizmy egzekwowania dostępu. Obejmuje to zarówno fizyczne, jak i logiczne mechanizmy egzekwowania dostępu, skoordynowane z myślą o potrzebach łańcucha dostaw. Podmioty powinny upewnić się, że zostały określone

konsekwencje dotyczące przypadków naruszeń zabezpieczeń kontroli dostępu. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

Zabezpieczenie rozszerzone:

1. *EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | WYCOFANIE UPRAWNIEŃ DOSTĘPU*

   Dodatkowe wytyczne dotyczące obszaru C-SCRM: Szybkie wycofanie uprawnień ma kluczowe znaczenie dla zapewnienia, że dostawcy, deweloperzy, integratorzy systemów, dostawcy zewnętrznych usług systemowych i inni dostawcy usług związanych z ICT/OT, którzy nie potrzebują już dostępu lub którzy nadużywają swoich przywilejów dostępu, tracą możliwość dostępu do systemu podmiotu. Podmioty powinny zawrzeć w swoich umowach wymóg, aby wykonawcy i podwykonawcy niezwłocznie zwracali podmiotowi dane uwierzytelniające (np. tokeny, karty PIV lub CAC itp.) Podmioty muszą również wdrożyć procesy umożliwiające szybkie wykonanie cofnięcia uprawnień dostępu. Przykładem takiej sytuacji może być przeniesienie umowy pomiędzy dwoma integratorami systemów, choć obsługą umowy nadal zajmują się ci sami pracownicy. W takiej sytuacji podmiot powinien wyłączyć istniejące konta, wycofać stare dane uwierzytelniające, założyć nowe konta i wydać nowe dane uwierzytelniające.

   Poziom(y): 2, 3

2. *EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | KONTROLOWANE UDOSTĘPNIANIE INFORMACJI*

   Dodatkowe wytyczne dotyczące obszaru C-SCRM: Udostępnianie informacji dotyczących łańcucha dostaw powinno być weryfikowane

przed ich udostępnieniem podmiotom zewnętrznym. Podmioty mogą wymieniać informacje ze swoimi dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych oraz innymi dostawcami usług związanych z ICT/OT. Kontrolowane udostępnianie informacji przez podmiot chroni przed ryzykiem związanym z ich ujawnieniem.

Poziom(y): 2, 3

AC-4 EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Informacje dotyczące łańcucha dostaw mogą być przekazywane w ramach szeroko pojętego łańcucha dostaw wielu interesariuszom, których lista obejmuje podmiot oraz interesariuszy organizacji publicznych, dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT. Określenie wymogów i sposobu kontroli przepływu informacji powinno zapewnić, że tylko wymagane informacje są przekazywane różnym uczestnikom łańcucha dostaw. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

Zabezpieczenie rozszerzone:

1. *EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | METADANE*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Metadane istotne z punktu widzenia obszaru C-SCRM są obszerne i obejmują działania w ramach cyklu życia systemu, na przykład informacje o systemach i komponentach systemów, a także szczegóły dotyczące zamówień i dostaw są uznawane za metadane i mogą wymagać odpowiedniej ochrony. Podmioty powinny określić, jakie metadane są bezpośrednio istotne dla bezpieczeństwa ich łańcucha

dostaw i wdrożyć środki kontroli przepływu informacji w celu ochrony stosownych metadanych.

Poziom(y): 2, 3

2. *EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | UWIERZYTELNIANIE DOMENY*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: W kontekście C-SCRM podmioty powinny określić różne punkty wyjściowe i docelowe dla informacji dotyczących łańcucha dostaw oraz informacji, które przez niego przepływają. Dzięki temu podmioty mogą zapewnić widoczność przepływu informacji w łańcuchu dostaw.

Poziom(y): 2, 3

3. *EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | WALIDACJA METADANYCH*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Z punktu widzenia obszaru C-SCRM kluczowe znaczenie ma walidacja danych i ich powiązania z metadanymi. Duża część danych przekazywanych w łańcuchu dostaw jest walidowana poprzez weryfikację powiązanych z nimi metadanych. Podmiot powinien zapewnić odpowiednie filtrowane oraz kontrolę w celu walidacji danych przed wprowadzeniem danych do łańcucha dostaw.

Poziom(y): 2, 3

4. *EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | FIZYCZNE LUB LOGICZNE ODDZIELENIE PRZEPŁYWÓW INFORMACJI*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien zapewnić oddzielenie przepływów informacji dotyczących systemu informacyjnego i łańcucha dostaw[45]. Podmioty mogą wdrożyć różne

[45] Informacje o ryzyku związanym z cyberbezpieczeństwem w całym łańcuchu dostaw są określone w glosariuszu dołączonym do niniejszego dokumentu.

mechanizmy, takie jak szyfrowanie lub podpisy cyfrowe. Podmioty mogą stawiać czoła wielu wyzwaniom związanym z kontrolą przepływu informacji między dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych oraz innymi dostawcami usług związanych z ICT/OT, jeśli w tym celu wykorzystywane są publiczne sieci.

Poziom(y): 3

AC-5 ROZDZIAŁ OBOWIĄZKÓW

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien zagwarantować zapewnienie odpowiedniego podziału obowiązków w przypadku decyzji dotyczących nabycia elementów system informacyjnego oraz łańcucha dostaw. Podział obowiązków pomaga zapewnić odpowiednie zabezpieczenia komponentów wchodzących w skład łańcucha dostaw podmiotu, na przykład uniemożliwienie programistom przesyłania napisanego przez nich kodu ze środowisk deweloperskich do środowisk produkcyjnych. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

AC-6 ZASADA WIEDZY KONIECZNEJ

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Dodatkowe wytyczne dotyczące obszaru C-SCRM znajdują się w części poświęconej zabezpieczeniom rozszerzonym. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Zabezpieczenia rozszerzone:

5. *ZASADA WIEDZY KONIECZNEJ | UPRZYWILEJOWANY DOSTĘP DLA UŻYTKOWNIKÓW SPOZA ORGANIZACJI*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zapewnić, że wdrożyły zabezpieczenia uniemożliwiające użytkownikom spoza podmiotu uzyskanie uprzywilejowanego dostępu do łańcucha dostaw podmiotu i powiązanych informacji. Jeżeli wśród użytkowników znajdują się niezależni konsultanci, dostawcy, deweloperzy, integratorzy systemów, dostawcy zewnętrznych usług systemowych oraz inni dostawcy usług związanych z ICT/OT, może zaistnieć potrzeba wdrożenia odpowiednich wymogów dotyczących dostępu wykorzystujących zasady minimalnych uprawnień w celu dokładnego określenia, które informacje lub komponenty są dostępne, jak długo, z jaką częstotliwością, przy użyciu jakich metod dostępu i przez kogo. Zrozumienie, które komponenty są kluczowe może pomóc w zrozumieniu poziomu szczegółowości w odniesieniu do zasady minimalnych uprawnień dla użytkowników niebędących pracownikami podmiotu.

Poziom(y): 2, 3

AC-17 DOSTĘP ZDALNY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Coraz częściej dostęp do łańcuchów dostaw odbywa się w sposób zdalny. Niezależnie od tego, czy chodzi o rozwój, utrzymanie czy obsługę systemów informacyjnych, podmioty powinny wdrożyć bezpieczne mechanizmy zdalnego dostępu i umożliwiać dostęp zdalny tylko sprawdzonym pracownikom. Dostęp zdalny do łańcucha dostaw podmiotu (w tym rozproszonych środowisk rozwoju oprogramowania) powinien być ograniczony do pracowników podmiotu lub wykonawcy i tylko wtedy, gdy jest to wymagane do realizacji ich zadań. Wymagania dotyczące zdalnego dostępu – takie jak korzystanie

z bezpiecznej sieci VPN, stosowanie uwierzytelniania wieloskładnikowego lub ograniczanie dostępu w określonych godzinach pracy lub z określonych lokalizacji geograficznych – muszą być odpowiednio zdefiniowane w umowach. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F.

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *DOSTĘP ZDALNY | OCHRONA INFORMACJI O MECHANIZMACH*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny upewnić się, że szczegółowe wymagania są właściwie zdefiniowane, a dostęp do informacji dotyczących systemu informacyjnego i łańcucha dostaw jest chroniony przed nieuprawnionym użyciem i ujawnieniem. Ponieważ ujawnienie danych i metadanych dotyczących łańcucha dostaw lub dostęp do nich może mieć istotne konsekwencje dla realizacji misji podmiotu, należy podjąć odpowiednie działania w celu zweryfikowania zarówno łańcucha dostaw, jak i procesów kadrowych, aby zapewnić wdrożenie odpowiednich zabezpieczeń. Należy upewnić się, że dostęp zdalny do takich informacji jest uwzględniony w wymaganiach.

Poziom(y): 2, 3

AC-18 DOSTĘP BEZPRZEWODOWY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Łańcuch dostaw podmiotu może obejmować infrastrukturę bezprzewodową, która wspomaga logistykę łańcucha dostaw (np. obsługa urządzeń identyfikacyjnych wykorzystujących częstotliwości radiowe [RFID] oraz funkcje oprogramowania odpytujące zdalne serwery). Systemy oraz komponenty łańcucha dostaw przemieszczają się w łańcuchu dostaw,

ponieważ są przenoszone z jednej lokalizacji do drugiej, zarówno w obrębie wewnętrznego środowiska podmiotu, jak i podczas dostaw od integratorów systemów lub dostawców. Zapewnienie odpowiednich i bezpiecznych mechanizmów dostępu w ramach łańcucha dostaw umożliwia ochronę systemów informacyjnych i ich komponentów, a także technologii logistycznych i metadanych wykorzystywanych w logistyce (np. w ramach czujników śledzenia). Podmiot powinien jednoznacznie określić w polityce odpowiednie mechanizmy kontroli dostępu do sieci bezprzewodowej dla łańcucha dostaw oraz wdrożyć odpowiednie zabezpieczenia.

Poziom(y): 1, 2, 3

AC-19 KONTROLA DOSTĘPU DO URZĄDZEŃ PRZENOŚNYCH

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Wykorzystanie urządzeń mobilnych (np. laptopów, tabletów, czytników e-booków, smartfonów, zegarków) jest powszechnym zjawiskiem w łańcuchu dostaw. Są one wykorzystywane do bezpośredniego wspierania działalności podmiotu, a także stanowią jego elementy pozwalające na śledzenie i obsługę logistyki łańcucha dostaw, systemy informacyjne, a także ich komponenty, które przemieszczają się w łańcuchach dostaw podmiotu lub integratorów systemów. Podmiot powinien zapewnić, że mechanizmy kontroli dostępu są jasno określone i wdrożone w procesie zarządzania komponentami łańcucha dostaw podmiotu. Przykład takiego wdrożenia obejmuje mechanizmy kontroli dostępu wykorzystujące zdalne skanery RFID do śledzenia komponentów przemieszczanych w łańcuchu dostaw. Mechanizmy sterowania dostępem należy również wdrożyć w odniesieniu do wszelkich powiązanych z urządzeniami danych i metadanych.

Poziom(y): 2, 3

AC-20 WYKORZYSTANIE SYSTEMÓW ZEWNĘTRZNYCH

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Zewnętrzne systemy informacyjne podmiotów obejmują systemy dostawców, deweloperów,

integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT. W przeciwieństwie do wewnętrznej struktury, w ramach której możliwe jest bezpośrednie i ciągłe monitorowanie, w przypadku relacji z dostawcą zewnętrznym informacje mogą być udostępniane na żądanie, a ich zakres powinien być ujęty w umowie. Dostęp do łańcucha dostaw z takich zewnętrznych systemów informacyjnych powinien być monitorowany i kontrolowany. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Poziom(y): 1, 2, 3

Zabezpieczenia rozszerzone:

1. *WYKORZYSTANIE SYSTEMÓW ZEWNĘTRZNYCH | OGRANICZENIA DOTYCZĄCE DOZWOLONEGO UŻYTKOWANIA*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: To zabezpieczenie rozszerzone pomaga ograniczyć ryzyko związane z łańcuchem dostaw wynikające z ekspozycji na systemy dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych i innych dostawców usług związanych z ICT/OT.

Poziom(y): 2, 3

2. *WYKORZYSTANIE SYSTEMÓW ZEWNĘTRZNYCH | OGRANICZONE WYKORZYSTANIE SYSTEMÓW NIENALEŻĄCYCH DO ORGANIZACJI*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Urządzenia, które nie należą do podmiotu (np. przynoszone przez pracowników w ramach polityki „przynieś własne urządzenie”) zwiększają narażenie podmiotu na ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw. Obejmuje to urządzenia używane przez dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług

związanych z ICT/OT. Podmioty powinny dokonać przeglądu korzystania przez pracowników z urządzeń nienależących do podmiotu i podjąć decyzję opartą na ryzyku, czy zamierzają zezwolić na korzystanie z takich urządzeń, czy raczej postanawiają zapewnić pracownikom własne urządzenia. Podmioty powinny przekazywać urządzenia pracownikom wewnętrznym, w przypadku których poziom ryzyka jest niedopuszczalny.

Poziom(y): 2, 3

AC-21 UDOSTĘPNIANIE INFORMACJI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Przekazywanie informacji w ramach łańcucha dostaw może pomóc w zarządzaniu ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw. Mogą one obejmować podatności, zagrożenia, poziom krytyczności systemów i komponentów lub informacje o dostawach. Wymiana informacji powinna być starannie kontrolowana, aby zapewnić, że dostęp do informacji mają tylko upoważnione osoby w łańcuchu dostaw podmiotu. Podmioty powinny jasno określić granice wymiany informacji dotyczące wymogów czasowych, informacyjnych, umownych, bezpieczeństwa, dostępu, systemu i innych. Podmioty powinny monitorować i sprawdzać niezamierzone lub zamierzone przypadki udostępniania informacji w ramach łańcucha dostaw, w tym dzielenie się informacjami z dostawcami, programistami, integratorami systemów, dostawcami zewnętrznych usług systemowych oraz innymi dostawcami usług związanych z ICT/OT.

Poziom(y): 1, 2

AC-22 TREŚCI PUBLICZNIE DOSTĘPNE

Dodatkowe wytyczne dotyczące obszaru C-SCRM: W kontekście obszaru C-SCRM publicznie dostępne treści mogą obejmować zapytania o udzielenie informacji, zapytania ofertowe lub informacje o dostawie systemów i komponentów. Informacje te powinny być przeglądane

w celu zapewnienia, że tylko stosowne treści są udostępniane publicznie, zwłaszcza jeśli towarzyszą one innym informacjom.

Poziom(y): 2, 3

AC-23 OCHRONA PRZED PRZESZUKIWANIEM DANYCH

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa w ramach zwalczania zagrożeń wewnętrznych i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Poziom(y): 2, 3

AC-24 PRZYZNAWANIE PRAW DOSTĘPU

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny przydzielić decyzje dotyczące kontroli dostępu, aby wspierać autoryzowany dostęp do łańcucha dostaw. Należy zapewnić, że w przypadku korzystania z usług integratora systemu lub zewnętrznego dostawcy usług istnieją spójne wymagania dotyczące decyzji w zakresie kontroli dostępu oraz sposobu wdrożenia tych wymagań. Może to wymagać określenia takich wymagań w umowach gwarancji świadczenia usługi, które w wielu przypadkach mogą stanowić część procesu nawiązywania relacji między podmiotem a integratorem systemu lub dostawcą usług zewnętrznych. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Poziom(y): 1, 2, 3

KATEGORIA AT: UŚWIADAMIANIE I SZKOLENIA

Dokument [NSC 200] określa minimalne wymagania bezpieczeństwa w zakresie uświadamiania i szkolenia w następujący sposób:

> *Organizacje powinny: (I) zapewnić, aby menedżerowie i użytkownicy organizacyjnych systemów informacyjnych byli informowani o zagrożeniach bezpieczeństwa związanych z ich działalnością oraz o obowiązujących przepisach prawa, zarządzeniach wykonawczych, dyrektywach, zasadach, standardach, instrukcjach, przepisach lub procedurach związanych z bezpieczeństwem organizacyjnych systemów informacyjnych; oraz (II) zapewnić, aby personel organizacyjny był odpowiednio przeszkolony w zakresie wykonywania powierzonych mu zadań i obowiązków związanych z bezpieczeństwem informacji.*

Niniejszy dokument rozszerza zakres środków bezpieczeństwa związanych ze świadomością i szkoleniem zawartych w dokumencie [NSC 200] o zagadnienia dotyczące obszaru C-SCRM. Uświadomienie pracownikom problemów związanych z obszarem C-SCRM jest kluczem do skutecznej realizacji strategii C-SCRM. Świadomość i szkolenie w zakresie zagrożeń związanych z cyberbezpieczeństwem w całym łańcuchu dostaw gwarantuje zrozumienie problematyki oraz odpowiednich procesów i zabezpieczeń, które mogą pomóc w ograniczeniu ryzyka. Podmioty powinny zapewnić świadomość i szkolenie w zakresie C-SCRM pracownikom na wszystkich szczeblach – powinny objąć pracowników w jednostkach zajmujących się zagadnieniami bezpieczeństwa informacji, zamówień i zaopatrzenia, zarządzania ryzykiem podmiotu, inżynierii, rozwoju oprogramowania, systemów informacyjnych, prawa, kadrowymi i innymi. Podmioty powinny również współpracować z dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT w celu zapewnienia, że pracownicy mający styczność z łańcuchami dostaw podmiotu, są odpowiednio uwrażliwieni i przeszkoleni na temat zagadnień związanych z obszarem C-SCRM.

AT-1 POLITYKA I PROCEDURY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny wyznaczyć osobę na stanowisku kierowniczym, odpowiedzialną za opracowanie, dokumentowanie i rozpowszechnianie zasad i procedur szkoleń dotyczących między innymi zagadnień związanych z obszarem C-SCRM i szkoleń specjalistycznych dla osób odpowiedzialnych za łańcuch dostaw. Podmioty powinny włączyć szkolenia i zwiększanie świadomości w zakresie zarządzania ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw z szeroko pojętym programem szkoleń i zwiększania świadomości w zakresie bezpieczeństwa. Szkolenie C-SCRM powinno być skierowane zarówno do pracowników podmiotu, jak i jego kontrahentów. Zasada ta powinna zapewnić, że szkolenie dotyczące wpływu na cyberbezpieczeństwo łańcucha dostaw jest wymagane w przypadku osób lub stanowisk, które mają wpływ na łańcuch dostaw, takich jak osoba odpowiedzialna za system informacyjny, pracownicy działów zamówień i zaopatrzenia, pracownicy logistyki, inżynierowie systemów, menadżerowie programów, działy IT, jakości oraz reagowania na incydenty.

Procedury szkoleniowe C-SCRM powinny obejmować:

a. Role w całym łańcuchu dostaw i cyklu życia systemu/komponentu, aby ograniczyć możliwości spowodowania negatywnych konsekwencji przez osoby pracujące na tych stanowiskach;

b. Wymagania dotyczące interakcji pomiędzy pracownikami podmiotu a osobami niezatrudnionymi przez podmiot, które uczestniczą w łańcuchu dostaw w całym cyklu życia systemu, oraz

c. Włączenie informacji zwrotnych i wniosków wypływających z działań w obszarze C-SCRM do szkolenia C-SCRM.

Poziom(y): 1, 2

AT-2 SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Dodatkowe wytyczne dotyczące wyłącznie obszaru C-SCRM zostały przedstawione w formie zabezpieczeń rozszerzonych. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Zabezpieczenie rozszerzone:

1. *SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | ĆWICZENIA PRAKTYCZNE*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zapewnić praktyczne ćwiczenia w ramach szkoleń, które symulują zdarzenia i incydenty związane z cyberbezpieczeństwem w łańcuchu dostaw. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

2. *SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | ZAGROŻENIA WEWNĘTRZNE*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zapewnić szkolenie w zakresie rozpoznawania i zgłaszania potencjalnych sygnałów wskazujących na występowanie zagrożeń wewnętrznych w łańcuchu dostaw. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

3. *SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | INŻYNIERIA SPOŁECZNA ORAZ WYDOBYWANIE*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zapewnić szkolenie w zakresie umiejętności rozpoznawania i zgłaszania potencjalnych i rzeczywistych przypadków inżynierii społecznej związanych z łańcuchem dostaw. Podmioty powinny

wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

4. *SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | PODEJRZANE KOMUNIKATY I NIETYPOWE ZACHOWANIA SYSTEMU*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien zapewnić szkolenie w zakresie rozpoznawania podejrzanych komunikatów lub nietypowych zachowań systemów łańcucha dostaw podmiotu. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

5. *SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | ZAAWANSOWANE TRWAŁE ZAGROŻENIA*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Zapewnienie szkolenia w zakresie rozpoznawania podejrzanych komunikatów dotyczących zaawansowanego trwałego zagrożenia typu APT (*ang. advanced persistent threat*) w łańcuchu dostaw podmiotu. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

6. *SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | ŚRODOWISKA ZAGROŻEŃ ZWIĄZANYCH Z CYBERBEZPIECZEŃSTWEM*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zapewnić szkolenia dotyczące cyberzagrożeń dotyczących środowiska łańcucha dostaw podmiotu. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Poziom(y): 2

AT-3 SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Uwzględnienie zagrożeń związanych z cyberbezpieczeństwem w całym łańcuchu dostaw w procesie zamówień oraz zaopatrzenia jest niezbędne dla skuteczności wdrożenia działań w zakresie C-SCRM. Pracownicy zajmujący się zamówieniami i zaopatrzeniem wymagają szkoleń na temat wymogów, klauzul oraz czynników oceny dotyczących obszaru C-SCRM, które należy uwzględnić w procesie realizacji zamówień oraz na temat włączania zagadnień dotyczących obszaru C-SCRM do każdego etapu procesu zamówień. Podobne wymagania dotyczące szkoleń powinny dotyczyć osób odpowiedzialnych za przeprowadzanie ocen zagrożenia. Reagowanie na zagrożenia i zidentyfikowane ryzyka wymaga szkolenia w zakresie świadomości i raportowania. Podmioty powinny zapewnić deweloperom szkolenia z zakresu bezpiecznych praktyk programistycznych, a także stosowania narzędzi do skanowania podatności. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Zabezpieczenia rozszerzone:

1. *SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH | FIZYCZNE ŚRODKI BEZPIECZEŃSTWA*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Obszar C-SCRM jest związany z szeregiem mechanizmów i procedur zabezpieczeń fizycznych w ramach kolejnych etapów łańcucha dostaw, takich jak produkcja, wysyłka, odbiór, fizyczny dostęp do obiektów, kontrola stanów magazynowych i magazynowanie. Pracownicy podmiotu i integratorów systemów, którzy zapewniają organizacji wsparcie rozwojowe i operacyjne, powinni przejść szkolenie dotyczące obsługi tych mechanizmów zabezpieczeń oraz związanych z nimi zagrożeń dla cyberbezpieczeństwa w całym łańcuchu dostaw.

Poziom(y): 2

2. *SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH | SZKOLENIE Z ZAGADNIEŃ DOTYCZĄCYCH KONTRWYWIADU*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty działające w sektorze publicznym powinny zapewnić pracownikom specjalistyczne szkolenie w zakresie zagadnień dotyczących kontrwywiadu, które umożliwi im gromadzenie, interpretowanie i działanie na podstawie szeregu źródeł danych, które mogą sygnalizować obecność adwersarza w łańcuchu dostaw. Szkolenie z zagadnień dotyczących kontrwywiadu powinno obejmować przynajmniej podstawowe i znane sygnały ostrzegawcze, najważniejsze obszary wymiany informacji oraz wymagania dotyczące raportowania.

Poziom(y): 2

AT-4 DOKUMENTACJA SZKOLENIOWA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny prowadzić dokumentację dotyczącą szkoleń dotyczących obszaru C-SCRM, szczególnie szkoleń dotyczących kluczowego personelu zajmującego się zamówieniami oraz zagadnień związanych z kontrwywiadem.

Poziom(y): 2

KATEGORIA AU: AUDYT I ROZLICZALNOŚĆ

Dokument [NSC 200] określa minimalne wymagania bezpieczeństwa w zakresie audytu i rozliczalności w następujący sposób:

> *Organizacje powinny: (I) tworzyć, chronić i przechowywać rejestry audytu systemu informacyjnego w zakresie niezbędnym do umożliwienia monitorowania, analizy, badania i zgłaszania bezprawnych, nieautoryzowanych lub nieodpowiednich działań systemu informacyjnego; oraz (II) zapewnić, aby działania poszczególnych użytkowników systemu informacyjnego mogły być jednoznacznie powiązane z tymi użytkownikami, tak, aby mogli oni zostać pociągnięci do odpowiedzialności za swoje działania.*

Środki audytu i rozliczalności związane z obszarem C-SCRM dostarczają informacji przydatnych w przypadku incydentu lub naruszenia zasad ochrony cyberbezpieczeństwa łańcucha dostaw. Podmioty powinny zapewnić, że identyfikują oraz kontrolują zdarzenia dotyczące cyberbezpieczeństwa w łańcuchu dostaw w granicach ich systemów informacyjnych przy użyciu odpowiednich mechanizmów audytu (np. dzienniki systemowe, dzienniki systemu wykrywania włamań, dzienniki zapory sieciowej, sprawozdania papierowe, formularze, listy kontrolne, zapisy cyfrowe). Mechanizmy audytu powinny być również skonfigurowane tak, aby działały w rozsądnych ramach czasowych, określonych przez politykę podmiotu. Podmioty mogą zachęcać swoich dostawców systemów, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT do takiego samego postępowania i mogą zawrzeć w umowach wymogi dotyczące audytu. Podmioty nie powinny jednak wdrażać mechanizmów audytu w systemach znajdujących się poza ich granicami, w tym u dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT.

AU-1 POLITYKA I PROCEDURY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty muszą wyznaczyć odpowiedniego menadżera wyższego szczebla,

odpowiedzialnego za opracowanie, dokumentację oraz rozpowszechnianie polityki i procedur audytu i rozliczalności, w tym audytu systemów informacyjnych i sieci łańcucha dostaw. Polityka i procedury dotyczące audytu i rozliczalności powinny uwzględniać działania związane ze śledzeniem oraz ich dostępność w przypadku innych działań realizowanych w ramach łańcucha dostaw, takich jak zarządzanie konfiguracją. Polityka ta nie powinna obejmować działań dostawców, programistów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT, chyba że działania te są realizowane w ramach systemów informacyjnych i sieci łańcucha dostaw podmiotu nabywającego. Procedury polityki audytu i rozliczalności powinny uwzględniać audyty dostawców jako sposób badania jakości konkretnego dostawcy oraz ryzyka, jakie stanowi on dla podmiotu i jego łańcucha dostaw.

Poziom(y): 1, 2, 3

AU-2 AUDYT ZDARZEŃ

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Obserwowalne zdarzenie w systemie informacyjnym lub sieci łańcucha dostaw należy zidentyfikować jako zdarzenie wymagające udokumentowania i audytu w łańcuchu dostaw w oparciu o kontekst i wymagania cyklu życia systemu podmiotu. Do zdarzeń wymagających udokumentowania i audytu można zaliczyć zmiany w oprogramowaniu lub sprzęcie, nieudane próby dostępu do systemów informacyjnych łańcucha dostaw lub zmiany dotyczące kodu źródłowego. Informacje o takich zdarzeniach powinny być wychwytywane przez odpowiednie mechanizmy zabezpieczeń oraz być możliwe do prześledzenia i zweryfikowania. Zgromadzone informacje powinny obejmować rodzaj zdarzenia, datę/godzinę, długość i częstotliwość występowania. Audyt może pomóc między innymi w wykryciu nadużyć systemów informacyjnych lub sieci łańcucha dostaw, spowodowanego przez zagrożenia wewnętrzne. Pliki dziennika są kluczowym materiałem

pozwalającym na dostrzeganie trendów operacyjnych i długotrwałych problemów. W związku z tym podmioty powinny włączyć analizy plików dziennika do procesów odnawiania umów z dostawcami, aby ustalić, czy istnieją problemy systemowe. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 1, 2, 3

AU-3 ZAWARTOŚĆ REJESTRÓW AUDYTU

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Dokumentacja audytu zdarzeń w łańcuchu dostaw musi być odpowiednio gromadzona oraz utrzymywania w sposób zgodny z wymogami dotyczącymi przechowywania dokumentacji oraz zapewniający integralność i poufność informacji i danych o ich źródłach. W niektórych przypadkach takie dane mogą być wykorzystane w postępowaniu dyscyplinarnym lub sądowym. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 1, 2, 3

AU-6 PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien zapewnić, że zarówno zdarzenia dotyczące łańcucha dostaw, jak i bezpieczeństwa informacji, które są zdarzeniami wymagającymi zapewnienia śladu audytowego, są odpowiednio filtrowane i korelowane na potrzeby analiz i sprawozdawczości. Na przykład, jeśli nowa aktualizacja lub poprawka zostanie uwierzytelniona nieważnym podpisem cyfrowym, stwierdzenie nadesłania poprawki kwalifikuje się jako zdarzenie podlegające audytowi

łańcucha, podczas gdy nieważny podpis jest zdarzeniem podlegającym audytowi bezpieczeństwa informacji. Połączenie tych dwóch zdarzeń może być źródłem informacji, które są wartościowe z punktu widzenia obszaru C-SCRM. Podmiot powinien dostosować poziom przeglądu dokumentacji z audytu w oparciu o zmiany dotyczące ryzyka (np. informacji o aktywnych zagrożeniach, profilu ryzyka) w przypadku konkretnego dostawcy. Umowy powinny wyraźnie określać, w jaki sposób ustalenia audytu będą zgłaszane i rozstrzygane.

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE| KORELACJA Z INFORMACJAMI ZE ŹRÓDEŁ NIETECHNICZNYCH*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: W kontekście obszaru C-SCRM źródła nietechniczne obejmują zmiany w polityce bezpieczeństwa lub operacyjnej podmiotu, zmiany w procesach zamówień lub kontraktowania oraz powiadomienia od dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT dotyczące planów aktualizacji, ulepszeń, poprawek lub wycofania/utylizacji systemu/komponentu.

Poziom(y): 3

AU-10 NIEZAPRZECZALNOŚĆ

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny wdrożyć rozwiązania zapewniające niezaprzeczalność w celu ochrony oryginalności i integralności zarówno systemów informacyjnych, jak i sieci łańcucha dostaw. Przykłady obszarów wymagających niezaprzeczalności obejmują metadane łańcucha dostaw, które opisują elementy, komunikację w łańcuchu dostaw oraz informacje o przyjęciu dostawy. W przypadku systemów informacyjnych przykładem może być aktualizacja

oprogramowania, a także wymiana podzespołów ważnego systemu sprzętowego. Weryfikacja, że takie komponenty pochodzą od producenta oryginalnego wyposażenia stanowi element niezaprzeczalności.

Poziom(y): 3

Zabezpieczenia rozszerzone:

1. *NIEZAPRZECZALNOŚĆ | KOJARZENIE TOŻSAMOŚCI*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: To zabezpieczenie rozszerzone usprawnia śledzenie w łańcuchu dostaw i ułatwia udowodnienie pochodzenia.

Poziom(y): 2

2. *NIEZAPRZECZALNOŚĆ | POTWIERDZANIE ZWIĄZKU TOŻSAMOŚCI TWÓRCY INFORMACJI*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: To zabezpieczenie rozszerzone potwierdza związek między pochodzeniem a komponentem w łańcuchu dostaw, dając tym samym gwarancję pochodzenia.

Poziom(y): 2, 3

3. *NIEZAPRZECZALNOŚĆ | ŁAŃCUCH DOWODOWY*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Łańcuch dowodowy ma kluczowe znaczenie dla weryfikacji pochodzenia i identyfikowalności w łańcuchu dostaw. Pomaga również w weryfikacji integralności systemu i komponentów.

Poziom(y): 2, 3

AU-12 TWORZENIE ZAPISÓW AUDYTU

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zapewnić, że istnieją mechanizmy generowania dokumentacji audytu gromadzące wszystkie istotne zdarzenia w łańcuchu dostaw. Przykłady takich zdarzeń to aktualizacje wersji komponentów, dopuszczenia

komponentów po testach akceptacyjnych, dane logistyczne dotyczące zapasów lub informacje o transporcie. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

AU-13 MONITOROWANIE UJAWNIANIA INFORMACJI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: W kontekście zagadnień związanych z obszarem C-SCRM ujawnienie informacji może nastąpić na wiele sposobów, w tym poprzez informacje z otwartego źródła. Na przykład errata dostarczona przez dostawcę może ujawnić informacje o systemie podmiotu, które zwiększają ryzyko dotyczące tego systemu. Podmioty powinny zapewnić monitorowanie systemów wykonawców w celu wykrycia nieuprawnionego ujawnienia wszelkich danych oraz zapewnić, że zapisy umowne zawierają wymogi, które wymuszą powiadomienie podmiotu w określonych ramach czasowych i tak szybko jak to możliwe, w przypadku jakiegokolwiek potencjalnego lub rzeczywistego nieuprawnionego ujawnienia informacji. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

AU-14 AUDYT SESJI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny objąć pracowników kontraktowych audytami sesji w celu wykrywania zagrożeń dla bezpieczeństwa w łańcuchu dostaw. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka

bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

AU-16 AUDYT MIĘDZYORGANIZACYJNY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: W kontekście zagadnień dotyczących obszaru C-SCRM ten środek bezpieczeństwa obejmuje korzystanie przez podmiot z infrastruktury integratora systemów lub dostawcy zewnętrznych usług systemowych. Podmioty powinny dodać do umów zapisy dotyczące koordynacji wymogów na temat dokumentacji audytu oraz zawrzeć umowy o wymianie informacji z dostawcami.

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *AUDYT MIĘDZYORGANIZACYJNY | UDOSTĘPNIANIE INFORMACJI Z AUDYTU*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Niezależnie od rodzaju środowiska, podmiot oraz integratorzy systemów oraz dostawcy zewnętrznych usług systemowych powinni ustanowić szereg wymogów dotyczących procesu wymiany informacji z audytów. W przypadku integratora systemu i zewnętrznego dostawcy usług oraz podmiotu należy z wyprzedzeniem uzgodnić umowę gwarancji świadczenia usługi dotyczącą rodzaju wymaganych danych oraz możliwości ich dostarczenia, aby zapewnić, że podmiot uzyska odpowiednie informacje z audytu wymagane w celu zapewnienia stosowania odpowiednich zabezpieczeń w celu zaspokojenia potrzeb w zakresie ochrony działań biznesowych. Podmiot powinien zapewnić objęcie zasięgiem zarówno systemów informacyjnych, jak i sieci łańcucha dostaw w celu gromadzenia i udostępniania informacji. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Poziom(y): 2, 3

KATEGORIA CA: OCENA, AUTORYZACJA I MONITOROWANIE

Dokument [NSC 200] określa minimalne wymagania bezpieczeństwa w zakresie oceny, autoryzacji i monitorowania w następujący sposób:

> *Organizacje powinny: (I) okresowo oceniać środki bezpieczeństwa w systemach informacyjnych organizacji, w celu ustalenia, czy zabezpieczenia są skuteczne w ich stosowaniu; (II) opracowywać i wdrażać plany działania mające na celu wyeliminowanie niedociągnięć oraz zmniejszenie lub wyeliminowanie luk w zabezpieczeniach organizacyjnych systemów informacyjnych; (III) autoryzować działanie organizacyjnych systemów informacyjnych i wszelkich powiązanych połączeń systemów informacyjnych; oraz (IV) na bieżąco monitorować środki bezpieczeństwa systemu informacyjnego w celu zapewnienia ciągłej skuteczności zabezpieczeń.*

Podmioty powinny uwzględnić zagadnienia związane z obszarem C-SCRM, w tym proces zarządzania ryzykiem w łańcuchu dostaw oraz stosowanie odpowiednich środków bezpieczeństwa określonych w niniejszej publikacji, do bieżących działań w zakresie oceny bezpieczeństwa i autoryzacji. Obejmuje to działania mające na celu ocenę i autoryzację systemów informacyjnych podmiotu, jak również zewnętrzne oceny dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz, w stosownych przypadkach, innych dostawców usług związanych z ICT/OT. Aspekty dotyczące łańcucha dostaw obejmują dokumentację, śledzenie łańcucha dowodowego i połączeń systemów w podmiotach i pomiędzy nimi, weryfikację szkoleń z zakresu cyberbezpieczeństwa w łańcuchu dostaw, weryfikację oświadczeń dostawców o zgodności z zasadami bezpieczeństwa, integralności produktu/komponentu oraz narzędzi i technik walidacji w zakresie nieinwazyjnych metod wykrywania podróbek lub złośliwego oprogramowania (np. koni trojańskich) przy pomocy kontroli autentyczności, w tym ręcznych kontroli produktów.

CA-1 POLITYKA I PROCEDURY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Należy włączyć opracowanie i wdrożenie polityki oraz procedur oceny i autoryzacji dotyczących cyberbezpieczeństwa w łańcuchu dostaw do zasad Ocena

zabezpieczeń oraz autoryzacji zabezpieczeń, a także związanych z nimi strategiami oraz planami wdrożenia programów C-SCRM, politykami oraz planami na poziomie systemu. Aby przeciwdziałać zagrożeniom związanym z cyberbezpieczeństwa w całym łańcuchu dostaw, podmioty powinny opracować politykę C-SCRM (lub, jeśli to konieczne, włączyć ją do istniejących polityk), aby ukierunkować działania C-SCRM w zakresie Ocena zabezpieczeń i autoryzacji. Polityka C-SCRM powinna określać role i obowiązki związane z obszarem C-SCRM w zakresie przeprowadzania Ocena zabezpieczeń i autoryzacji, wszelkie zależności pomiędzy tymi rolami oraz interakcje pomiędzy nimi. Ryzyko związane z bezpieczeństwem i prywatnością w skali całego podmiotu powinno być oceniane na bieżąco i obejmować wyniki oceny ryzyka w łańcuchu dostaw.

Poziom(y): 1, 2, 3

CA-2 OCENA ZABEZPIECZEŃ

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Organizacja powinna zapewnić, że plan Ocena zabezpieczeń zawiera odpowiednie środki bezpieczeństwa związane z obszarem C-SCRM i zabezpieczenia rozszerzone. Ocena zabezpieczeń powinna obejmować ocenę zarówno systemów informacyjnych, jak i łańcucha dostaw oraz zapewniać identyfikację i wykorzystanie do oceny bazowego zestawu zabezpieczeń istotnych dla podmiotu oraz zabezpieczeń rozszerzonych. Ocena zabezpieczeń mogą obejmować informacje pochodzące z audytów dostawców, przeglądów i informacji dotyczących łańcucha dostaw. Podmioty powinny opracować strategię gromadzenia informacji, w tym strategię prowadzenia ocen ryzyka łańcucha dostaw we współpracy z dostawcami. Taka współpraca pomaga podmiotom wykorzystać informacje od dostawców, ograniczyć nadmiarowość, określić potencjalne kierunki działania w zakresie reakcji na ryzyko oraz ograniczyć niepotrzebne działania dostawców. Osoby odpowiedzialne za działania w zakresie C-SCRM powinny dokonać przeglądu Ocena zabezpieczeń.

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *OCENA ZABEZPIECZEŃ | OCENY SPECJALISTYCZNE*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny stosować różne techniki i metodologie oceny, takie jak ciągłe monitorowanie czy analizy zagrożeń wewnętrznych oraz złośliwych użytkowników. Takie mechanizmy oceny powinny być dostosowane do kontekstu i wymagają od podmiotu dokładnego wglądu w łańcuch dostaw oraz określenia wymaganego zestawu działań służących do oceny i weryfikacji, czy wdrożono odpowiednie zabezpieczenia.

Poziom(y): 3

2. *OCENA ZABEZPIECZEŃ | WYKORZYSTYWANIE WYNIKÓW DOSTARCZANYCH PRZEZ INNE ORGANIZACJE*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: W obszarze C-SCRM podmioty powinny wykorzystywać zewnętrzne oceny bezpieczeństwa dotyczące dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT. Zewnętrzne oceny obejmują certyfikaty, badania przeprowadzone przez podmioty zewnętrzne oraz – w kontekście rządowym – wcześniejsze oceny przeprowadzone przez i służby państwowe. Certyfikaty Międzynarodowego Komitetu Normalizacyjnego (ISO, certyfikaty Common Criteria Recognition Arrangement (CCRA), mogą być również wykorzystywane przez podmioty, jeśli wydane przez nie certyfikaty spełniają potrzeby podmiotu.

Poziom(y): 3

CA-3 WYMIANA INFORMACJI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Wymiana informacji lub danych pomiędzy systemami wymaga stosownych zabezpieczeń z punktu widzenia łańcucha dostaw. Obejmuje to zrozumienie charakterystyki

interfejsu i połączeń między systemami i komponentami, a także danych udostępnionych przy pomocy tych komponentów lub systemów deweloperom, integratorom systemów, zewnętrznym dostawcom usług systemowych, innym dostawcom usług związanych z ICT/OT oraz – w niektórych przypadkach – także dostawcom. Należy wprowadzić odpowiednie umowy gwarancji świadczenia usług, aby zapewnić zgodność z wymogami dotyczącymi wymiany informacji określonymi przez podmiot, ponieważ przekazywanie informacji między systemami w różnych domenach bezpieczeństwa lub prywatności, w których obowiązują różne polityki bezpieczeństwa lub prywatności, może wiązać się z ryzykiem naruszenia zasad bezpieczeństwa lub prywatności jednej lub więcej domen. Przykłady takich połączeń mogą obejmować:

a. Wspólne środowisko programistyczne i operacyjne dla podmiotu i integratora systemów;

b. Połączenie pozwalające na aktualizację produktów z serwerem dostawcy oprogramowania komercyjnego;

c. Transakcje zawierające zapytania oraz pobieranie danych w systemie przetwarzania, który znajduje się w środowisku współdzielonym dostawcy zewnętrznych usług systemowych;

Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Poziom(y): 3

CA-5 PLAN I ETAPY DZIAŁANIA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: W przypadku planu i etapów działań na poziomie systemu podmioty muszą zapewnić opracowanie oddzielnego planu i wyznaczenie etapów działań dotyczących obszaru C-SCRM, który obejmuje zarówno systemy informacyjne, jak i łańcuch dostaw. Plan działania i etapy dotyczące obszaru C-SCRM

powinny zawierać zadania do wykonania z zaleceniem ich wykonania przed lub po autoryzacji systemu, zasoby wymagane do ich realizacji, kamienie milowe ustanowione w celu weryfikacji realizacji zadań oraz planowane daty ich osiągnięcia. Podmiot powinien uwzględnić w tych planach wpływ podatności na systemy informacyjne lub łańcuch dostaw, wszelkie działania naprawcze mające na celu usunięcie podatności oraz wszelkie działania w zakresie ciągłego monitorowania. Plan ten powinien stanowić część pakietu autoryzacyjnego.

Poziom(y): 2, 3

CA-6 AUTORYZACJA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Osoby autoryzujące powinny uwzględniać działania związane z obszarem C-SCRM w decyzjach autoryzacyjnych. Aby to osiągnąć, ryzyka związane z łańcuchem dostaw i środki bezpieczeństwa udokumentowane w planach C-SCRM lub planach bezpieczeństwa systemu oraz planach i etapach działania dotyczących obszaru C-SCRM powinny być włączone do pakietu autoryzacyjnego w ramach procesu decyzyjnego. Ryzyko powinno być określone, a związane z nim środki bezpieczeństwa dobrane na podstawie wyników analiz krytyczności, zagrożeń i podatności. Osoby autoryzujące mogą korzystać z wytycznych zawartych w rozdziale 2 niniejszego dokumentu, jak również z dokumentu NISTIR 8179 w celu przeprowadzenia procesu oceny.

Poziom(y): 1, 2, 3

CA-7 CIĄGŁE MONITOROWANIE

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Wytyczne dotyczące tego środka bezpieczeństwa dotyczące obszaru C-SCRM znajdują się w rozdziale 2 niniejszej publikacji. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 1, 2, 3

Zabezpieczenia rozszerzone:

3. *CIĄGŁE MONITOROWANIE | ANALIZY TRENDÓW*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Informacje zebrane podczas ciągłego monitorowania oraz analizy trendów służą jako podstawa decyzji dotyczących obszaru C-SCRM, w tym analiz krytyczności, analiz podatności i zagrożeń oraz ocen ryzyka. Stanowią również źródło danych, które mogą być wykorzystane w procesie reakcji na incydenty oraz pozwolą na wykrycie naruszenia zasad ochrony łańcucha dostaw, w tym zagrożeń wewnętrznych.

Poziom(y): 3

KATEGORIA CM: ZARZĄDZANIE KONFIGURACJĄ

Dokument [NSC 200] określa minimalne wymagania bezpieczeństwa w zakresie zarządzania konfiguracją w następujący sposób:

> *Organizacje powinny: (I) ustanowić i utrzymywać podstawowe konfiguracje i wykazy organizacyjnych systemów informacyjnych (w tym sprzętu, oprogramowania, oprogramowania układowego i dokumentacji) w odpowiednich cyklach życia rozwoju systemu; oraz (II) ustanowić i egzekwować ustawienia konfiguracji zabezpieczeń dla produktów technologii informacyjnych stosowanych w organizacyjnych systemach informacyjnych.*

Zarządzanie konfiguracją pozwala na śledzenie zmian konfiguracji w trakcie cyklu życia systemu wprowadzonych do systemów, komponentów oraz dokumentacji w ramach systemów informacyjnych i sieci. Świadomość zmian wprowadzonych w systemach, komponentach i dokumentacji, źródło zmian oraz tożsamość osób wprowadzających i autoryzujących zmiany są niezwykle ważne. Zarządzanie konfiguracją stanowi również dowód w dochodzeniach dotyczących naruszenia cyberbezpieczeństwa w łańcuchu dostaw, gdyż pozwala ustalić, czy dane zmiany konfiguracji były autoryzowane, czy też nie. Podmioty powinny stosować środki bezpieczeństwa dotyczące zarządzania konfiguracją we własnych systemach oraz zachęcać do ich stosowania swoich dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT. Więcej informacji na temat zarządzania konfiguracją znajduje się w dokumencie NISTIR 7622.

CM-1 POLITYKA I PROCEDURY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Zarządzanie konfiguracją ma wpływ na niemal każdy aspekt łańcucha dostaw. Zarządzanie konfiguracją ma kluczowe znaczenie dla zdolności podmiotu do ustalania pochodzenia komponentów, w tym śledzenia ich w całym cyklu życia systemu i łańcuchu dostaw. Właściwie zdefiniowane i wdrożone możliwości w zakresie zarządzania konfiguracją daje większą pewność w całym cyklu życia systemu i łańcuchu dostaw, że komponenty

są autentyczne i nie zostały zmodyfikowane w sposób nieautoryzowany. Definiując politykę i procedury zarządzania konfiguracją, podmioty powinny brać pod uwagę cały cykl życia systemu, w tym procedury wprowadzania i usuwania komponentów związanych z systemem informacyjnym podmiotu. Polityka zarządzania konfiguracją powinna obejmować elementy konfiguracji, wytyczne dotyczące przechowywania danych na temat konfiguracji i odpowiednich metadanych oraz śledzenie konfiguracji i odpowiednich metadanych. Podmiot powinien koordynować działania w zakresie polityki zarządzania konfiguracją z dostawcami, programistami, integratorami systemów, zewnętrznymi dostawcami usług systemowych oraz innymi dostawcami usług związanych z ICT/OT.

Poziom(y): 1, 2, 3

CM-2 KONFIGURACJA BAZOWA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny ustalić konfigurację bazową zarówno systemu informacyjnego, jak i środowiska programistycznego. W tym celu powinny udokumentować konfigurację, dokonać jej formalnego przeglądu i uzyskać zgodę odpowiednich interesariuszy. Celem konfiguracji bazowej jest zapewnienie punktu wyjścia do śledzenia zmian w komponentach, kodzie bądź w ustawieniach w całym cyklu życia systemu. Regularne przeglądy i aktualizacje konfiguracji bazowych mają kluczowe znaczenie z punktu widzenia identyfikowalności i weryfikacji pochodzenia. Konfiguracja bazowa musi uwzględniać środowisko operacyjne podmiotu oraz wszelkich istotnych dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT mających kontakt z systemami informacyjnymi i sieciami organizacji. Jeśli na przykład integrator systemu wykorzystuje istniejącą infrastrukturę organizacji, należy podjąć odpowiednie działania w celu ustanowienia konfiguracji bazowej, która odzwierciedla odpowiedni zestaw uzgodnionych kryteriów dostępu i działania.

Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *KONFIGURACJA BAZOWA | ŚRODOWISKA ROZWOJOWE I TESTOWE*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien utrzymywać lub wymagać utrzymania konfiguracji bazowej środowisk rozwojowych, testowych (i wdrożeniowych, jeśli dotyczy) stosownych dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT, a także konfiguracji wszystkich interfejsów.

Poziom(y): 2, 3

CM-3 ZABEZPIECZANIE ZMIAN KONFIGURACJI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny określić, wdrożyć, monitorować i kontrolować Ustawienia konfiguracji i zmiany w systemach informacyjnych oraz sieciach przez cały cykl życia systemu. Ten środek bezpieczeństwa zwiększa identyfikowalność na potrzeby działań związanych z obszarem C-SCRM. Poniższe rozszerzenia zabezpieczeń CM-3 (1), (2), (4) i (8) określonych w dokumencie NSC 800-53 stanowią mechanizmy, które mogą zostać wykorzystane w ramach działań w obszarze C-SCRM do gromadzenia danych oraz zarządzania danymi dotyczącymi kontroli zmian. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

1. *ZABEZPIECZANIE ZMIAN KONFIGURACJI | AUTOMATYCZNA DOKUMENTACJA, POWIADOMIENIE I ZAKAZ ZMIAN*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zdefiniować zestaw zmian w systemach, które są kluczowe z punktu widzenia ochrony systemu informacyjnego oraz podstawowych lub współdziałających systemów i sieci. Zmiany te mogą być określone na podstawie analizy krytyczności (obejmującej komponenty, procesy i funkcje) oraz w przypadkach istnienia podatności, które nie zostały jeszcze naprawione (np. ze względu na braki zasobów). Proces kontroli zmian powinien również obejmować monitorowanie zmian potencjalnie wpływających na istniejące środki bezpieczeństwa, aby zapewnić, że dany środek bezpieczeństwa nadal funkcjonuje zgodnie z wymaganiami.

Poziom(y): 2, 3

2. *ZABEZPIECZANIE ZMIAN KONFIGURACJI | TESTOWANIE, WALIDACJA I DOKUMENTACJA ZMIAN*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien testować, walidować i dokumentować zmiany w systemie przed ich wdrożeniem.

Poziom(y): 2, 3

3. *ZABEZPIECZANIE ZMIAN KONFIGURACJI | PRZEDSTAWICIELE DS. BEZPIECZEŃSTWA I PRYWATNOŚCI*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien zapewnić, że jego przedstawiciele ds. bezpieczeństwa i prywatności są członkami pionu odpowiedzialnego za kontrolę zmian w konfiguracji.

Poziom(y): 2, 3

4. *ZABEZPIECZANIE ZMIAN KONFIGURACJI | ZAPOBIEGANIE ZMIANOM LUB OGRANICZANIE ZMIAN W KONFIGURACJI*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien zapobiegać lub ograniczać możliwości zmian w konfiguracji systemu do okoliczności określonych przez podmiot.

Poziom(y): 2, 3

CM-4 ANALIZY WPŁYWU

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny wziąć pod uwagę zmiany w systemie informacyjnym, a także w powiązanych systemach i sieciach, aby określić, czy zmiany te wpływają na istniejące środki bezpieczeństwa i uzasadniają zastosowanie dodatkowej lub innej metody ochrony w celu utrzymania akceptowalnego poziomu ryzyka cyberbezpieczeństwa w całym łańcuchu dostaw. Należy upewnić się, że interesariusze – inżynierowie systemu i inżynierowie bezpieczeństwa systemu – uczestniczą w działaniach związanych z analizą wpływu, aby zapewnić, że działania w zakresie C-SCRM uwzględniają ich punkt widzenia. Zabezpieczenie rozszerzone CM-4 (1) zawarte w dokumencie NSC 800-53 jest mechanizmem, który można wykorzystać do ochrony systemu informacyjnego przed podatnościami, które mogą być wprowadzone poprzez środowisko testowe.

Poziom(y): 3

1. *ANALIZY WPŁYWU | ODDZIELNE ŚRODOWISKA TESTOWE*

Wszelkie zmiany w systemach należy analizować w oddzielnym środowisku testowym przed wdrożeniem ich do środowiska operacyjnego. Należy weryfikować zmiany pod kątem wpływu na bezpieczeństwo i prywatność, a także wszelkie wady, usterki, zaniedbania, niekompatybilności lub złośliwych działań.

Poziom(y): 3

Powiązane środki bezpieczeństwa: SA-11, SC-7.

CM-5 OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zapewnić, że wymagania dotyczące fizycznych i logicznych ograniczeń dostępu do konfiguracji systemów informacyjnych i sieci są zdefiniowane i uwzględnione we wdrożonych przez podmiot systemach kontroli dostępu. Przykłady obejmują ograniczenie dostępu do konfiguracji centralnie zarządzanych procesów aktualizacji komponentów oprogramowania oraz instalowania aktualizacji lub poprawek.

Poziom(y): 2, 3

Zabezpieczenie rozszerzone:

1. *OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | AUTOMATYCZNE EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU I DOKUMENTACJA*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny wdrożyć mechanizmy zapewniające automatyczne Egzekwowanie uprawnień dostępu oraz dokumentowanie aktywności w systemach informacyjnych oraz sieciach i powiązanych systemach.

Poziom(y): 3

2. *OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | OGRANICZENIE DOSTĘPU DO BIBLIOTEK*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny pamiętać, że biblioteki oprogramowania mogą być uznane za elementy konfiguracji, do których dostęp powinien być ograniczony i zarządzany odgórnie.

Poziom(y): 3

CM-6 USTAWIENIA KONFIGURACJI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny nadzorować modyfikowanie ustawień konfiguracyjnych swoich systemów

informacyjnych i sieci w całym cyklu życia systemu. Metody nadzoru obejmują okresową weryfikację, sprawozdawczość i przeglądy. Powstałe w ten sposób informacje mogą być udostępniane różnym stronom, które mają dostęp do systemów informacyjnych i sieci podmiotu, są do nich podłączone lub biorą udział w ich tworzeniu, w zależności od potrzeb. Zmiany powinny być przetestowane i zatwierdzone przed ich wprowadzeniem. Ustawienia konfiguracji powinny być monitorowane i kontrolowane, a wyznaczone osoby powinny być informowane o zmianie. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *USTAWIENIA KONFIGURACJI | AUTOMATYCZNE ZARZĄDZANIE, STOSOWANIE I WERYFIKACJA*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien, jeśli jest to możliwe, stosować zautomatyzowane mechanizmy zarządzania, stosowania i weryfikacji ustawień konfiguracyjnych.

Poziom(y): 3

2. *USTAWIENIA KONFIGURACJI | REAGOWANIE NA NIEAUTORYZOWANE ZMIANY*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien zapewnić, że wyznaczeni pracownicy działu bezpieczeństwa lub IT są powiadamiani o nieautoryzowanych zmianach ustawień konfiguracyjnych. Jeśli dostawcy, deweloperzy, integratorzy systemów, dostawcy zewnętrznych usług systemowych i inni dostawcy usług związanych z ICT/OT są odpowiedzialni za takie nieautoryzowane zmiany, takie zdarzenie

stanowi incydent C-SCRM, który powinien być udokumentowany oraz obserwowany w celu monitorowania trendów. Aby spojrzeć na zagadnienie z szerszej perspektywy, wybrana grupa interesariuszy zajmujących się obszarem C-SCRM powinna ocenić wpływ nieautoryzowanych zmian w łańcuchu dostaw. Po dokonaniu oceny wpływu, odpowiedni interesariusze powinni wesprzeć proces opracowania oraz wdrożenia stosownych strategii łagodzących w celu zapewnienia kompleksowego rozwiązania.

Poziom(y): 3

CM-7 ZASADA MINIMALNEJ FUNKCJONALNOŚCI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Zasada minimalnej funkcjonalności ogranicza powierzchnię ataku. Podmioty powinny wybierać komponenty, które zapewniają elastyczność umożliwiającą specyfikację oraz wdrożenie minimalnych wymaganych funkcjonalności. Podmioty powinny zapewnić przestrzeganie zasady minimalizacji funkcjonalności w swoich systemach i sieciach informacyjnych oraz w całym cyklu życia systemu. Mechanizm zabezpieczenia rozszerzonego CM-7 (9) opisanego w dokumencie NSC 800-53 może zostać zastosowany do ochrony systemów informacyjnych i sieci przed podatnościami, które mogą zostać do niego wprowadzone przy pomocy nieautoryzowanych urządzeń podłączanych do systemów podmiotu. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 3

Zabezpieczenia rozszerzone:

1. *ZASADA MINIMALNEJ FUNKCJONALNOŚCI | PRZEGLĄD OKRESOWY*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Poziom(y): 2, 3

2. *ZASADA MINIMALNEJ FUNKCJONALNOŚCI | NIEAUTORYZOWANE OPROGRAMOWANIE*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny określić wymagania i wdrożyć odpowiednie procesy w celu wykrywania niedozwolonego oprogramowania. Jednym z działań wspomagających wdrożenie takiego rozwiązania jest wprowadzenie zakazu używania oprogramowania wątpliwej jakości lub nieautoryzowanego. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Poziom(y): 2, 3

3. *ZASADA MINIMALNEJ FUNKCJONALNOŚCI | AUTORYZOWANE OPROGRAMOWANIE*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny określić wymagania i wdrożyć odpowiednie procesy w celu określenia listy oprogramowania dopuszczonego do użytku. Jednym z działań wspomagających wdrożenie takiego rozwiązania jest wprowadzenie nakazu używania wyłącznie dozwolonego oprogramowania. Zasada ta może także obejmować wymagania dotyczące alertów w przypadku wprowadzenia do środowiska podmiotu nowego oprogramowania i jego aktualizacji. Przykładem takich wymagań jest dopuszczenie oprogramowania

otwartoźródłowego tylko wtedy, gdy kod jest dostępny do oceny przez podmiot i uznany za dopuszczalny do wykorzystania.

Poziom(y): 3

4. *ZASADA MINIMALNEJ FUNKCJONALNOŚCI | ŚRODOWISKA Z OGRANICZONYMI UPRAWNIENIAMI*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien zapewnić, że mechanizmy uwierzytelniania kodu, takie jak podpisy cyfrowe, są wykorzystywane podczas wykonywania kodu w celu zapewnienia integralności oprogramowania, oprogramowania sprzętowego i informacji w systemach informacyjnych i sieciach.

Poziom(y): 2, 3

5. *ZASADA MINIMALNEJ FUNKCJONALNOŚCI | OCHRONA INFORMACJI O MECHANIZMACH*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien uzyskać kod binarny lub kod źródłowy bezpośrednio od producenta, dewelopera lub z innego dopuszczalnego, zweryfikowanego źródła.

Poziom(y): 3

6. *ZASADA MINIMALNEJ FUNKCJONALNOŚCI | WYKONYWALNY KOD BINARNY LUB ŹRÓDŁOWY*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: W przypadku wyjątkowego dopuszczenia do użycia oprogramowania bez dołączonego kodu źródłowego i z ograniczoną gwarancją lub bez gwarancji ze względu na istotne wymogi związane z misją lub bieżącą działalnością, zgoda osoby zatwierdzającej powinna być uzależniona od wyraźnego włączenia przez podmiot oceny ryzyka dotyczącego cyberbezpieczeństwa w łańcuchu dostaw do szerszej oceny takiego oprogramowania, a także od wdrożenia środków bezpieczeństwa w celu uwzględnienia wszelkich zidentyfikowanych i ocenionych ryzyk.

Poziom(y): 2, 3

7. *ZASADA MINIMALNEJ FUNKCJONALNOŚCI | ZAKAZ UŻYWANIA NIEAUTORYZOWANEGO SPRZĘTU*

Podmioty powinny określić wymagania i wdrożyć odpowiednie procesy w celu wykrywania niedozwolonego sprzętu. Jednym z działań wspomagających wdrożenie takiego rozwiązania jest wprowadzenie zakazu używania sprzętu wątpliwej jakości lub nieautoryzowanego. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Poziom(y): 2, 3

CM-8 INWENTARYZACJA KOMPONENTÓW SYSTEMU

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zapewnić, że krytyczne komponenty systemów informacyjnych i sieci są uwzględnione w stosownych wykazach. Wykaz musi zawierać informacje dotyczące odpowiedzialności za kluczowe komponenty. Wykazy powinny obejmować na przykład specyfikacje sprzętu, informacje o licencjach na oprogramowanie, numery wersji oprogramowania, osoby odpowiedzialne, a także – w przypadku komponentów lub urządzeń sieciowych – nazwy urządzeń i ich adresy sieciowe. Specyfikacje mogą obejmować nazwę producenta, typ urządzenia, model, numer seryjny i fizyczną lokalizację. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom. Podmioty powinny określić wymogi oraz sposoby przepływu informacji zapewniające, że tylko wymagane informacje są przekazywane różnym uczestnikom łańcucha dostaw. Jeśli informacje są współdzielone i przekazywane kolejnym odbiorcom, powinny być opatrzone informacją na temat twórcy danego podzbioru. Podmioty powinny rozważyć sporządzenie specyfikacji materiałowych komponentów oprogramowania w przypadku stosownych klas oprogramowania, w tym oprogramowania komercyjnego, oprogramowania otwartoźródłowego oraz

oprogramowania opracowanego wewnątrz podmiotu. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *INWENTARYZACJA KOMPONENTÓW SYSTEMU: | AKTUALIZACJE PODCZAS INSTALACJI I USUWANIA*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podczas instalowania, aktualizowania lub usuwania systemu informacyjnego, komponentu systemu informacyjnego lub komponentu sieci podmiot powinien zaktualizować wykaz, aby zapewnić możliwość śledzenia krytycznych komponentów. Ponadto należy zaktualizować konfigurację systemu informacyjnego, aby zapewnić dokładność wykazu zabezpieczeń łańcucha dostaw, a następnie ponownie przeprowadzić proces ustalania poziomu bazowego.

Poziom(y): 3

2. *INWENTARYZACJA KOMPONENTÓW SYSTEMU | AUTOMATYZACJA UTRZYMANIA*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien wdrożyć zautomatyzowane mechanizmy utrzymania, aby zapewnić, że zmiany w wykazie elementów systemów informacyjnych oraz sieci są monitorowane pod kątem ich instalacji, aktualizacji i usuwania. Jeśli automatyczne utrzymanie jest przeprowadzane z uprzednio określoną częstotliwością i obejmuje automatyczne zestawianie istotnych informacji o stanie poszczególnych określonych elementów, podmiot powinien zapewnić, że aktualne informacje są dostępne dla odpowiednich zainteresowanych stron w celu ich przeglądu i oceny. Określona częstotliwość gromadzenia danych powinna być nieprzewidywalna, aby ograniczyć ryzyko obejścia mechanizmów bezpieczeństwa przez zagrożenie wewnętrzne.

Poziom(y): 3

3. *INWENTARYZACJA KOMPONENTÓW SYSTEMU | INFORMACJE O ROZLICZALNOŚCI*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien zapewnić, że informacje o rozliczalności są gromadzone w przypadku systemów informacyjnych i sieci. Informacje zawarte w wykazach elementów systemu i sieci powinny wskazywać osoby, które są odpowiedzialne za jego nabycie, a także użytkowników końcowych, w tym wszelki personel pomocniczy, który może zajmować się administracją lub używać danego systemu bądź komponentu.

Poziom(y): 3

4. *INWENTARYZACJA KOMPONENTÓW SYSTEMU | OCENIONE KONFIGURACJE I ZATWIERDZONE ODCHYLENIA*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Ocenione konfiguracje i zatwierdzone odchylenia muszą być udokumentowane i obserwowane. Wszelkie zmiany w bazowych konfiguracjach systemów informacyjnych i sieci wymagają przeglądu przez odpowiednich interesariuszy, aby zapewnić, że zmiany te nie spowodują zwiększenia narażenia na ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw.

Poziom(y): 3

5. *INWENTARYZACJA KOMPONENTÓW SYSTEMU | SCENTRALIZOWANE REPOZYTORIUM*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty mogą zdecydować się na wdrożenie scentralizowanych wykazów, które obejmują składniki wszystkich systemów informacyjnych podmiotu, sieci i ich komponentów. Scentralizowane repozytoria wykazów dają możliwość zwiększenia efektywności analizy systemów informacyjnych, sieci i ich komponentów. Takie repozytoria mogą również pomóc podmiotom w szybkim określeniu lokalizacji i osób

odpowiedzialnych za komponenty, które zostały skompromitowane, naruszone lub wymagają działań łagodzących. Podmiot powinien zapewnić, że scentralizowane repozytorium zawiera informacje dotyczące łańcucha dostaw, wymagane do właściwego rozliczania komponentów (np. znaczenie dla łańcucha dostaw, informacje o osobie odpowiedzialnej za system informacyjny, sieć lub komponent).

Poziom(y): 3

6. *INWENTARYZACJA KOMPONENTÓW SYSTEMU | AUTOMATYCZNE ŚLEDZENIE LOKALIZACJI*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Stosując zautomatyzowane mechanizmy śledzenia lokalizacji komponentów systemu informacyjnego według fizycznej lokalizacji, podmiot powinien uwzględnić potrzeby związane ze śledzeniem systemu informacyjnego, sieci i ich komponentów, aby zapewnić kompletność wykazu.

Poziom(y): 2, 3

7. *INWENTARYZACJA KOMPONENTÓW SYSTEMU | PRZYPISANIE KOMPONENTÓW DO SYSTEMÓW*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Przypisując komponenty do systemów, podmiot powinien zapewnić, że systemy informacyjne i sieci wraz ze wszystkimi istotnymi komponentami są zinwentaryzowane, oznaczone i odpowiednio przypisane. Takie rozwiązanie USPRAWNIA szybką inwentaryzację wszystkich komponentów istotnych dla systemów informacyjnych i sieci oraz umożliwia śledzenie komponentów, które są uważane za krytyczne i wymagają specjalnego traktowania w ramach działań związanych z ochroną systemów informacyjnych i sieci.

Poziom(y): 3

8. *INWENTARYZACJA KOMPONENTÓW SYSTEMU |SPECYFIKACJE MATERIAŁOWE KOMPONENTÓW OPROGRAMOWANIA DLA PROJEKTÓW OTWARTOŹRÓDŁOWYCH*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Jeżeli podmiot korzysta z projektu otwartoźródłowego, który nie posiada specyfikacji materiałowej komponentów oprogramowania wymaganej przez podmiot, rzeczony podmiot musi: 1) Opracować specyfikację materiałową komponentów oprogramowania dotyczącą projektu otwartoźródłowego; 2) Przeznaczyć środki na projekt w celu dodania tej informacji; bądź 3) Opracować specyfikację materiałową komponentów oprogramowania przy pierwszym użyciu każdej wersji projektu, z którego korzysta.

Poziom(y): 3

CM-9 PLAN ZARZĄDZANIA KONFIGURACJĄ

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zapewnić, że działania w obszarze C-SCRM zostaną uwzględnione w działaniach związanych z planowaniem zarządzania konfiguracją. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *PLAN ZARZĄDZANIA KONFIGURACJĄ | PRZYPISANIE ODPOWIEDZIALNOŚCI*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny określić wszystkie stosowne role związane z działaniami dotyczącymi zarządzania konfiguracją systemów informacyjnych i sieci. Podmioty powinny zapewnić, że wymagania i zdolności

w zakresie zarządzania konfiguracją są odpowiednio uwzględnione lub zawarte w następujących działaniach łańcucha dostaw: określenie wymagań, rozwój, testowanie, badania i analizy rynku, zamówienia publiczne i umowy, instalacja lub usunięcie komponentów, integracja systemu, eksploatacja i utrzymanie.

Poziom(y): 2, 3

CM-10 OGRANICZENIA W UŻYCIU OPROGRAMOWANIA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zapewnić, że licencje na oprogramowanie używane w ich systemach i sieciach informacyjnych są udokumentowane, śledzone i utrzymywane. Mechanizmy śledzenia powinny zapewniać możliwość śledzenia użytkowników i wykorzystania licencji w celu uzyskania informacji dotyczących dostępu oraz wdrożenia stosownych zabezpieczeń. Na przykład, gdy pracownik zostaje zwolniony, licencja użytkownika powinna zostać wycofana, a dokumentacja licencji powinna zostać zaktualizowana, aby odzwierciedlić tę zmianę. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *OGRANICZENIA W UŻYCIU OPROGRAMOWANIA | OPROGRAMOWANIE OTWARTOŹRÓDŁOWE*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Wybierając oprogramowanie, podmioty powinny przeanalizować wszystkie opcje i związane z nimi ryzyko, uwzględniając komponenty otwartoźródłowe oraz oprogramowanie komercyjne. W przypadku korzystania z oprogramowania otwartoźródłowego, podmiot powinien zrozumieć i przeanalizować typowe procedury związane z pochodzeniem, zarządzaniem konfiguracją, źródłami, plikami binarnymi, frameworkami, bibliotekami, dostępnością do użytku

i testowania obowiązujące w społecznościach rozwijających tego rodzaju oprogramowanie oraz wszelkie inne informacje, które mogą mieć wpływ na poziomy narażenia na ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw. Liczne rozwiązania otwartoźródłowe są obecnie wykorzystywane przez podmioty, między innymi w zintegrowanych środowiskach programistycznych (*ang. integrated development environments - IDE*) i serwerach internetowych. Podmiot powinien:

a. Śledzić wykorzystanie oprogramowania otwartoźródłowego i związanej z nim dokumentacji.

b. Zapewnić, że wykorzystanie oprogramowania otwartoźródłowego jest zgodne z warunkami licencjonowania i że warunki te są akceptowalne dla podmiotu.

c. Zapewnić dokumentowanie i monitorowanie dystrybucji oprogramowania w odniesieniu do umowy licencyjnej w celu kontroli kopiowania i dystrybucji oraz

d. Oceniać i okresowo kontrolować łańcuch dostaw oprogramowania otwartoźródłowego twórcy oprogramowania (np. informacje dotyczące pochodzenia, zarządzania konfiguracją, wykorzystania bibliotek wielokrotnego użytku itp.) Oceny tej można dokonać poprzez pozyskanie istniejących i często ogólnodostępnych dokumentów, a także wykorzystanie doświadczeń opartych na procesach aktualizacji i pobierania oprogramowania, w których podmiot mógł uczestniczyć.

Poziom(y): 2, 3

CM-11 OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Ten środek bezpieczeństwa obejmuje użytkowników systemu informacyjnego podmiotu oraz sieci, którzy nie są zatrudnieni przez podmiot.

Użytkownikami tymi mogą być dostawcy, deweloperzy, integratorzy systemów, dostawcy zewnętrznych usług systemowych oraz inni dostawcy usług związanych z ICT/OT.

Poziom(y): 2, 3

CM-12 POŁOŻENIE (LOKACJA) INFORMACJI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Informacji znajdujących się w różnych lokalizacjach fizycznych mogą dotyczyć różne zagrożenia dla cyberbezpieczeństwa w całym łańcuchu dostaw, w zależności od konkretnej lokalizacji tych informacji. Komponenty, które pochodzą lub które zostały zainstalowane w różnych lokalizacjach fizycznych mogą również podlegać różnym ryzykom związanym z łańcuchem dostaw, w zależności od konkretnej lokalizacji pochodzenia lub instalacji. Podmioty powinny zarządzać tym ryzykiem poprzez kontrolę dostępu i określenie dozwolonych lub niedozwolonych lokalizacji geograficznych dla tworzenia kopii zapasowych/odzyskiwania danych, instalacji poprawek/aktualizacji oraz przesyłania/współdzielenia informacji. Mechanizm zabezpieczenia rozszerzonego CM-12 (1) opisanego w dokumencie NSC 800-53, można wykorzystać w celu umożliwienia automatycznej lokalizacji komponentów.

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *POŁOŻENIE (LOKACJA) INFORMACJI | ZAUTOMATYZOWANE NARZĘDZIA WSPIERAJĄCE LOKALIZACJĘ INFORMACJI*

Należy stosować zautomatyzowane narzędzia do identyfikacji informacji w komponentach systemu podmiotu w celu zapewnienia, że odpowiednie środki bezpieczeństwa są wykorzystywane w celu ochrony informacji podmiotu i prywatności osób.

Poziom(y): 2, 3

CM-13 MAPOWANIE DZIAŁAŃ NA DANYCH

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Oprócz działań na danych osobowych, konieczne jest zrozumienie i udokumentowanie działań na danych systemowych dotyczących informacji wrażliwych lub niejawnych. Mapowanie działań na danych powinno być również prowadzone w celu mapowania urządzeń Internetu rzeczy (*ang. Internet of Things - IoT*), wbudowanych lub samodzielnych systemów IoT lub działań na danych systemu IoT. Zrozumienie, jakie informacje niejawne lub informacje IoT są przetwarzane, poziom ich wrażliwości oraz wpływ na środowisko fizyczne, a także sposób przetwarzania informacji wrażliwych lub IoT (np. czy działania na danych są widoczne dla osób lub czy dane są przetwarzane w innej części systemu) oraz informacje na temat osób odpowiedzialnych za działania pozwalają na ustalenie niezbędnego kontekstu kluczowego dla oceny stopnia ryzyka. Mapy danych mogą być ilustrowane na różne sposoby, a poziom szczegółowości może być różny w zależności od misji i potrzeb biznesowych podmiotu. Mapa danych może być nakładką na dowolny artefakt systemu, z którego korzysta podmiot. Opracowanie tej mapy może wymagać koordynacji między pracownikami odpowiedzialnymi za program i bezpieczeństwo w odniesieniu do działań związanych z danymi objętymi ochroną oraz składników, które stanowią część systemu.

Poziom(y): 2, 3

CM-14 PODPISYWANIE KOMPONENTÓW

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zweryfikować, czy nabyte komponenty sprzętu i oprogramowania są autentyczne przy pomocy cyfrowych podpisów pochodzących z zaufanych urzędów certyfikacji. Weryfikacja komponentów przed zezwoleniem na instalację pomaga podmiotom zmniejszyć ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw.

Poziom(y): 3

KATEGORIA CP: PLANOWANIE AWARYJNE / CIĄGŁOŚĆ DZIAŁANIA

Dokument [NSC 200] określa minimalne wymagania bezpieczeństwa w zakresie planowania awaryjnego w następujący sposób:

> *Organizacje powinny ustanawiać, utrzymywać i skutecznie wdrażać plany reagowania w sytuacjach awaryjnych. Do tych działań należą: tworzenie kopii zapasowych danych i odzyskiwanie ich po awarii dla organizacyjnych systemów informacyjnych. Ma to zapewnić dostępność krytycznych zasobów informacyjnych i ciągłość operacji w sytuacjach awaryjnych.*

Plan ciągłości działania dotyczące cyberbezpieczeństwa w łańcuchu dostaw obejmuje planowanie skorzystania z usług alternatywnych dostawców komponentów systemu, alternatywnych dostawców systemów i usług, alternatywnych tras dostaw krytycznych komponentów systemu oraz uwzględnia ataki typu denial-of-service (DoS) na łańcuch dostaw. Takie plany awaryjne pomagają zapewnić, że istniejący dostawcy usług wdrożyli skuteczne plany utrzymania ciągłości działalności, zwłaszcza gdy dostawca świadczy usługi wspierające kluczowe piony realizujące misję podmiotu. Ponadto wiele technik stosowanych w planowaniu awaryjnym, takich jak alternatywne miejsca przetwarzania, obejmuje dodatkowe łańcuchy dostaw z towarzyszącymi im zagrożeniami dla cyberbezpieczeństwa. Podmioty powinny zapewnić, że rozumieją ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw oraz zależności związane z działaniami w zakresie planowania awaryjnego.

CP-1 POLITYKA I PROCEDURY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny włączyć działania w zakresie C-SCRM do polityki planowania awaryjnego oraz strategii i planu wdrożenia zarządzania ryzykiem w łańcuchu dostaw, a także polityki oraz planu zarządzania ryzykiem w łańcuchu dostaw. Polityka powinna obejmować systemy informacyjne i sieć łańcucha dostaw oraz opisywać scenariusze obejmujące co najmniej następujące sytuacje:

a. Awaria komponentów i ich późniejsza wymiana;

b. Planowana wymiana związana z ulepszeniami, konserwacją, uaktualnieniami i modernizacją; oraz

c. Zakłócenia w funkcjonowaniu produktu i/lub usługi.

Poziom(y): 1, 2, 3

CP-2 PLAN CIĄGŁOŚCI DZIAŁANIA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny określić i wdrożyć plan awaryjny dla systemów informacyjnych i sieci łańcucha dostaw, aby zapewnić przygotowanie do złagodzenia skutków utraty danych lub zakłócenia działania systemu. Należy wprowadzić mechanizmy awaryjne dla łańcucha dostaw, sieci, systemów informacyjnych (zwłaszcza ich komponentów krytycznych) i procesów, aby zapewnić ochronę przed naruszeniem zasad ochrony i zapewnić odpowiednie przełączanie awaryjne i terminowe przywracanie do akceptowalnego stanu.

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *PLAN CIĄGŁOŚCI DZIAŁANIA | KOORDYNACJA Z POWIĄZANYMI PLANAMI*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Należy skoordynować proces opracowywania planów awaryjnych w zakresie ryzyka związanego z łańcuchem dostaw z interesariuszami podmiotu odpowiedzialnymi za powiązane plany.

Poziom(y): 2, 3

2. *PLAN CIĄGŁOŚCI DZIAŁANIA | PLANOWANIE ALTERNATYW*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: To zabezpieczenie rozszerzone zwiększa dostępność sieci łańcucha dostaw lub komponentów systemu informacyjnego.

Poziom(y): 2, 3

3. *PLAN CIĄGŁOŚCI DZIAŁANIA | KOORDYNACJA Z DOSTAWCAMI ZEWNĘTRZNYCH USŁUG*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zapewnić, by sieć łańcucha dostaw, systemy informacyjne i komponenty dostarczane przez dostawcę zewnętrznych usług były odpowiednio zabezpieczone przed awarią (personel, sprzęt i zasoby sieciowe) w celu ograniczania lub zapobiegania przerwom w świadczeniu usług lub zapewnienia terminowego przywrócenia sprawności. Podmioty powinny zapewnić, że wymagania dotyczące planowania awaryjnego są zdefiniowane jako część umowy gwarancji świadczenia usług. Umowa może zawierać szczegółowe warunki, które dotyczą krytycznych komponentów i wsparcia funkcjonalności w przypadku ataków typu DoS w celu zapewnienia ciągłości operacji. Podmioty powinny koordynować działania z dostawcami zewnętrznych usług, aby określić istniejące praktyki dostawców w zakresie planów awaryjnych i rozwinąć je zgodnie z misją podmiotu i jego potrzebami biznesowymi. Taka koordynacja pomoże w obniżeniu kosztów i skutecznym wdrożeniu. Podmioty powinny wymagać od swoich głównych wykonawców, którzy dostarczają usługi lub produkty o znaczeniu krytycznym dla misji i działalności lub umożliwiające jej prowadzenie, wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Poziom(y): 3

4. *PLAN CIĄGŁOŚCI DZIAŁANIA | OKREŚLENIE KRYTYCZNYCH ZASOBÓW*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Należy określić krytyczne zasoby (w tym sprzęt, oprogramowanie i personel) oraz opracować i wdrożyć odpowiednie wymogi planowania awaryjnego

w celu zapewnienia ciągłości działalności. Kluczowym krokiem w tym procesie jest przeprowadzenie analizy krytyczności komponentów, funkcji i procesów w celu określenia wszystkich krytycznych zasobów. Dodatkowe wskazówki dotyczące analiz krytyczności znajdują się w rozdziale 2 oraz w dokumencie NISTIR 8179.

Poziom(y): 3

CP-3 SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zadbać o to, aby krytyczni dostawcy zostali objęci szkoleniami dotyczącymi postępowania w przypadku awarii. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA | SYMULOWANE ZDARZENIA*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zapewnić, że dostawcy, deweloperzy, integratorzy systemów, dostawcy zewnętrznych usług systemowych oraz inni dostawcy usług związanych z ICT/OT, których role i obowiązki wiążą się ze świadczeniem usług krytycznych, są uwzględniani w ćwiczeniach i szkoleniach dotyczących sytuacji awaryjnych.

Poziom(y): 3

CP-4 TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zapewnić, że krytyczni dostawcy są objęci testami dotyczącymi sytuacji

awaryjnych. Podmiot - w porozumieniu z dostawcą (dostawcami) usług - powinien przetestować możliwości zapewnienia ciągłości oraz odporność, w tym między innymi przełączenie awaryjne podstawowej lokalizacji produkcyjnej do lokalizacji zapasowej. Testy te mogą być prowadzone niezależnie od szkoleń lub w ich trakcie. Podmioty powinny odwoływać się do wyników oceny zagrożeń C-SCRM, aby opracować scenariusze, które pozwolą sprawdzić wytrzymałość podmiotu oraz przywrócenie pełnej sprawności po wystąpieniu zagrożenia C-SCRM.

Poziom(y): 2, 3

CP-6 ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Alternatywne miejsca przechowywania danych zarządzane przez dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych i innych dostawców usług związanych z ICT/OT są uwzględniane jako część sieci łańcucha dostaw podmiotu. Podmioty powinny stosować odpowiednie środki bezpieczeństwa dotyczącego cyberbezpieczeństwa w łańcuchu dostaw w odniesieniu do tych miejsc przechowywania danych.

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII | ODDZIELENIE OD GŁÓWNEGO MAGAZYNU*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: To zabezpieczenie rozszerzone zwiększa odporność sieci łańcucha dostaw, systemu informacyjnego lub komponentów systemu informacyjnego.

Poziom(y): 2, 3

CP-7 ZAPASOWE MIEJSCE PRZETWARZANIA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Alternatywne miejsca przetwarzania danych zarządzane przez dostawców, deweloperów,

integratorów systemów, dostawców zewnętrznych usług systemowych i innych dostawców usług związanych z ICT/OT są uwzględniane jako część sieci łańcucha dostaw podmiotu. Podmioty powinny stosować odpowiednie środki bezpieczeństwa dotyczącego cyberbezpieczeństwa w łańcuchu dostaw w odniesieniu do tych miejsc przetwarzania danych.

Poziom(y): 2, 3

CP-8 USŁUGI TELEKOMUNIKACYJNE

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny włączyć do swojego łańcucha dostaw alternatywnych dostawców usług telekomunikacyjnych w celu wsparcia krytycznych systemów informacyjnych.

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *USŁUGI TELEKOMUNIKACYJNE | ROZDZIELENIE DOSTAWCÓW GŁÓWNYCH I ALTERNATYWNYCH*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Rozdzielenie dostawców głównych i alternatywnych wspiera odporność łańcucha dostaw na zagrożenia związane z cyberbezpieczeństwem.

Poziom(y): 2, 3

2. *USŁUGI TELEKOMUNIKACYJNE | PLAN CIĄGŁOŚCI DZIAŁANIA DOSTAWCY*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: W przypadku działań dotyczących obszaru C-SCRM plany awaryjne powinny zapewniać rozdzielenie infrastruktury, usług, procesów i personelu dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT.

Poziom(y): 2, 3

CP-11 ALTERNATYWNE PROTOKOŁY KOMUNIKACJI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zapewnić, że najważniejsi dostawcy zostaną uwzględnieni w planach awaryjnych, szkoleniach i testach w ramach włączania alternatywnych protokołów komunikacyjnych w celu zapewnienia odporności łańcucha dostaw.

Poziom(y): 2, 3

KATEGORIA IA: IDENTYFIKACJA I UWIERZYTELNIANIE

Dokument [NSC 200] określa minimalne wymagania bezpieczeństwa w zakresie identyfikacji i uwierzytelniania w następujący sposób:

> *Organizacje powinny identyfikować użytkowników systemu informacyjnego, procesy działające w imieniu użytkowników lub urządzenia oraz uwierzytelniać (lub weryfikować) tożsamości tych użytkowników, procesów lub urządzeń, jako wymóg zasadniczy umożliwiający dostęp do organizacyjnych systemów informacyjnych.*

Dokument NSC 800-161*s* rozszerza rodzinę środków zabezpieczających dotyczących identyfikacji i uwierzytelniania opisanych w dokumencie [NSC 200] o identyfikację i uwierzytelnianie komponentów, poza uwierzytelnianiem osób (użytkowników) i procesów działających w imieniu osób w sieci łańcucha dostaw. Identyfikacja i uwierzytelnianie mają kluczowe znaczenie dla działań w zakresie C-SCRM, ponieważ zapewniają możliwość śledzenia osób, procesów działających w imieniu osób oraz określonych systemów i ich komponentów w sieci łańcucha dostaw podmiotu. Identyfikacja i uwierzytelnianie są wymagane do odpowiedniego zarządzania ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw, aby zarówno zmniejszyć ryzyko naruszenia cyberbezpieczeństwa łańcucha dostaw, jak i wygenerować dowody w przypadku naruszenia cyberbezpieczeństwa łańcucha dostaw.

IA-1 POLITYKA I PROCEDURY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien - w określonych przez siebie odstępach czasu, dokonywać przeglądu, udoskonalać i aktualizować swoje polityki i procedury zarządzania tożsamością i dostępem, aby zapewnić, że krytyczne role i procesy w sieci łańcucha dostaw zostały określone oraz że krytyczne systemy, komponenty i procesy podmiotu zostały zidentyfikowane w celu zapewnienia identyfikowalności. Powinno to obejmować określenie komponentów krytycznych, które w przeszłości mogły nie być uwzględnione w ramach procesów identyfikacji i uwierzytelniania. Należy pamiętać, że zapewnienie identyfikacji dla wszystkich produktów

w łańcuchu dostaw może być nieopłacalne, dlatego należy dokonać świadomego wyboru. Podmiot powinien zaktualizować odpowiednie plany wdrożenia oraz strategie C-SCRM, a także politykę oraz plany C-SCRM.

Poziom(y): 1, 2, 3

IA-2 IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI)

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zapewnić określenie i stosowanie identyfikacji i wymogów dla użytkowników podmiotu mających dostęp do systemu ICT/OT lub sieci łańcucha dostaw. Użytkownikami mogą być pracownicy, osoby o statusie równoważnym do pracowników (np. wykonawcy, gościnni naukowcy itp.) oraz integratorzy systemów pełniący funkcje wykonawcze. Kryteria takie jak czas pracy na danym stanowisku mogą pomóc w określeniu, jakie mechanizmy identyfikacji i uwierzytelniania powinny być stosowane. Podmiot może zdecydować się na określenie zestawu ról i powiązanie poziomu uprawnień w celu zapewnienia właściwego wdrożenia tego zabezpieczenia. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 1, 2, 3

IA-3 IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny wdrożyć możliwości dokładnej i pozytywnej identyfikacji urządzeń i oprogramowania w ramach swojego łańcucha dostaw, a po zidentyfikowaniu zweryfikować, czy ich tożsamość jest autentyczna. Urządzenia, które wymagają unikalnej identyfikacji i uwierzytelniania między urządzeniami, powinny być zdefiniowane według typu, urządzenia lub połączenia typu i urządzenia. Oprogramowanie wymagające

uwierzytelnienia powinno być identyfikowane za pomocą znacznika identyfikacji oprogramowania (*ang. software identification tag - SWID*), który umożliwia weryfikację pakietu oprogramowania oraz uwierzytelnienie podmiotu wydającego pakiet oprogramowania.

Poziom(y): 1, 2, 3

IA-4 ZARZĄDZANIE IDENTYFIKATOREM

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Identyfikatory umożliwiają większą wykrywalność i identyfikowalność. W ramach łańcucha dostaw podmiotu identyfikatory powinny być przypisane do systemów, osób, dokumentacji, urządzeń i komponentów. W niektórych przypadkach identyfikatory mogą być utrzymywane przez cały cykl życia systemu, od koncepcji do wycofania z użytku, jednak powinny co najmniej obejmować cały okres funkcjonowania systemu w podmiocie.

W przypadku rozwoju oprogramowania identyfikatory powinny być przydzielane dla komponentów, które stanowią element konfiguracji. W przypadku urządzeń i systemów operacyjnych identyfikatory powinny być przypisane w momencie, gdy wchodzą do łańcucha dostaw podmiotu, np. gdy są przekazywane na własność podmiotu lub pod jego kontrolę poprzez wysyłkę i odbiór lub poprzez pobranie.

Dostawcy, deweloperzy, integratorzy systemów, dostawcy zewnętrznych usług systemowych i inni dostawcy usług związanych z ICT/OT zazwyczaj używają własnych identyfikatorów do celów śledzenia w ramach własnego łańcucha dostaw. Podmioty powinny skorelować te identyfikatory z identyfikatorami przypisanymi przez siebie w celu zapewnienia identyfikowalności i rozliczalności. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

Powiązane środki bezpieczeństwa: IA-3 (1), IA-3 (2), IA-3 (3) oraz IA-3 (4)

Zabezpieczenia rozszerzone:

1. *ZARZĄDZANIE IDENTYFIKATOREM | ZARZĄDZANIE MIĘDZYORGANIZACYJNE*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: To zabezpieczenie rozszerzone zwiększa identyfikowalność i ułatwia potwierdzenie pochodzenia komponentów w ramach łańcucha dostaw poprzez koordynację zarządzania identyfikatorami przez podmiot i jego dostawców, twórców, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT. Obejmuje systemy informacyjne i ich komponenty, a także osoby zaangażowane w działania w ramach łańcucha dostaw.

Poziom(y): 1, 2, 3

IA-5 ZARZĄDZANIE METODAMI UWIERZYTELNIANIA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Ten środek bezpieczeństwa wspiera identyfikowalność i niezaprzeczalność w całym łańcuchu dostaw. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | ZMIANA DANYCH UWIERZYTELNIAJĄCYCH PRZED DOSTAWĄ*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: To zabezpieczenie rozszerzone zapewnia weryfikację łańcucha dowodowego w ramach łańcucha dostaw podmiotu.

Poziom(y): 3

2. *ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | SFEDEROWANE ZARZĄDZANIE POŚWIADCZENIAMI*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: To zabezpieczenie rozszerzone zapewnia weryfikację pochodzenia oraz łańcucha dowodowego w ramach łańcucha dostaw podmiotu.

Poziom(y): 3

IA-8 IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI)

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Dostawcy, deweloperzy, integratorzy systemów, dostawcy zewnętrznych usług systemowych oraz inni dostawcy usług związanych z ICT/OT mogą wchodzić w kontakt z łańcuchem dostaw podmiotu w celu świadczenia usług (np. usług rozwojowych/integracyjnych, wsparcia produktów itp.) Podmioty powinny zarządzać ustanawianiem, kontrolą, stosowaniem i odwoływaniem poświadczeń identyfikacyjnych oraz uwierzytelnianiem użytkowników spoza podmiotu w ramach łańcucha dostaw. Podmioty powinny również zapewnić szybką realizację czynności związanych z identyfikacją i uwierzytelnianiem, zwłaszcza w przypadku cofania poświadczeń, aby pomóc ograniczyć ekspozycję na ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw, takie jak te, które powstają w wyniku zagrożeń wewnętrznych.

Poziom(y): 2, 3

IA-9 IDENTYFIKACJA I UWIERZYTELNIANIE USŁUG

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zapewnić, że identyfikacja i uwierzytelnianie są zdefiniowane i zarządzane w odniesieniu do dostępu do usług (np. aplikacji internetowych wykorzystujących certyfikaty cyfrowe, usług lub aplikacji, które wysyłają zapytania do bazy danych) w całym łańcuchu dostaw. Podmioty powinny upewnić się, że wiedzą, jakie usługi są zamawiane i od których dostawców.

Usługi będące przedmiotem zamówienia powinny być wymienione w zatwierdzonym wykazie usług dla podmiotu lub powinny obejmować stosowne środki bezpieczeństwa. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

KATEGORIA IR: REAGOWANIE NA INCYDENTY

Dokument [NSC 200] określa minimalne wymagania bezpieczeństwa w zakresie reagowania na incydenty w następujący sposób:

> *Organizacje powinny: (I) ustanowić operacyjną zdolność obsługi incydentów dla organizacyjnych systemów informacyjnych, która obejmuje odpowiednie przygotowanie, wykrywanie, analizę, powstrzymywanie, odzyskiwanie i działania związane z reagowaniem na potrzeby użytkownika; oraz (II) śledzić, dokumentować i zgłaszać incydenty odpowiednim organom.*

Naruszenie zasad ochrony łańcucha dostaw może obejmować każdą z następujących grup – dostawcy, deweloperzy, integratorzy systemów, dostawcy zewnętrznych usług systemowych raz dostawców innych usług dotyczących ICT/OT. Podmioty powinny zapewnić, by ich mechanizmy zabezpieczeń w zakresie reagowania na incydenty uwzględniały obszar C-SCRM, w tym informacje na temat tego, w jaki sposób, kiedy i komu będą zgłaszane incydenty lub które informacje będą udostępniane przez dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych, innych dostawców usług związanych z ICT/OT oraz wszelkie właściwe organy międzyorganizacyjne, a także udostępniane wyżej wymienionym podmiotom lub wymieniane pomiędzy nimi. Reagowanie na incydenty pomoże określić, czy dany incydent jest związany z łańcuchem dostaw.

IR-1 POLITYKA I PROCEDURY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny włączyć zagadnienia dotyczące obszaru C-SCRM do polityki i procedur reagowania na incydenty oraz powiązanych planów, polityk strategii oraz planów wdrożenia C-SCRM. Polityka i procedury muszą zawierać wytyczne dotyczące sposobu reagowania na incydenty związane z łańcuchem dostaw oraz incydenty związane z cyberbezpieczeństwem, które mogą skomplikować łańcuch dostaw lub wpłynąć na jego działanie. Osoby pracujące w określonych środowiskach związanych z realizacją misji lub konkretnymi systemami muszą rozpoznawać incydenty dotyczące

cyberbezpieczeństwa w łańcuchu dostaw. Polityki reagowania na incydenty powinny określać, kiedy i w jaki sposób zagrożenia i incydenty powinny być obsługiwane, zgłaszane i zarządzane.

Dodatkowo polityka powinna określać zasady, właściwe osoby oraz sposoby komunikacji z innymi zainteresowanymi stronami lub partnerami w ramach szerszego łańcucha dostaw w przypadku zagrożenia lub incydentu związanego z cyberbezpieczeństwem. Podmioty publiczne muszą przekazywać informacje na temat ryzyka związanego z łańcuchem dostaw, gdy uprawniony podmiot zwróci się o informacje dotyczące konkretnego źródła, artykułu objętego zabezpieczeniem lub zamówienia, lub gdy organ wykonawczy ustali, że istnieje uzasadniona podstawa do stwierdzenia, że istnieje znaczne ryzyko związane z łańcuchem dostaw w odniesieniu do źródła, zamówienia lub artykułu objętego zabezpieczeniem.

Dwukierunkowa komunikacja z partnerami z łańcucha dostaw powinna być określona w umowach z dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych i innymi dostawcami usług związanych z ICT/OT w celu poinformowania wszystkich zaangażowanych stron o incydencie dotyczącym cyberbezpieczeństwa łańcucha dostaw. Informacje o incydentach mogą być również udostępniane w stosownych przypadkach uprawnionym podmiotom takim jak sądy, prokuratura, Policja, ABW CSIRT poziomu krajowego.
W zależności od powagi zdarzenia może zaistnieć potrzeba przyspieszonej komunikacji w ramach łańcucha dostaw. Należy zawrzeć odpowiednie umowy z dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych i innymi dostawcami usług związanych z ICT/OT, aby zapewnić szybkość komunikacji, reakcji, działań naprawczych i innych powiązanych działań. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Na poziomach 2 i 3 należy wprowadzić procedury i metody reagowania na incydenty specyficzne dla danego podmiotu, przeprowadzić szkolenia (należy rozważyć uwzględnienie w szkoleniach bezpieczeństwa operacyjnego [*ang. Operations Security - OPSEC*] i wszelkich stosownych informacji o zagrożeniach) oraz ustanowić skoordynowaną komunikację w całym łańcuchu dostaw w celu zapewnienia skutecznych i skoordynowanych działań w zakresie reagowania na incydenty.

Poziom(y): 1, 2, 3

Zabezpieczenia rozszerzone:

1. *POLITYKA I PROCEDURY | WYMIANA INFORMACJI O INCYDENTACH C-SCRM*

Podmioty powinny zapewnić, że ich polityki i procedury reagowania na incydenty zawierają wytyczne dotyczące skutecznej wymiany informacji o incydentach i innych kluczowych wskaźnikach ryzyka w łańcuchu dostaw. Wytyczne powinny obejmować co najmniej gromadzenie, zestawianie i dystrybucję informacji o incydentach z różnych źródeł danych, takich jak publiczne repozytoria danych, płatne usługi subskrypcyjne oraz wewnętrzne zespoły ds. analizy zagrożeń.

Podmioty działające w sektorze publicznym powinny określić szczegółowe wytyczne dotyczące zasad komunikacji w ramach
Poziom(y): 1, 2, 3

IR-2 SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zapewnić, że krytyczni dostawcy są objęci szkoleniami z zakresu reagowania na incydenty. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

IR-3 TESTOWANIE REAGOWANIA NA INCYDENTY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zapewnić, że krytyczni dostawcy uczestniczą w testach reagowania na incydenty lub że korzystają z takich możliwości.

Poziom(y): 2, 3

IR-4 OBSŁUGA INCYDENTÓW

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podejrzane zdarzenia w zakresie cyberbezpieczeństwa w łańcuchu dostaw, powinny uruchomić procesy obsługi incydentów C-SCRM w organizacji. Więcej informacji zawiera Załącznik G, w tym zadanie 3.4 obejmujące przykłady incydentów w łańcuchu dostaw. Dodatkowe wytyczne dotyczące wyłącznie obszaru C-SCRM zostały przedstawione w formie zabezpieczeń rozszerzonych.

Poziom(y): 1, 2, 3

Zabezpieczenia rozszerzone:

1. *OBSŁUGA INCYDENTÓW | ZAGROŻENIA WEWNĘTRZNE*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: To zabezpieczenie rozszerzone pozwala na ograniczenie narażenia systemów informacyjnych, sieci i procesów związanych z obszarem C-SCRM na zagrożenia wewnętrzne. Podmioty powinny zapewnić, aby możliwości obsługi incydentów związanych z zagrożeniami wewnętrznymi uwzględniały potencjalne zagrożenia wewnętrzne związane z dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych oraz innymi pracownikami dostawców usług związanych z ICT/OT, którzy mają dostęp do systemów ICT/OT w ramach granicy autoryzacji.

Poziom(y): 1, 2, 3

2. *OBSŁUGA INCYDENTÓW | ZAGROŻENIA WEWNĘTRZNE WEWNĄTRZ ORGANIZACJI*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: To zabezpieczenie rozszerzone pozwala na ograniczenie narażenia systemów informacyjnych, sieci i procesów związanych z obszarem C-SCRM na zagrożenia wewnętrzne. Podmioty powinny zapewnić koordynację działań dotyczących zagrożeń wewnętrznych ze swoimi dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych oraz innymi dostawcami usług związanych z ICT/OT.

Poziom(y): 1, 2, 3

3. *OBSŁUGA INCYDENTÓW | KOORDYNACJA ŁAŃCUCHA DOSTAW*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: W zarządzanie incydentami w zakresie bezpieczeństwa łańcucha dostaw i reagowanie na nie może być zaangażowanych wiele podmiotów. Po wstępnej analizie incydentu i podjęciu decyzji o sposobie działania (w niektórych przypadkach może to być także brak działania), podmiot może być zmuszony do koordynacji działań ze swoimi dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych, innymi dostawcami usług związanych z ICT/OT oraz wszelkimi właściwymi organami w celu prowadzenia komunikacji, usprawnienia reagowania na incydent, ustalenia przyczyn źródłowych i podjęcia działań naprawczych. Podmioty powinny udostępniać informacje w sposób bezpieczny wykorzystując w tym celu wyznaczony zespół pracowników na kluczowych stanowiskach, aby umożliwić bardziej kompleksowe podejście do obsługi incydentów. Wybór dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych i innych usługodawców związanych z ICT/OT posiadających stosowne możliwości obsługi incydentów związanych

z cyberbezpieczeństwem w łańcuchu dostaw jest istotny dla zmniejszenia narażenia na ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw. Jeśli przejrzystość obsługi incydentów jest ograniczona ze względu na charakter relacji, należy określić w umowie zestaw dopuszczalnych kryteriów. Zaleca się przegląd (i ewentualną zmianę) umowy w oparciu o wnioski wyciągnięte z poprzednich incydentów. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Poziom(y): 2

4. *OBSŁUGA INCYDENTÓW | ZINTEGROWANY ZESPÓŁ REAGOWANIA NA INCYDENTY*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien włączyć zespół zajmujący się badaniem incydentów lub odpowiednie kompetencje w tym zakresie do zintegrowanego zespołu reagowania na incydenty w łańcuchu dostaw. W sytuacjach, gdzie jest to wymagane i praktyczne, zintegrowane zespoły reagowania na incydenty powinny również obejmować pracowników z wielu regionów geograficznych, a także innych interesariuszy, takich jak dostawcy, deweloperzy, integratorzy systemów, dostawcy zewnętrznych usług systemowych oraz inni dostawcy usług związanych z ICT/OT.

Poziom(y): 3

IR-5 MONITOROWANIE INCYDENTÓW

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny dopilnować, aby umowy z dostawcami zawierały wymogi dotyczące śledzenia i dokumentowania incydentów, decyzji dotyczących reagowania oraz podjętych działań.

Poziom(y): 2, 3

IR-6 ZGŁASZANIE INCYDENTÓW

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Dodatkowe wytyczne dotyczące wyłącznie obszaru C-SCRM zostały przedstawione w formie zabezpieczenia rozszerzonego IR-6(3) w publikacji NSC 800-53.

Poziom(y): 3

Zabezpieczenia rozszerzone:

1. *ZGŁASZANIE INCYDENTÓW | KOORDYNACJA ŁAŃCUCHA DOSTAW*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Informacje o incydentach bezpieczeństwa przekazywane przez podmiot do dostawców, twórców oprogramowania, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT i w drugą stronę wymagają ochrony. Podmiot powinien zapewnić, że informacje są przeglądane i zatwierdzane przed ich przekazaniem na podstawie umów z dostawcami i wszelkimi odpowiednimi organami. Wszelkie eskalacje lub wyjątki od tej zasady powinny być jasno określone w umowie. Podmiot powinien zapewnić, że dane dotyczące incydentów są odpowiednio chronione i upewnić się, że przesyłać i odbierać je mogą wyłącznie upoważnione osoby. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Poziom(y): 3

IR-7 WSPARCIE REAGOWANIA NA INCYDENTY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Dodatkowe wytyczne dotyczące wyłącznie obszaru C-SCRM zostały przedstawione w formie zabezpieczenia rozszerzonego IR-7(2) w publikacji NSC 800-53.

Poziom(y): 3

Zabezpieczenia rozszerzone:

1. *POMOC W REAGOWANIU NA INCYDENTY | KOORDYNACJA Z DOSTAWCAMI ZEWNĘTRZNYMI*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Umowy podmiotu z głównymi wykonawcami powinny określać warunki, w których dopuszczony lub wyznaczony przez rząd podmiot zewnętrzny będzie w stanie zaoferować lub będzie zobowiązany do zapewnienia pomocy w reagowaniu na incydenty, jak również zadania i zakres odpowiedzialności tego podmiotu.

Poziom(y): 3

IR-8 PLAN REAGOWANIA NA INCYDENTY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny koordynować, opracować i wdrożyć plan odpowiedzi na incydenty, który obejmuje obowiązki w zakresie wymiany informacji z najważniejszymi dostawcami oraz podmiotami ujętymi w stosownych przepisach prawnych. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Powiązane środki bezpieczeństwa: IR-10

Poziom(y): 2, 3

IR-9 REAKCJA NA WYCIEK / UJAWNIENIE INFORMACJI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Łańcuch dostaw jest narażony na wyciek informacji. Podmiot powinien uwzględnić wycieki informacji związanych z łańcuchem dostaw w szerszym planie reagowania na wycieki informacji. To może wymagać koordynacji działań z każdą z następujących grup – dostawcy, deweloperzy, integratorzy systemów, dostawcy zewnętrznych usług systemowych raz dostawców innych usług dotyczących ICT/OT. Szczegóły dotyczące koordynacji

powinny być zawarte w umowie. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Poziom(y): 3

Powiązane środki bezpieczeństwa: SA-4

KATEGORIA MA: UTRZYMANIE I WSPARCIE

Dokument [NSC 200] określa minimalne wymagania bezpieczeństwa w zakresie utrzymania w następujący sposób:

> *Organizacje powinny: (I) przeprowadzać okresową i terminową obsługę organizacyjnych systemów informacyjnych; oraz (II) zapewniać skuteczne zabezpieczenia narzędzi, technik, mechanizmów i personelu wykorzystywanego do przeprowadzania konserwacji systemu informacyjnego.*

Utrzymanie jest usługą wykonywaną w wielu przypadkach przez jednostki, które nie wchodzą w skład struktur podmiotu. W związku z tym utrzymanie staje się częścią łańcucha dostaw. Procesy utrzymania obejmują wykonywanie aktualizacji i wymiany komponentów. Zasady oraz działania dotyczące obszaru C-SCRM należy stosować w sytuacjach związanych z utrzymaniem, w tym oceniać narażenie na ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw, wybierać środki bezpieczeństwa związane z obszarem C-SCRM, wdrażać te środki bezpieczeństwa i monitorować ich skuteczność.

MA-1 POLITYKA I PROCEDURY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zapewnić włączenie zagadnień związanych z obszarem C-SCRM do polityk i procedur utrzymania oraz wszelkich powiązanych strategii/planów wdrożenia działań w zakresie zarządzania ryzykiem w łańcuchu dostaw, polityk dotyczących zarządzania ryzykiem w łańcuchu dostaw oraz stosownych planów dla wszystkich systemów informacyjnych i sieci.
W przypadku wielu umów dotyczących utrzymania informacje na temat celów i wymogów związanych z misją, organizacją i systemem mogą być udostępniane i przesyłane między podmiotami a jego dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych i innymi dostawcami usług związanych z ICT/OT, co prowadzi do powstawania słabych punktów i umożliwia przeprowadzenie ataku. W wielu przypadkach utrzymanie systemów jest zlecane integratorowi systemów – w takich przypadkach należy podjąć stosowne

działania oraz wdrożyć odpowiednie zabezpieczenia. Nawet jeśli prace związane z utrzymaniem nie są zlecane podmiotowi zewnętrznemu, łańcuch dostaw wpływa na aktualizacje, poprawki, częstotliwość prac, części zamienne i inne aspekty utrzymania systemu.

Należy zdefiniować zasady utrzymania zarówno dla systemu, jak i dla sieci. Polityka utrzymania powinna uwzględniać środki bezpieczeństwa oparte na ocenie ryzyka (w tym analizę krytyczności), takie jak dostęp zdalny, stanowiska oraz cechy pracowników odpowiedzialnych za utrzymanie, którzy posiadają dostęp do systemów, częstotliwość aktualizacji, czas trwania umowy, ścieżkę logistyczną i metody aktualizacji lub utrzymania oraz mechanizmy monitorowania i audytu. Polityka utrzymania powinna określać, które narzędzia są dozwolone lub niedozwolone. Na przykład, w przypadku utrzymania oprogramowania, umowa powinna jasno określać kod źródłowy, przypadki testowe i inne elementy wymagane do utrzymania systemu lub komponentów.

Polityki utrzymania muszą być dopracowane oraz rozszerzane na każdym poziomie. Na poziomie 1 polityka powinna wyraźnie stwierdzać, że działania w zakresie C-SCRM powinny być stosowane w całym cyklu życia systemu, w tym w pracach związanych z jego utrzymaniem. Na poziomie 2 polityka powinna uwzględniać potrzeby operacyjne oraz najważniejsze obszary realizacji misji. Na poziomie 3 polityki powinny uwzględniać potrzeby konkretnych systemów. Wymagania z poziomu 1, takie jak utrzymanie realizowane przez podmioty zewnętrzne, powinny być przekazywane kaskadowo na poziomy 2 i 3. Na przykład w sytuacji, gdy nie jest dozwolone korzystanie z takich usług na poziomie 1, nie powinno być również dozwolone na poziomach 2 lub 3.

Podmiot powinien przekazać stosowne wymogi polityki utrzymania wykonawcom oraz wymagać od nich wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Poziom(y): 1, 2, 3

MA-2 NADZÓR NAD UTRZYMANIEM

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Dodatkowe wytyczne dotyczące wyłącznie obszaru C-SCRM zostały przedstawione w formie zabezpieczenia rozszerzonego MA-2 (2) w publikacji NSC 800-53.

Zabezpieczenia rozszerzone:

1. *NADZÓR NAD UTRZYMANIEM | ZAUTOMATYZOWANE DZIAŁANIA ZWIĄZANE Z UTRZYMANIEM*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zapewnić, że wszystkie zautomatyzowane działania związane z utrzymaniem systemów i sieci łańcucha dostaw są kontrolowane i zarządzane zgodnie z polityką utrzymania. Przykłady zautomatyzowanych działań związanych z utrzymaniem mogą obejmować aktualizacje i poprawki do produktów komercyjnych, funkcje kontaktu z serwerem dostawcy z informacją zwrotną o awarii itp. Zarządzanie tymi działaniami może wymagać ustanowienia procesów wdrożeniowych z odpowiednimi mechanizmami wspierającymi w celu zapewnienia weryfikacji lub filtrowania w stosownych przypadkach. Procesy te mogą być szczególnie ważne w przypadku krytycznych systemów i komponentów.

Poziom(y): 3

MA-3 NARZĘDZIA UTRZYMANIOWE

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Narzędzia z utrzymaniowe są uważane za część łańcucha dostaw. Jednocześnie każde z nich ma także własny łańcuch dostaw. Należy uwzględnić działania dotyczące obszaru C-SCRM, gdy podmiot nabywa lub unowocześnia narzędzie utrzymaniowe (np. wprowadza aktualizację środowiska programistycznego lub narzędzia testowego); dotyczy to także wyboru, zamawiania, przechowywania i integracji narzędzia. Podmiot powinien przeprowadzać ciągłe przeglądy oraz zatwierdzać

Narzędzia utrzymaniowe, w tym narzędzia używane przez dostawców zewnętrznych usług. Podmiot powinien również włączyć działania w zakresie C-SCRM do oceny części zamiennych związanych z narzędziami utrzymania. Ten środek bezpieczeństwa może być wdrożony na poziomach 2 i 3, w zależności od kształtu procesów zaopatrzenia, obsługi i nadzoru nad tymi narzędziami w podmiocie.

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *NARZĘDZIA UTRZYMANIOWE | KONTROLA NARZĘDZI*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien wdrożyć testy akceptacyjne w celu sprawdzenia, czy narzędzia utrzymaniowe infrastruktury łańcucha dostaw ICT są zgodne z oczekiwaniami. Narzędzia utrzymaniowe powinny podlegać autoryzacji oraz powinny być odpowiednio udokumentowane, poddane wstępnej weryfikacji oraz przetestowane pod kątem podatności, prawidłowości konfiguracji zabezpieczeń i deklarowanej funkcjonalności.

Poziom(y): 3

2. *NARZĘDZIA UTRZYMANIOWE | KONTROLA NOŚNIKÓW*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien sprawdzić, czy nośniki zawierające programy diagnostyczne i testowe, które dostawcy wykorzystują w systemach informacyjnych podmiotu, działają zgodnie z oczekiwaniami i realizują wyłącznie wymagane funkcje. Wykorzystanie nośników zawierających Narzędzia utrzymaniowe powinno być zgodne z polityką i procedurami podmiotu oraz podlegać wstępnej autoryzacji. Podmioty powinny również zapewnić, że funkcjonalność narzędzi nie wykracza poza uzgodnione ramy.

Poziom(y): 3

3. *NARZĘDZIA UTRZYMANIOWE | ZAPOBIEGANIE NIEAUTORYZOWANEMU USUNIĘCIU*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Nieautoryzowane usunięcie z łańcucha dostaw narzędzi związanych z utrzymaniem systemów i sieci może wiązać się z zagrożeniami dla łańcucha dostaw, takimi jak nieuprawniona modyfikacja, zastąpienie podrobionym rozwiązaniem lub wprowadzeniem złośliwego oprogramowania, gdy narzędzie znajduje się poza kontrolą podmiotu. Narzędzia utrzymaniowe systemów i sieci mogą obejmować zintegrowane środowisko programistyczne (*ang. integrated development environment - IDE*), a także narzędzia do testowania lub skanowania podatności. W przypadku działań związanych z obszarem C-SCRM ważne jest, aby podmiot autoryzował, śledził i kontrolował każdy przypadek usunięcia takich narzędzi. Gdy systemy i narzędzia sieciowe mają dostęp do systemu informacyjnego podmiotu, powinny pozostać własnością lub zasobem osoby bądź jednostki odpowiedzialnej za system, a w przypadku ich usunięcia lub wykorzystania w innym miejscu podmiotu powinny być obserwowane i śledzone. Narzędzia ICT związane z utrzymaniem, zarówno te, które są obecnie używane, jak i te, które są przechowywane, nie powinny opuszczać siedziby podmiotu, dopóki ich usunięcie nie zostanie zatwierdzone (tj. przypadki usunięcia nie powinny wykraczać poza uzgodniony zakres, a sam proces należy przeprowadzić zgodnie z ustalonymi zasadami i procedurami podmiotu).

Poziom(y): 3

MA-4 UTRZYMANIE ZDALNE

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Usługi utrzymania mogą być świadczone przez podmioty zewnętrzne, na przykład pracowników wykonawcy. Należy wprowadzić odpowiednie zabezpieczenia, aby skutecznie zarządzać powiązanym ryzykiem. Środki

bezpieczeństwa stosowane w odniesieniu do pracowników podmiotu zajmujących się utrzymaniem powinny być stosowane także w odniesieniu do wszelkich dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT pełniących podobną rolę w zakresie utrzymania i egzekwowane na mocy umów z dostawcami usług.

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *UTRZYMANIE ZDALNE | PORÓWNYWALNE BEZPIECZEŃSTWO I SANITYZACJA*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Jeżeli dostawcy, deweloperzy, integratorzy systemów, dostawcy zewnętrznych usług systemowych lub inni dostawcy usług związanych z ICT/OT wykonują jakiekolwiek usługi utrzymania, diagnostykę systemów lub komponentów systemu poza siedzibą podmiotu, podmiot powinien zapewnić, że:

- Podejmowane są odpowiednie działania w celu weryfikacji, czy dane środowisko spełnia odpowiednie wymogi dotyczące bezpieczeństwa w zakresie utrzymania i diagnostyki zgodnie z umowami pomiędzy organizacją a dostawcą.
- Przeprowadzono odpowiednie procesy sanityzacji w celu usunięcia wszelkich danych dotyczących podmiotu, które znajdują się w komponentach.
- Przeprowadzono odpowiednią diagnostykę, aby upewnić się, że komponenty zostały poddane sanityzacji, co zapobiega wprowadzeniu złośliwego oprogramowania do systemu podmiotu lub sieci łańcucha dostaw.

Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Poziom(y): 2, 3

MA-5 PERSONEL UTRZYMANIOWY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Personel utrzymaniowy może być zatrudniany przez dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych lub innych dostawców usług związanych z ICT/OT, w związku z tym należy wprowadzić odpowiednie zabezpieczenia w celu zarządzania powiązanym ryzykiem. Środki bezpieczeństwa stosowane w odniesieniu do wewnętrznych pracowników utrzymania podmiotu powinny być stosowane także w odniesieniu do wszelkich pracowników wykonawców, którzy realizują podobne obowiązki w zakresie utrzymania, a także egzekwowane poprzez umowy z dostawcami usług.

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *PERSONEL UTRZYMANIOWY | CUDZOZIEMCY*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Weryfikacja cudzoziemców mających dostęp do systemów oraz usług niepowiązanych z bezpieczeństwem narodowym musi uwzględniać kwestie związane z obszarem C-SCRM i być rozszerzona na wszystkich pracowników wykonawcy. Podmioty powinny określić w umowach wszelkie ograniczenia lub wymogi dotyczące weryfikacji dotyczące cudzoziemców oraz przekazać te wymogi odpowiednim podwykonawcom.

Poziom(y): 2, 3

MA-6 TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien dokonywać zakupu części zamiennych oraz części zapasowych u producentów oryginalnego wyposażenia, autoryzowanych dystrybutorów lub autoryzowanych sprzedawców oraz zadbać o stosowny czas realizacji zamówienia. Jeśli producenci nie są dostępni, podmiot powinien dokonać

zakupu u autoryzowanego dystrybutora. Jeśli nie jest dostępny producent ani autoryzowany dystrybutor, podmiot powinien dokonać zakupu u autoryzowanego sprzedawcy. Podmioty powinny zweryfikować, czy dany dystrybutor lub sprzedawca jest autoryzowany. W miarę możliwości podmioty powinny korzystać z listy zatwierdzonych dystrybutorów/sprzedawców. Jeśli jedyną alternatywą jest zakup od nieautoryzowanego dystrybutora lub na rynku wtórnym, należy przeprowadzić ocenę ryzyka obejmującą analizę krytyczności i zagrożeń w celu określenia dodatkowych środków zabezpieczających, które należy zastosować. Na przykład podmiot powinien sprawdzić, czy dany dostawca nie oferował podróbek, nie prowadził niewłaściwych praktyk lub czy nie był uwikłany w sprawy karne. Szczegóły dotyczące analizy krytyczności i zagrożeń znajdują się w rozdziale 2 niniejszego dokumentu. Podmiot powinien utrzymywać zapasy najważniejszych komponentów, jeżeli jest to wykonalne, w przypadku, gdy nabycie takich części może być niemożliwe w wymaganych ramach czasowych.

Poziom(y): 3

MA-7 KONSERWACJA W TERENIE

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny korzystać z zaufanych organizacji, gdy wymagane są dodatkowe zabezpieczenia i kontrole jakości, jeśli jest to możliwe lub praktyczne. Zaufane organizacje powinny znajdować się na zatwierdzonej liście i mieć wdrożone dodatkowe środki bezpieczeństwa.

Powiązane środki bezpieczeństwa: MA-2, MA-4, MA-5

Poziom(y): 3

MA-8 MONITOROWANIE KONSERWACJI I WYMIANA INFORMACJI (NOWY)

Środek bezpieczeństwa: Podmiot monitoruje stan systemów i komponentów oraz informuje dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych

usługodawców związanych z ICT/OT, jeśli rezultaty nie spełniają wymogów lub specyfikacji.

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Śledzenie wskaźników awaryjności komponentów dostarcza nabywcy przydatnych informacji, które pomagają zaplanować sytuacje awaryjne, alternatywne źródła dostaw i wymiany. Wskaźniki częstotliwości występowania awarii są również przydatne do monitorowania jakości i niezawodności systemów i komponentów. Informacje te stanowią użyteczną informację zwrotną dla dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT, którzy mogą dzięki nim podjąć działania naprawcze i wdrożyć procesy ciągłego doskonalenia. Na Poziomie 2 organizacje powinny śledzić i przekazywać wskaźniki częstotliwości występowania awarii dostawcom (producentom i/lub autoryzowanemu dystrybutorowi). Wskaźniki częstotliwości występowania awarii oraz problemy, które mogą wskazywać na awarie, w tym przyczyny źródłowe, powinny być określane przez personel techniczny podmiotu (np. deweloperów, administratorów lub inżynierów utrzymania) na poziomie 3 i eskalowane na poziom 2. Osoby te są w stanie zweryfikować problem i określić alternatywy techniczne.

Powiązane środki bezpieczeństwa: IR-4(10)

Poziom(y): 3

KATEGORIA MP: OCHRONA NOŚNIKÓW DANYCH

Dokument [NSC 200] określa minimalne wymagania bezpieczeństwa w zakresie ochrony nośników w następujący sposób:

> *Organizacje powinny: (I) chronić nośniki systemowe, zarówno papierowe, jak i cyfrowe; (II) zezwolić na dostęp do informacji o nośnikach systemu informacyjnego tylko upoważnionym użytkownikom; oraz (III) przeprowadzać sanityzację lub niszczyć nośniki systemu informacyjnego przed utylizacją lub dopuszczeniem do ponownego użycia.*

Sam nośnik może być elementem przemierzającym łańcuch dostaw lub zawierającym informacje o łańcuchu dostaw podmiotu. Dotyczy to zarówno fizycznych, jak i logicznych nośników, takich jak dokumentacja systemowa na papierze lub w plikach elektronicznych, dokumentacja wysyłki i dostawy z informacjami o nabywcy, pamięci Flash zawierające kod źródłowy oprogramowania, a także kompletne routery lub serwery, które zawierają trwałe nośniki. Informacje zawarte na nośnikach mogą być informacjami wrażliwymi. Dodatkowo nośnik jest wykorzystywany w całym cyklu życia systemu, od koncepcji do utylizacji. Podmioty powinny zapewnić, że kontrola ochrony nośników jest stosowana zarówno do nośników podmiotu, jak i nośników otrzymanych od dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych i innych dostawców usług związanych z ICT/OT w całym cyklu życia systemu.

MP-1 POLITYKA I PROCEDURY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: W całym łańcuchu dostaw przekazywane są różne dokumenty i informacje na różnorodnych nośnikach fizycznych i elektronicznych. Informacje te mogą obejmować różne dane wrażliwe oraz własność intelektualną pochodzącą od dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT, w związku z czym powinny być odpowiednio chronione. Polityka i procedury ochrony nośników

powinny również uwzględniać kwestie związane z łańcuchem dostaw, w tym nośniki w łańcuchu dostaw podmiotu i w całym procesie cyklu życia systemu.

Poziom(y): 1, 2

MP-4 PRZECHOWYWANIE NOŚNIKÓW DANYCH

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Środki bezpieczeństwa w zakresie przechowywania nośników powinny obejmować działania związane z obszarem C-SCRM. Podmioty powinny określić i zawrzeć w umowach zasady i polityki dotyczące przechowywania nośników (np. szyfrowania) dotyczące dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT, którzy posiadają polityki kontroli dostępu. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Poziom(y): 1, 2

MP-5 TRANSPORT NOŚNIKÓW DANYCH

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien uwzględnić działania związane z obszarem C-SCRM dotyczące transportu nośników przez pracowników podmiotu lub osoby trzecie. Niektóre z technik ochrony nośników podczas transportu i przechowywania obejmują techniki kryptograficzne i zatwierdzone usługi nadzoru.

Poziom(y): 1, 2

MP-6 SANITYZACJA NOŚNIKÓW DANYCH

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny określić i zawrzeć w umowach (np. w treści umów) zasady i polityki dotyczące sanityzacji nośników dotyczące dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych

oraz innych dostawców usług związanych z ICT/OT, którzy posiadają polityki kontroli dostępu. Nośniki są wykorzystywane w całym cyklu życia systemu. Nośniki przemieszczające się lub przebywające w łańcuchu dostaw mogą powstawać w jego dowolnym punkcie. Mogą zostać wprowadzone przez dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT. Mogą być nowe, odnowione lub ponownie wykorzystane. Sanityzacja nośników ma kluczowe znaczenie dla zagwarantowana, że wszystkie informacje i dane są usunięte przed użyciem, ponownym wykorzystaniem lub utylizacją nośnika. W przypadku nośników zawierających informacje wrażliwe, podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Poziom(y): 2, 3

Powiązane środki bezpieczeństwa: MP-6(1), MP-6(2), MP-6(3), MP-6(7), MP-6(8)

KATEGORIA PE: OCHRONA FIZYCZNA I ŚRODOWISKOWA

Dokument [NSC 200] określa minimalne wymagania bezpieczeństwa w zakresie zabezpieczeń fizycznych i środowiskowych w następujący sposób:

> *Organizacje powinny: (i) ograniczyć fizyczny dostęp do systemów informacyjnych, sprzętu i odpowiednich środowisk operacyjnych tylko do upoważnionych osób; (II) chronić fizyczne instalacje i infrastrukturę wsparcia systemów informacyjnych; (III) zapewnić narzędzia wsparcia dla systemów informacyjnych; (IV) chronić systemy informacyjne przed zagrożeniami środowiskowymi; oraz (V) zapewnić odpowiednie zabezpieczenia środowiskowe w obiektach zawierających systemy informacyjne.*

Łańcuchy dostaw obejmują światy fizyczny i logiczny. Czynniki fizyczne mogą obejmować warunki pogodowe i drogowe, które mogą wpływać na transport komponentów (lub urządzeń) z jednej lokalizacji do drugiej pomiędzy osobami lub podmiotami w ramach łańcucha dostaw. Jeśli nie zostaną odpowiednio uwzględnione jako część procesów zarządzania ryzykiem związanym z obszarem C-SCRM, ryzyka fizyczne i środowiskowe mogą mieć negatywny wpływ na zdolność podmiotu do terminowego otrzymywania komponentów krytycznych, co z kolei może wpłynąć na zdolność do realizacji misji podmiotu. Podmioty powinny wymagać wdrożenia odpowiednich zabezpieczeń fizycznych i środowiskowych w ramach swojego łańcucha dostaw.

PE-1 POLITYKA I PROCEDURY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien włączyć praktyki i wymagania dotyczące obszaru C-SCRM do własnych zasad i procedur zabezpieczeń fizycznych i środowiskowych. Stopień ochrony powinien być współmierny do stopnia integracji. Polityka zabezpieczeń fizycznych i środowiskowych powinna zapewnić, że fizyczne punkty styku łańcucha dostaw są objęte odpowiednią ochroną, a zabezpieczenia są kontrolowane.

Poziom(y): 1, 2, 3

PE-2 ZEZWOLENIA NA DOSTĘP FIZYCZNY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zapewnić, że dostęp do informacji, systemów lub centrów danych (w tym danych wrażliwych lub niejawnych) mają tylko upoważnione osoby, które potrzebują fizycznego dostępu. Upoważnienia takie powinny określać czynności, które dana osoba może lub których nie może wykonywać w ramach dostępu (np. przeglądać, zmieniać, konfigurować, podłączać, usuwać, wstawiać itp.)

Umowy powinny uwzględniać wymogi w zakresie autoryzacji dostępu fizycznego, a podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Autoryzacja pracowników powinna być zgodna z zatwierdzonym protokołem, który zawiera dokumentację upoważnienia i określa wszelkie warunki wstępne lub ograniczenia, które dotyczą takiego upoważnienia (np. dana osoba musi być eskortowana przez pracownika, dana osoba musi mieć identyfikator, dana osoba może uzyskiwać fizyczny dostęp w normalnych godzinach pracy itp.)

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *ZEZWOLENIA NA DOSTĘP FIZYCZNY | DOSTĘP NA PODSTAWIE STANOWISKA LUB ROLI*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Zezwolenia na dostęp fizyczny na podstawie stanowiska lub roli powinna obejmować pracowników podmiotów publicznych oraz pracowników podmiotów współpracujących (np. dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT). W przypadku stosowania autoryzacji na podstawie stanowiska lub roli, rodzaj i poziom dostępu dozwolony dla danej roli lub stanowiska musi być wcześniej ustalony i udokumentowany.

Poziom(y): 2, 3

PE-3 KONTROLA DOSTĘPU FIZYCZNEGO

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Kontrola dostępu fizycznego powinna obejmować osoby i podmioty wchodzące w skład łańcucha dostaw podmiotu. Przed przyznaniem dostępu do infrastruktury łańcucha dostaw i wszelkich istotnych komponentów należy przeprowadzić proces weryfikacji oparty na określonych przez podmiot wymaganiach i zasadach. Procesy przyznawania, utrzymywania i cofania dostępu powinny spełniać rygorystyczne zasady polityki kontroli dostępu w podmiocie. Szybkość wycofywania autoryzacji dostępu dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT, którzy wymagają dostępu do obiektów fizycznych i centrów danych będących własnością podmiotu lub dostawców zewnętrznych usług powinna być zgodna z czynnościami wykonywanymi w ramach ich umów. Szybkie wycofywanie autoryzacji jest niezwykle ważne, gdy dany podmiot lub dana osoba traci potrzebę uzyskiwania dostępu fizycznego.

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *KONTROLA DOSTĘPU FIZYCZNEGO | DOSTĘP DO SYSTEMU*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Kontrola dostępu fizycznego powinna obejmować pracowników wykonawcy. Każdy pracownik wykonawcy, który świadczy usługi wymagające fizycznego dostępu do infrastruktury łańcucha dostaw i wszelkich istotnych elementów, powinien podlegać wymogom kontroli dostępu. Polityki i procedury powinny być spójne z tymi stosowanymi wobec pracowników wewnętrznych posiadających podobne uprawnienia w zakresie dostępu fizycznego.

Poziom(y): 2, 3

2. *KONTROLA DOSTĘPU FIZYCZNEGO | OBIEKTY I SYSTEMY*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Określając zakres, częstotliwość oraz losowość kontroli zabezpieczeń obiektów, podmioty powinny uwzględniać ryzyko eksfiltracji związane z zastosowaniem ukrytych urządzeń podsłuchowych. Urządzenia takie mogą obejmować podsłuchy, podsłuchy ruchome, symulatory stacji bazowych i inne technologie podsłuchowe, które mogą doprowadzić do wycieku wrażliwych informacji.

Poziom(y): 2, 3

3. *KONTROLA DOSTĘPU FIZYCZNEGO | OCHRONA PRZED MANIPULACJĄ*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Ochrona przed manipulacją ma kluczowe znaczenie dla zmniejszenia ryzyka związanego z cyberbezpieczeństwem produktów. Podmiot powinien wdrożyć sprawdzone techniki ochrony przed manipulacją w ramach łańcucha dostaw. W przypadku produktów krytycznych podmiot powinien wymagać wdrożenia mechanizmów ochrony przed manipulacją i oceniać stopień ich wdrożenia. Ocena może obejmować również to, czy i w jaki sposób takie mechanizmy są wymagane i stosowane przez podmioty należące do łańcucha dostaw dostawcy.

Poziom(y): 2, 3

PE-6 MONITOROWANIE DOSTĘPU FIZYCZNEGO

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Osoby, które mają fizyczny dostęp do obiektów podmiotu lub usługodawcy zewnętrznego, centrów danych, informacji lub zasobów fizycznych – w tym za pośrednictwem łańcucha dostaw – mogą być pracownikami podmiotu, wykonawcami pracującymi na miejscu lub zdalnie, gośćmi, osobami trzecimi (np. pracownikami obsługi technicznej zatrudnionymi na podstawie umowy z wykonawcą) lub osobami powiązanymi z podmiotem w łańcuchu dostaw. Podmiot powinien monitorować działania tych osób w celu zmniejszenia

ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw lub wymagać takiego monitorowania w umowach.

Poziom(y): 1, 2, 3

PE-16 DOSTAWA I USUWANIE

Dodatkowe wytyczne dotyczące obszaru C-SCRM: To zabezpieczenie rozszerzone zmniejsza ryzyko związane z cyberbezpieczeństwem, które powstaje podczas fizycznego dostarczania lub usuwania komponentów sprzętowych z systemów informacyjnych podmiotu lub łańcucha dostaw. Obejmuje bezpieczeństwo transportu, weryfikację dostarczonych komponentów oraz weryfikację procedur sanityzacji. Kwestie związane z ryzykiem obejmują znaczenie komponentu dla realizacji misji, a także środowisko rozwoju, eksploatacji lub utrzymania (np. tajne laboratorium integracyjne i testowe).

Poziom(y): 3

PE-17 ZAPASOWE MIEJSCE PRACY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien wprowadzić zabezpieczenia chroniące przed zagrożeniami dla cyberbezpieczeństwa związanymi z pracownikami podmiotu lub wykonawcy w obrębie infrastruktury łańcucha dostaw lub w czasie uzyskiwania dostępu z alternatywnych miejsc pracy. Może to obejmować pracowników podmiotów zewnętrznych, którzy mogą pracować w alternatywnych miejscach pracy.

Poziom(y): 3

PE-18 LOKALIZACJA KOMPONENTÓW SYSTEMU

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Zagrożenia fizyczne i środowiskowe mają wpływ na dostępność produktów, które są lub będą nabywane i fizycznie transportowane do lokalizacji podmiotu. Podmioty powinny dokładnie rozważyć kwestie miejsca produkcji, magazynowania

lub dystrybucji komponentów systemu informacyjnego, które są kluczowe dla działalności organizacji, w procesie planowania alternatywnych dostawców tych komponentów.

Poziom(y): 1, 2, 3

Powiązane środki bezpieczeństwa: CP-6, CP-7

PE-20 MONITOROWANIE I ŚLEDZENIE ZASOBÓW

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien w miarę możliwości wykorzystywać technologie lokalizacji zasobów do śledzenia systemów i komponentów transportowanych pomiędzy podmiotami w ramach łańcucha dostaw, pomiędzy obszarami chronionymi lub w magazynie, gdy oczekują na wdrożenie, testowanie, konserwację lub utylizację. Metody śledzenia obejmują znaczniki RFID, podpisy cyfrowe czy rejestry blockchain. Technologie te pomagają chronić przed:

a. Przekierowaniem systemu lub komponentu w celu wymiany na podrobioną lub zmodyfikowaną wersję.

b. Utratą poufności, integralności lub dostępności funkcji i danych systemu lub komponentu (w tym danych zawartych w komponencie i danych dotyczących komponentu).

c. Przerwaniem łańcucha dostaw i procesów logistycznych dla krytycznych komponentów. Oprócz zapewnienia możliwości ochrony, technologie lokalizacji zasobów pomagają również w gromadzeniu danych, które mogą być wykorzystane do zarządzania incydentami.

Poziom(y): 2, 3

PE-23 LOKALIZACJA OBIEKTU

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny uwzględniać lokalizację obiektu (np. centrów danych) przy ocenie ryzyka związanego z dostawcami. Czynniki mogą obejmować lokalizację geograficzną zabezpieczenia fizyczne stosowane w obiekcie lub obiektach,

lokalne zarządzanie i kontrolę nad takimi obiektami, potencjalne zagrożenia środowiskowe (np. lokalizacja w strefie zagrożonej wstrząsami sejsmicznymi, warunkami atmosferycznymi, itp.) oraz alternatywne lokalizacje obiektów. Podmioty powinny również ocenić, czy na lokalizację centrum produkcyjnego lub dystrybucyjnego mogą mieć wpływ czynniki geopolityczne, ekonomiczne lub inne. W przypadku dostawców lub produktów o znaczeniu krytycznym podmioty powinny uwzględnić w umowach wszelkie wymogi lub ograniczenia dotyczące lokalizacji zakładów dostawców (lub ich dostawców z łańcucha dostaw) i przekazać te wymogi odpowiednim wykonawcom niższego szczebla.

Poziom(y): 2, 3

Powiązane środki bezpieczeństwa: SA-9(8)

KATEGORIA PL: PLANOWANIE

Dokument [NSC 200] określa minimalne wymagania bezpieczeństwa w zakresie planowania w następujący sposób:

> *Organizacje powinny opracowywać, dokumentować, okresowo aktualizować i wdrażać plany bezpieczeństwa dla organizacyjnych systemów informacyjnych, które opisują mechanizmy zabezpieczeń obowiązujące lub planowane dla systemów informacyjnych oraz reguły zachowania osób uzyskujących dostęp do systemów informacyjnych.*

Działania w zakresie C-SCRM powinny wpływać na planowanie bezpieczeństwa, w tym na takie obszary jak architektura bezpieczeństwa, koordynacja z innymi podmiotami oraz opracowanie Planów Bezpieczeństwa Systemu. Nabywając produkty i usługi od dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT, podmioty mogą działać w tych samych obiektach, ich pracownicy mogą przebywać na terenie siedziby podmiotu, mogą także korzystać z systemów informacyjnych należących do tych podmiotów. W tych i innych stosownych sytuacjach podmioty powinny koordynować swoje działania w zakresie planowania bezpieczeństwa z tymi organizacjami, aby zapewnić odpowiednią ochronę procesów podmiotu, systemów informacyjnych oraz systemów i komponentów przechodzących przez łańcuch dostaw. Tworząc architektury bezpieczeństwa, podmioty powinny uwzględnić różnorodność komponentów i dostawców, aby zarządzać ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw – obejmuje to także możliwość zakończenia działalności przez dostawcę lub zaprzestania produkcji określonych komponentów. Wreszcie, jak informują autorzy w rozdziale 2 i Załączniku C, podmioty powinny włączyć środki bezpieczeństwa związane z obszarem C-SCRM do swoich ram reagowania na ryzyko (poziom 1 i poziom 2), jak również do swoich planów C-SCRM (poziom 3).

PL-1 POLITYKA I PROCEDURY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Polityka i procedury planowania bezpieczeństwa powinny obejmować działania związane z obszarem C-SCRM. Obejmuje to opracowanie, rozpowszechnienie i aktualizację polityki bezpieczeństwa, polityki operacyjnej i procedur dotyczących obszaru C-SCRM w celu kształtowania wymagań dotyczących zamówień, zaopatrzenia lub rozwoju oraz późniejszego wdrażania, eksploatacji i utrzymania systemów, interfejsów systemowych i połączeń sieciowych. Polityka i procedury C-SCRM stanowią materiał źródłowy pozwalający na opracowanie strategii i planu wdrożenia C-SCRM na poziomie 1 oraz planu bezpieczeństwa systemów i planów C-SCRM na poziomie 3, które opierają się na ich wytycznych. Na poziomie 3 należy zapewnić, działania dotyczące obszaru C-SCRM dotyczą pełnego cyklu życia systemu.

Poziom(y): 2

Powiązane środki bezpieczeństwa: PL-2, PM-30

PL-2 PLANY BEZPIECZEŃSTWA SYSTEMU I OCHRONY PRYWATNOŚCI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Plan bezpieczeństwa systemu powinien obejmować zagadnienia związane z obszarem C-SCRM. Podmiot może zdecydować się na opracowanie oddzielnego planu C-SCRM dla pojedynczego systemu lub włączyć środki bezpieczeństwa związane z zarządzaniem ryzykiem w łańcuchu dostaw do planu bezpieczeństwa systemu. Plan bezpieczeństwa systemu lub plan C-SCRM dotyczący systemu stanowią element strategii i planu wdrożenia C-SCRM na poziomie 1 oraz polityki C-SCRM na poziomie 1 i 2 oraz opierają się na ich wytycznych. Oprócz koordynacji wewnętrznej, podmiot powinien koordynować swoje plany bezpieczeństwa systemu z dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych oraz innymi dostawcami usług związanych z ICT/OT, co umożliwi im opracowanie i utrzymanie stosownych planów bezpieczeństwa systemu. Budowa

i eksploatacja systemu wymagają znaczącej koordynacji i współpracy pomiędzy podmiotem i pracownikami integratora systemu. Taka koordynacja i współpraca powinny być uwzględnione w planie bezpieczeństwa systemu lub oddzielnym planie C-SCRM. Plany te powinny również uwzględniać, że dostawcy lub zewnętrzni usługodawcy mogą nie być w stanie dostosować rozwiązania do wymagań nabywcy. Zaleca się, aby dostawcy, deweloperzy, integratorzy systemów, dostawcy zewnętrzni usług systemowych i inni dostawcy usług związanych z ICT/OT również opracowali plany C-SCRM dotyczące systemów (tj. systemów wykonawców), które przetwarzają informacje podmiotów publicznych, a następnie przekazali ten wymóg odpowiednim wykonawcom niższego szczebla.

Rozdział 2, a także załączniki C i D zawierają wytyczne dotyczące strategii, polityki i planów C-SCRM. Środki bezpieczeństwa zawarte w niniejszej publikacji powinny być stosowane do części planów bezpieczeństwa systemu poświęconej obszarowi C-SCRM.

Poziom(y): 3

Powiązane środki bezpieczeństwa: PM-30

PL-4 ZASADY POSTĘPOWANIA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Pojęcie zasad zachowania dotyczy pracowników wykonawcy oraz pracowników wewnętrznych organizacji. Wykonawcy są odpowiedzialni za zapewnienie, że ich pracownicy przestrzegają obowiązujących zasad zachowania. Poszczególni wykonawcy nie powinni mieć dostępu do systemów lub danych organizacji, dopóki nie potwierdzą i nie wykażą zgodności z tym środkiem bezpieczeństwa. Niespełnienie tego środka bezpieczeństwa może skutkować odebraniem dostępu.

Poziom(y): 2, 3

PL-7 KONCEPCJA BEZPIECZEŃSTWA DZIAŁAŃ OPERACYJNYCH

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Koncepcja działań operacyjnych (*ang. concept of operations - CONOPS*) powinna opisywać, jak podmiot zamierza eksploatować system z punktu widzenia C-SCRM. Powinna uwzględniać zagadnienia dotyczące obszaru C-SCRM oraz być aktualizowana i zarządzana w całym cyklu życia systemu stosownego systemu w celu uwzględnienia ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw.

Poziom(y): 3

PL-8 ARCHITEKTURY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Architektura bezpieczeństwa i prywatności określa sposób wdrażania metod, mechanizmów i możliwości ochrony bezpieczeństwa i prywatności systemów i sieci, a także tworzonego systemu informacyjnego. Architektura bezpieczeństwa ma kluczowe znaczenie z punktu widzenia C-SCRM, ponieważ pomaga zapewnić, że kwestie bezpieczeństwa są uwzględnione w całym cyklu życia systemu. Podmioty powinny rozważyć wdrożenie architektur „zerowego zaufania" i zapewnić, że architektura bezpieczeństwa jest dobrze rozumiana przez deweloperów, inżynierów systemu i inżynierów bezpieczeństwa systemu. Ten środek bezpieczeństwa dotyczy zarówno pracowników podmiotów publicznych, jak i pracowników organizacji sektora prywatnego.

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *ARCHITEKTURY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | RÓŻNORODNOŚĆ DOSTAWCÓW*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Różnorodność dostawców oferuje szereg możliwości rozwiązania problemów związanych z bezpieczeństwem informacji i łańcuchem dostaw.

Podmiot powinien uwzględnić ten środek bezpieczeństwa w odniesieniu do dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT.

Podmiot powinien zaplanować potencjalne zastąpienie dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT w przypadku, gdy jeden z nich nie będzie w stanie dłużej spełniać wymagań podmiotu (np. w związku z zakończeniem działalności lub niewywiązywaniem się ze zobowiązań umownych). W stosownych przypadkach umowy powinny być sformułowane w taki sposób, aby różne części komponentów mogły zostać zastąpione podobnym modelem dostępnym w podobnej cenie od innego producenta w przypadku wystąpienia określonych zdarzeń (np. wycofanie z produkcji, niedostateczne osiągi, problemy produkcyjne itp.).

Należy uwzględnić różnych dostawców w przypadku komponentów komercyjnych lub rządowych podczas oceny bezpieczeństwa zamówień. Ocena rozwiązań alternatywnych powinna obejmować na przykład porównanie funkcji, interoperacyjność, dostępność oraz możliwość zapewnienia wielu ścieżek dostawy. Uzyskanie kodu źródłowego, skryptów kompilacyjnych oraz testów dla komponentu oprogramowania może pozwolić podmiotowi na przekazanie innej jednostce zadania utrzymania tego komponentu, jeśli zajdzie taka potrzeba.

Poziom(y): 2, 3

PL-9 ZARZĄDZANIE CENTRALNE

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Środki bezpieczeństwa związane z obszarem C-SCRM powinny być zarządzane centralnie na poziomie 1 przy pomocy strategii i planu wdrożenia C-SCRM oraz na poziomie 1 i 2 przy pomocy polityki C-SCRM. Biuro zarządzania

programem C-SCRM opisane w rozdziale 2 centralnie zarządza środkami bezpieczeństwa związanymi z obszarem C-SCRM na poziomach 1 i 2. Na poziomie 3 środki bezpieczeństwa związane z obszarem C-SCRM są zarządzane na szczeblu poszczególnych systemów informacyjnych na podstawie planów bezpieczeństwa systemów lub planów C-SCRM.

Poziom(y): 1, 2

PL-10 WYBÓR ZABEZPIECZEŃ BAZOWYCH

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny włączyć środki bezpieczeństwa związane z obszarem C-SCRM do swoich podstawowych zabezpieczeń. Podmioty powinny określić i ustanowić środki bezpieczeństwa związane z obszarem C-SCRM w oparciu o wymagania C-SCRM określone w ramach każdego z poziomów. Biuro zarządzania programem C-SCRM może pomóc w określeniu poziomu bazowego środków bezpieczeństwa związanych z obszarem C-SCRM, które spełniają wspólne wymagania C-SCRM dla różnych grup interesów lub podmiotu jako całości.

Poziom(y): 1, 2

KATEGORIA PM: PROGRAMY ZARZĄDZANIA

Dokument [NSC 200] określa minimalne wymagania bezpieczeństwa w zakresie zarządzania programem w następujący sposób:

> *Organizacje powinny: (I) opracowywać i rozpowszechniać plan programu bezpieczeństwa informacji (ang. Information Security Program Plan) 4; (II) przeglądać i aktualizować plan programu bezpieczeństwa informacji; (III) chronić plan bezpieczeństwa informacji przed nieautoryzowanym ujawnieniem i modyfikacją.*

W dokumencie [NSC 800-53] czytamy, że „środki bezpieczeństwa związane z zarządzaniem programem […] są realizowane na poziomie podmiotu i nie dotyczą poszczególnych systemów informacyjnych". Środki bezpieczeństwa te dotyczą całego podmiotu (np. podmiotu sektora publicznego) i wspierają realizację nadrzędnego programu bezpieczeństwa informacji podmiotu. Środki bezpieczeństwa w zakresie zarządzania programem wspierają działania w zakresie C-SCRM w skali całego podmiotu oraz stanowią ważny wkład w ich realizację.

Wszystkie środki bezpieczeństwa związane z zarządzaniem programem powinny być stosowane w kontekście C-SCRM. W ramach podmiotów publicznych biuro zarządzania programem C-SCRM lub podobna jednostka winna być odpowiedzialna za wdrażanie środków bezpieczeństwa w zakresie zarządzania programem. Rozdział 3 zawiera wytyczne dotyczące biura zarządzania programem C-SCRM oraz jego funkcji i obowiązków.

PM-2 ROLE KIEROWNICZE PROGRAMU BEZPIECZEŃSTWA INFORMACJI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Personel wyższego szczebla ds. bezpieczeństwa informacji (np. CISO) oraz odpowiedzialny za zamówienia i zaopatrzenie (np. Chief Acquisition Officer [CAO] lub Senior Procurement Executive [SPE]) są odpowiedzialni za działania w obszarze C-SCRM oraz ogólną koordynację i współpracę między organizacjami z innymi odpowiednimi pracownikami wyższego szczebla w podmiocie, takimi jak CIO, personelem ds. obiektów/ochrony fizycznej oraz osobami odpowiedzialnymi za zarządzanie ryzykiem. Koordynacja ta powinna występować niezależnie od konkretnej struktury podmiotu oraz nazw stanowisk zajmowanych przez

poszczególne osoby, których dotyczy niniejszy zapis. Koordynacją może zajmować się biuro zarządzania programem C-SCRM lub podobna jednostka. W rozdziale 2 znajdują się dodatkowe wytyczne dotyczące ról i obowiązków związanych z obszarem C-SCRM.

Poziom(y): 1, 2

PM-3 ZASOBY W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI I OCHRONY PRYWATNOŚCI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Realizacja przez podmiot programu działań związanych z obszarem C-SCRM wymaga przeznaczenia funduszy oraz skierowania pracowników, którzy zajmą się skutecznym wdrożeniem wymogów organizacji w zakresie C-SCRM. Rozdział 3 niniejszego dokumentu zawiera wytyczne dotyczące finansowania programów C-SCRM. Podmiot powinien również włączyć wymogi w zakresie C-SCRM do kluczowych inwestycji związanych z IT, aby zapewnić odpowiedni przydział środków w ramach procesu planowania budżetu oraz wniosków inwestycyjnych. Jeśli wsparcie działań w zakresie C-SCRM będzie wymagało wdrożenia infrastruktury RFID w celu zwiększenia bezpieczeństwa i poprawy efektywności zarządzania zapasami lub logistyką w łańcuchu dostaw podmiotu, prawdopodobnie wymagane będą odpowiednie inwestycje w celu zapewnienia skutecznego planowania i wdrożenia takich rozwiązań. Inne przykłady obejmują wszelkie inwestycje w środowisko rozwojowe lub testowe dla komponentów krytycznych. W takich przypadkach niezbędne są fundusze i zasoby potrzebne w celu nabycia i utrzymania odpowiednich systemów informacyjnych, sieci i komponentów w celu spełnienia określonych wymogów C-SCRM i realizacji misji podmiotu.

Poziom(y): 1, 2

PM-4 PLAN DZIAŁANIA I ETAPY WPROWADZANIA ZABEZPIECZEŃ

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Zagadnienia dotyczące obszaru C-SCRM powinny być włączone do dokumentów planu i etapów działania na wszystkich poziomach. Organizacje powinny opracować dokumenty planu i etapów działania na podstawie sprawozdań z oceny dotyczącej obszaru C-SCRM. Plany i etapy działania powinny być wykorzystywane przez organizacje do opisywania planowanych działań mających na celu poprawę niedociągnięć w środkach bezpieczeństwa związanych z obszarem C-SCRM ustalonych w trakcie oceny oraz ciągłego monitorowania postępów w realizacji tych działań.

Poziom(y): 2, 3

Powiązane środki bezpieczeństwa: CA-5, PM-30

PM-5 INWENTARYZACJA SYSTEMU

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Aktualna inwentaryzacja i Inwentaryzacja komponentów systemu są niezwykle ważnym elementem działań związanych z obszarem C-SCRM. Braki w tym obszarze mogą przełożyć się na niemożność określenia przez podmiot krytyczności systemów i dostawców, a w rezultacie brak możliwości realizacji działań w zakresie C-SCRM. Aby zapewnić prawidłowe określenie charakteru wszystkich dostawców oraz ich kategoryzację, podmioty powinny włączyć odpowiednie informacje o dostawcach do inwentaryzacji systemu oraz dbać o ich aktualność i dokładność. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

PM-6 MIARY SKUTECZNOŚCI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny stosować wskaźniki skuteczności w celu monitorowania wdrażania, skuteczności, efektywności i wpływu działań C-SCRM. Biuro zarządzania programem C-SCRM jest odpowiedzialne za tworzenie wskaźników skuteczności działań C-SCRM we współpracy z innymi interesariuszami, w tym za określenie odpowiednich odbiorców i decydentów oraz opracowanie wytycznych dotyczących gromadzenia danych, analizy i raportowania.

Poziom(y): 1, 2

PM-7 STRUKTURA ORGANIZACYJNA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Działania w zakresie C-SCRM powinny zostać włączone w procesy projektowania i utrzymywania architektury korporacyjnej.

Poziom(y): 1, 2

PM-8 PLAN INFRASTRUKTURY KRYTYCZNEJ

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Działania w zakresie C-SCRM powinny zostać włączone w procesy rozwoju i utrzymania planu infrastruktury krytycznej.

Poziom(y): 1

PM-9 STRATEGIA ZARZĄDZANIA RYZYKIEM

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Strategia zarządzania ryzykiem powinna uwzględniać ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw. Rozdział 2, Załącznik C i Załącznik D do niniejszego dokumentu zawierają wytyczne dotyczące włączenia C-SCRM do strategii zarządzania ryzykiem.

Poziom(y): 1

PM-10 PROCES AUTORYZACJI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Działania w zakresie C-SCRM powinny zostać włączone w procesy projektowania i wdrażania procesów autoryzacji.

Poziom(y): 1, 2

PM-11 DEFINICJA MISJI I PROCESU BIZNESOWEGO

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Misja podmiotu i procesy biznesowe powinny uwzględniać ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw. Zajmując się definicjami misji i procesów biznesowych, podmiot powinien zapewnić, że działania C-SCRM są włączone do procesów wsparcia w celu skutecznej realizacji misji. Na przykład system wspierający kluczowe działanie, który został zaprojektowany i wdrożony z myślą o łatwym demontażu i szybkiej wymianie w przypadku awarii jednego z komponentów, może wymagać zastosowania zawodnych komponentów sprzętowych. Z tego powodu konieczne może być zdefiniowanie działania C-SCRM w celu zapewnienia, że dostawca udostępni części zamienne komponentów, jeśli potrzebna będzie ich wymiana.

Poziom(y): 1, 2, 3

PM-12 ZAGROŻENIA WEWNĘTRZNE

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Program dotyczący zagrożeń wewnętrznych powinien obejmować działania związane z obszarem C-SCRM i być dostosowany zarówno do pracowników podmiotów publicznych, jak i innych podmiotów, które mają dostęp do systemów i sieci podmiotu. Ten środek bezpieczeństwa dotyczy wykonawców i podwykonawców i powinien być wdrożony w całym cyklu życia systemu.

Poziom(y): 1, 2, 3

PM-13 PERSONEL BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Rozwój i doskonalenie pracowników zajmujących się bezpieczeństwem i prywatnością powinny obejmować zagadnienia związane z obszarem C-SCRM, które powinny zostać włączone do treści szkoleń oraz inicjatyw opracowywanych w ramach programu. W rozdziale 2 znajdują się dodatkowe informacje dotyczące ról i obowiązków związanych z obszarem C-SCRM. Dokument NSC 800-161 może posłużyć jako źródło tematów i działań, które należy włączyć do programu rozwoju dla pracowników zajmujących się bezpieczeństwem i prywatnością.

Poziom(y): 1, 2

PM-14 TESTOWANIE, SZKOLENIE I MONITOROWANIE

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien wdrożyć proces zapewniający aktualizację i utrzymanie planów organizacyjnych dotyczących przeprowadzania testów ryzyka łańcucha dostaw, a także szkoleń i monitorowania związanych z systemami organizacyjnymi. Biuro zarządzania programem C-SCRM może zapewnić wytyczne i wsparcie w zakresie włączenia zagadnień związanych z obszarem C-SCRM do planów testów, szkolenia i monitorowania.

Poziom(y): 1, 2

PM-15 GRUPY I STOWARZYSZENIA ZAJMUJĄCE SIĘ BEZPIECZEŃSTWEM I OCHRONĄ PRYWATNOŚCI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Kontakty z grupami i stowarzyszeniami zajmującymi się bezpieczeństwem i prywatnością powinny dotyczyć praktyków C-SCRM oraz osoby odpowiedzialne za C-SCRM w podmiocie. W działania te należy włączyć grupy i stowarzyszenia związane z zamówieniami, prawem, infrastrukturą krytyczną oraz łańcuchem dostaw. Biuro zarządzania programem C-SCRM może pomóc w opracowaniu listy pracowników, którzy mogą skorzystać na

uczestnictwie w takich spotkaniach, opracowaniu listy grup oraz stosownych tematów i zagadnień.

Poziom(y): 1, 2

PM-16 OSTRZEGANIE O ZAGROŻENIACH

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Program świadomości zagrożeń powinien obejmować zagrożenia pochodzące z łańcucha dostaw. W zakresie świadomości zagrożeń w łańcuchu dostaw, interesariusze powinni dzielić się wiedzą zgodnie z polityką udostępniania informacji obowiązującą w podmiocie. Biuro zarządzania programem C-SCRM może pomóc w opracowaniu listy interesariuszy zajmujących się obszarem C-SCRM, których należy uwzględnić w procesach wymiany informacji o zagrożeniach, a także listy potencjalnych źródeł informacji o zagrożeniach dotyczących łańcucha dostaw.

Poziom(y): 1, 2

PM-17 OCHRONA NADZOROWANYCH INFORMACJI JAWNYCH PRZETWARZANYCH W SYSTEMACH ZEWNĘTRZNYCH

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Zasady i procedury dotyczące kontrolowanych informacji jawnych w systemach zewnętrznych powinny obejmować ochronę informacji dotyczących łańcucha dostaw. Powinny także obejmować ochronę informacji organizacji, które znajdują się w systemach zewnętrznych, ponieważ takie systemy zewnętrzne są częścią łańcucha dostaw agencji.

Poziom(y): 2

PM-18 PLAN PROGRAMU OCHRONY PRYWATNOŚCI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Plan programu ochrony prywatności powinien obejmować zagadnienia związane z obszarem C-SCRM. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom.

Poziom(y): 1, 2

PM-19 ROLE KIEROWNICZE PROGRAMU OCHRONY PRYWATNOŚCI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Rola lidera programu ochrony prywatności powinna być interesariuszem stosownych inicjatyw i działań związanych z obszarem C-SCRM.

Poziom(y): 1

PM-20 ROZPOWSZECHNIANIE INFORMACJI O PROGRAMIE OCHRONY PRYWATNOŚCI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Rozpowszechnianie informacji o programie ochrony prywatności powinno być chronione przed ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw.

Poziom(y): 1, 2

PM-21 REJESTROWANIE UJAWNIEŃ

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Dokumentacja ujawnień informacji powinna być chroniona przed ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw.

Poziom(y): 1, 2

PM-22 ZARZĄDZANIE JAKOŚCIĄ DANYCH OSOBOWYCH

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Zarządzanie jakością danych osobowych powinno uwzględniać zarządzanie ryzykiem związanym z cyberbezpieczeństwem związanym z danymi osobowymi w całym łańcuchu dostaw.

Poziom(y): 1, 2

PM-23 ORGAN ZARZĄDZANIA DANYMI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Jednostka odpowiedzialna za dane jest interesariuszem zagadnień związanych z obszarem C-SCRM i powinna być włączona do współpracy międzyorganizacyjnej i wymiany informacji na temat działań i inicjatyw C-SCRM.

Poziom(y): 1

PM-25 MINIMALIZACJA DANYCH OSOBOWYCH WYKORZYSTYWANYCH W TESTACH, SZKOLENIACH I BADANIACH

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Ryzyko związane z cyberbezpieczeństwem w łańcuchu dostaw dotyczące danych osobowych powinno być uwzględnione w politykach i procedurach minimalizacji opisanych w związku z tym środkiem bezpieczeństwa.

Poziom(y): 2

PM-26 ZARZĄDZANIE SKARGAMI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Proces i mechanizmy obsługi reklamacji powinny być chronione przed ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw. Podmioty powinny również włączyć środki bezpieczeństwa oraz zabezpieczenia prywatności związane z obszarem C-SCRM w przypadku obsługi reklamacji sprzedawców lub ogółu społeczeństwa (np. jednostki organizacji obsługujące zapytania dotyczące wykluczeń i usuwania).

Poziom(y): 2, 3

PM-27 SPRAWOZDAWCZOŚĆ W ZAKRESIE OCHRONY PRYWATNOŚCI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Proces i mechanizmy opracowywania sprawozdań dotyczących prywatności powinny być chronione przed ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw.

Poziom(y): 2, 3

PM-28 OPRACOWYWANIE RAM RYZYKA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Zagadnienia dotyczące obszaru C-SCRM powinny być włączone w proces określania ram ryzyka. Rozdział 2 i Załącznik C zawierają szczegółowe wytyczne dotyczące włączenia zagadnień związanych z obszarem C-SCRM do procesu określania ram ryzyka.

Poziom(y): 1

PM-29 ROLE KIEROWNICZE PROGRAMU ZARZĄDZANIA RYZYKIEM

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Role kierownicze w programie zarządzania ryzykiem powinny uwzględniać obowiązki związane z obszarem C-SCRM, a osoby pełniące te role powinny uczestniczyć w działaniach C-SCRM w całym podmiocie. Rozdział 2 i Załącznik C zawierają szczegółowe wytyczne dotyczące ról oraz zakresów odpowiedzialności związanych z obszarem C-SCRM.

Poziom(y): 1

PM-30 STRATEGIA ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Strategia zarządzania ryzykiem w łańcuchu dostaw (określana także mianem strategii C-SCRM) powinna być uzupełniona o plan wdrożenia C-SCRM, który określa szczegółowe inicjatywy i działania dla podmiotu wraz z harmonogramem i osobami odpowiedzialnymi za ich realizację. Ten plan wdrożenia może stanowić plan działań i etapów lub jego część. Na podstawie strategii C-SCRM i planu wdrożenia na poziomie 1 podmiot powinien określić i udokumentować środki bezpieczeństwa związane z obszarem C-SCRM, które powinny odpowiadać potrzebom podmiotu, programu i systemu. Wybrane środki bezpieczeństwa powinny być iteracyjnie włączane do polityki C-SCRM na poziomach 1 i 2, a także planu C-SCRM (lub planu bezpieczeństwa systemu, jeśli jest wymagany) na poziomie 3. Dodatkowe wytyczne dotyczące zarządzania ryzykiem znajdują się w rozdziale 2 oraz Załączniku C.

Poziom(y): 1, 2

Powiązane środki bezpieczeństwa: PL-2

PM-31 STRATEGIA CIĄGŁEGO MONITOROWANIA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Strategia i program ciągłego monitorowania powinny obejmować środki bezpieczeństwa związane z obszarem C-SCRM na poziomach 1, 2 i 3 zgodnie ze strategią zarządzania ryzykiem w łańcuchu dostaw.

Poziom(y): 1, 2, 3

Powiązane środki bezpieczeństwa: PM-30

PM-32 PRZEZNACZENIE

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Rozszerzanie przeznaczenia systemów wykorzystywanych do wspierania realizacji określonych misji lub działań naraża te systemy na niezamierzone ryzyko, w tym ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw. Stosowanie tego środka bezpieczeństwa powinno obejmować wyraźne uwzględnienie zagrożeń związanych z cyberbezpieczeństwem w całym łańcuchu dostaw.

Poziom(y): 2, 3

KATEGORIA PS: BEZPIECZEŃSTWO OSOBOWE

Dokument [NSC 200] określa minimalne wymagania bezpieczeństwa w zakresie bezpieczeństwa pracowników w następujący sposób:

> *Organizacje powinny: (I) zapewnić, aby osoby zajmujące odpowiedzialne stanowiska w organizacjach (w tym zewnętrzni dostawcy usług) były godne zaufania i spełniały ustalone kryteria bezpieczeństwa dla tych stanowisk; (II) zapewnić ochronę informacji i systemów informacyjnych organizacji w trakcie i po działaniach personalnych, takich jak rozwiązania umowy o pracę (współpracy) i zmiana zajmowanych stanowisk; oraz (III) stosować formalne sankcje za brak przestrzegania przez personel zasad i procedur bezpieczeństwa organizacyjnego.*

Pracownicy, którzy mają dostęp do łańcucha dostaw podmiotu, powinni być objęci środkami bezpieczeństwa wdrożonymi przez podmiot. Lista takich pracowników obejmuje specjalistów do spraw zamówień i zaopatrzenia, specjalistów do spraw zawierania umów, menadżerów programów, specjalistów do spraw łańcucha dostaw i logistyki, pracowników odpowiedzialnych za logistykę, wysyłki oraz odbiór, specjalistów do spraw technologii informacyjnych, specjalistów do spraw jakości, osoby odpowiedzialne za misje i procesy biznesowe, a także inżynierów do spraw bezpieczeństwa informacji. Podmioty powinny również współpracować z dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT w celu zapewnienia, że pracownicy mający styczność z łańcuchami dostaw podmiotu, są objęci stosownymi środkami bezpieczeństwa.

PS-1 POLITYKA I PROCEDURY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Na każdym poziomie polityka i procedury bezpieczeństwa dotyczące pracowników oraz związane z nimi strategie i plany wdrożenia C-SCRM, zasady C-SCRM oraz plany C-SCRM muszą określać role pracowników zaangażowanych w Proces nabycia, zarządzanie i realizację działań związanych z bezpieczeństwem łańcucha dostaw. Role te muszą również określać

obowiązki pracowników jednostki nabywającej w odniesieniu do relacji z dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych oraz innymi dostawcami usług związanych z ICT/OT. Polityki i procedury muszą uwzględniać pełny cykl życia rozwoju systemów oraz role i obowiązki wymagane do realizacji różnych działań związanych z infrastrukturą łańcucha dostaw.

Poziom 1: Stosowne role obejmują osoby odpowiedzialne za zarządzanie ryzykiem, CIO, CISO, osoby odpowiedzialne za umowy, logistykę, dostawy/odbiór, bezpieczeństwo zaopatrzenia i inne role, które zapewniają wsparcie działań w ramach łańcucha dostaw.

Poziom 2: Stosowne role obejmują menedżerów programów oraz osoby (np. wykonawcy) w ramach jednostki nabywającej, odpowiedzialnych za realizację programu (np. menadżer programu i inne osoby).

Poziom 3: Stosowne role obejmują inżynierów systemowych lub inżynierów ds. bezpieczeństwa systemu w całym cyklu życia systemu, począwszy od określenia wymagań, poprzez rozwój, testowanie, wdrażanie, utrzymanie, aktualizacje, wymianę, dostawę/odbiór oraz IT.

Role dostawcy, dewelopera, integratora systemu, dostawcy zewnętrznych usług systemowych oraz innych pracowników dostawcy usług związanych z ICT/OT odpowiedzialnych za realizację programu powinny być zapisane w umowie między jednostką nabywającą i tymi stronami.

Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Poziom(y): 1, 2, 3

Powiązane środki bezpieczeństwa: SA-4

PS-3 DOBÓR PERSONELU

Dodatkowe wytyczne dotyczące obszaru C-SCRM: W celu zmniejszenia ryzyka związanego z zagrożeniami wewnętrznymi, polityka i procedury zabezpieczeń personelu powinny być rozszerzone na wszystkich pracowników wykonawcy posiadających uprawnienia dostępu do systemów informacyjnych, komponentów systemu lub usług systemu informacyjnego. Działania w zakresie ciągłego monitorowania powinny być współmierne do poziomu dostępu wykonawcy do informacji wrażliwych, kontrolowanych i niejawnych oraz powinny być zgodne z szeroko pojętymi zasadami podmiotu. Wymogi dotyczące kontroli powinny zostać włączone do umów i przekazane podwykonawcom.

Poziom(y): 2, 3

PS-6 UMOWY DOSTĘPU / WSPÓŁPRACY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien opracować oraz udokumentować umowy dotyczące dostępu dla wszystkich wykonawców lub pracowników zewnętrznych, którzy mogą potrzebować fizycznego lub logicznego dostępu do danych, systemów lub sieci podmiotu. Umowy dotyczące dostępu powinny określać stosowny poziom i sposób dostępu do systemu informacyjnego i sieci łańcucha dostaw. Ponadto warunki dostępu powinny być zgodne z polityką bezpieczeństwa informacji podmiotu i mogą wymagać określenia dodatkowych ograniczeń, takich jak zezwolenie na dostęp w określonych przedziałach czasowych, z określonych miejsc lub tylko przez pracowników, którzy spełnili dodatkowe wymogi lub zostali zweryfikowani i sprawdzeni. Podmiot powinien wdrożyć mechanizmy kontrolne, aby przeglądać, monitorować, aktualizować i śledzić dostęp tych pracowników pod kątem zgodności z umową. Ze względu na to, że lista pracowników zmienia się w czasie, podmiot powinien wdrożyć terminowy i rygorystyczny proces aktualizacji dotyczący umów dotyczących dostępu. Jeżeli systemy informacyjne oraz produkty i usługi sieciowe są dostarczane

przez jednostkę w ramach podmiotu, mogą istnieć wcześniejsze umowy dotyczące dostępu. W przypadku braku takiej umowy, należy ją opracować.

Uwaga: O ile mechanizmy kontroli mogą być wdrożone na poziomie 3, proces podpisywania umów oraz ich aktualizacji powinien być wdrożony na poziomie 2 jako część działań związanych z zarządzaniem programem.

Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Poziom(y): 2, 3

PS-7 BEZPIECZEŃSTWO OSOBOWE STRON TRZECICH

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Pracownicy zewnętrzni, którzy mają dostęp do systemów i sieci informacyjnych podmiotu, musi spełniać te same wymogi bezpieczeństwa co pracownicy podmiotu. Przykłady takich pracowników mogą obejmować integratora systemu, dewelopera, dostawcę, dostawcę zewnętrznych usług systemowych, wykonawców lub usługodawców, którzy korzystają z systemów ICT/OT, a także pracowników utrzymania przysłanych przez dostawcę w celu rozwiązania problemów technicznych dotyczących komponentów systemu, których nie może rozwiązać podmiot lub integrator systemu.

Poziom(y): 2

KATEGORIA PT: PRZEJRZYSTOŚĆ PRZETWARZANIA DANYCH OSOBOWYCH

Przejrzystość przetwarzania danych osobowych to nowa rodzina środków zabezpieczających stworzona z myślą o rozwiązywaniu problemów związanych z przetwarzaniem i przejrzystością danych osobowych.

Podmiot powinien mieć na uwadze, że niektórzy dostawcy wdrożyli kompleksowe praktyki i systemy dotyczące bezpieczeństwa i prywatności, które mogą wykraczać poza wymagania podmiotu. Podmioty powinny współpracować z dostawcami w celu zrozumienia zakresu ich praktyk w zakresie ochrony prywatności oraz sposobu, w jaki spełniają one potrzeby podmiotu.

PT-1 POLITYKA I PROCEDURY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zapewnić, że kwestie związane z łańcuchem dostaw są uwzględnione w zasadach i procedurach dotyczących przetwarzania i przejrzystości danych osobowych, a także powiązanych dokumentach dotyczących obszaru C-SCRM – strategii, planu wdrożenia, polityce C-SCRM oraz planie C-SCRM. Zasady te mogą stanowić element ogólnej polityki bezpieczeństwa i prywatności lub mogą stanowić część wielu polityk.

Procedury mogą być ustanowione dla programu bezpieczeństwa i prywatności lub dla poszczególnych systemów informacyjnych. Zasady i procedury powinny dotyczyć celu, zakresu, ról, odpowiedzialności, zaangażowania kierownictwa, koordynacji między jednostkami podmiotu oraz zgodności z zasadami ochrony prywatności w celu wspierania systemów/komponentów w ramach systemów informacyjnych lub łańcucha dostaw.

Należy wprowadzić stosowne polityki i procedury, aby zapewnić, że umowy określają, jakie dane osobowe będą udostępniane, którzy pracownicy wykonawcy mogą mieć dostęp do danych osobowych, jakie środki bezpieczeństwa posłużą ochronie danych osobowych, jak długo potrwa przechowywanie tych danych i co się z nimi stanie po zakończeniu umowy.

a. W przypadku współpracy z nowym dostawcą należy upewnić się, że umowa zawiera najbardziej aktualny zestaw obowiązujących wymogów w zakresie bezpieczeństwa.

b. Wykonawcy muszą przestrzegać odpowiednich przepisów i polityk dotyczących bezpieczeństwa informacji (ochrony danych osobowych i innych informacji wrażliwych).

c. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Poziom(y): 1, 2, 3

KATEGORIA RA: OCENA RYZYKA

Dokument [NSC 200] określa minimalne wymagania bezpieczeństwa w zakresie oceny ryzyka w następujący sposób:

> *Organizacje powinny okresowo oceniać ryzyko odnoszące się do operacji organizacyjnych (w tym misji, funkcji, wizerunku lub reputacji), zasobów organizacyjnych i osób fizycznych, wynikających z działania organizacyjnych systemów informacyjnych i związanego z nimi przetwarzania, przechowywania lub przekazywania informacji organizacyjnych.*

Niniejszy dokument zawiera wytyczne dotyczące zarządzania ryzykiem związanym z cyberbezpieczeństwem podmiotu w łańcuchach dostaw i rozszerza zakres środków bezpieczeństwa o włączenie ocen ryzyka związanego z cyberbezpieczeństwem w łańcuchach dostaw. Więcej informacji znajduje się w rozdziale 2 i *Załączniku C*.

RA-1 POLITYKA I PROCEDURY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Oceny ryzyka powinny być przeprowadzane na poziomach podmiotu, misji/programu i operacyjnym. Ocena ryzyka na poziomie systemu powinna obejmować zarówno infrastrukturę łańcucha dostaw (np. środowiska rozwojowe i testowe oraz systemy dostaw), jak i systemy informacyjne oraz jego komponenty przechodzące przez łańcuch dostaw. Oceny ryzyka na poziomie systemu są w dużym stopniu związane z cyklem życia systemu i powinny wpisywać się w szersze działania podmiotu w zakresie ram zarządzania ryzykiem, które są realizowane w czasie cyklu życia systemu. Analiza krytyczności zapewni, że kluczowe funkcje i komponenty otrzymają wyższy priorytet ze względu na ich wpływ na realizację misji, jeśli nastąpi naruszenie ich zasad bezpieczeństwa. Zasady powinny obejmować role związane z cyberbezpieczeństwem w łańcuchu dostaw oraz ich związek z przeprowadzaniem oraz koordynowaniem ocen ryzyka w całym podmiocie (wykaz i opis ról znajduje się w rozdziale 2). Należy określić odpowiednie role w przypadku dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT.

Poziom(y): 1, 2, 3

RA-2 KATEGORYZACJA BEZPIECZEŃSTWA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Kategoryzacja zabezpieczeń w ramach działań związanych z obszarem C-SCRM jest kluczowa na każdym z trzech poziomów. Oprócz kategorii określonych w dokumencie [NSC 199], kategoryzacja zabezpieczeń w obszarze C-SCRM powinna być oparta na analizie krytyczności wykonanej w ramach cyklu życia systemu. Szczegółowy opis analizy krytyczności znajduje się w rozdziale 2 oraz w dokumencie [NISTIR 8179].

Poziom(y): 1, 2, 3

Powiązane środki bezpieczeństwa: RA-9

RA-3 SZACOWANIE RYZYKA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Ocena ryzyka powinna obejmować analizę krytyczności, zagrożeń, podatności, prawdopodobieństwa i wpływu – zostało to szczegółowo opisane w Załączniku C. Informacje, które należy zgromadzić i poddać przeglądowi, obejmują role, procesy i rezultaty nabycia, wdrażania i integracji systemów/komponentów oraz usług związanych z obszarem C-SCRM. Ocena ryzyka powinna być przeprowadzona na poziomach 1, 2 i 3. Oceny ryzyka na wyższych poziomach powinny obejmować zestawienia różnych ocen ryzyka przeprowadzonych na niższych poziomach i powinny przyczyniać się do zrozumienia ogólnego wpływu na dany poziom (np. na poziom podmiotu lub misji/działania). Oceny ryzyka związanego z obszarem C-SCRM powinny uzupełniać oceny ryzyka wykonywane w ramach całego cyklu życia systemu, a procesy powinny być odpowiednio dopasowane lub włączone do procesów zarządzania ryzykiem w podmiocie.

Poziom(y): 1, 2, 3

Powiązane środki bezpieczeństwa: RA-3(1)

RA-5 MONITOROWANIE I SKANOWANIE PODATNOŚCI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Monitorowanie podatności powinno obejmować dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT w łańcuchu dostaw podmiotu. Działanie to powinno obejmować stosowanie narzędzi do gromadzenia danych w celu zapewnienia wiedzy na temat możliwych podatności po stronie dostawców, a także systemów informacyjnych, komponentów systemu i surowych danych wejściowych, które są dostarczane w ramach łańcucha dostaw cyberbezpieczeństwa. Działania związane z monitorowaniem podatności powinny odbywać się na wszystkich trzech poziomach podmiotu. Ustalenie zakresu działań związanych z monitorowaniem podatności wymaga od podmiotów uwzględnienia zarówno dostawców, jak i ich poddostawców. W stosownych przypadkach podmiot może dostarczyć klientom sprawozdanie (*ang. Vulnerability Disclosure Report – VDR*) zawierające informacje o podatnościach, aby w ten sposób przedstawić kompleksową ocenę podatności komponentów wymienionych w specyfikacjach materiałowych komponentów oprogramowania. Sprawozdanie powinno zawierać analizę oraz wnioski opisujące wpływ (lub brak wpływu) podatności na komponent lub produkt. Sprawozdanie powinno również zawierać informacje na temat planów dotyczących CVE. Podmioty powinny rozważyć opublikowanie sprawozdania w ramach bezpiecznego portalu dostępnego dla klientów oraz podpisanie go zaufanym, weryfikowalnym kluczem prywatnym, który zawiera znacznik czasu wskazujący datę i godzinę podpisania i dokumentu. Podmioty powinny również rozważyć ustanowienie osobnego kanału informacyjnego dla klientów w przypadku pojawienia się podatności, które nie zostały ujawnione w sprawozdaniu. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *MONITOROWANIE I SKANOWANIE PODATNOŚCI | SZEROKOŚĆ I GŁĘBOKOŚĆ POKRYCIA*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty monitorujące łańcuch dostaw pod kątem podatności na zagrożenia powinny określić zakres monitorowania w oparciu o krytyczność oraz profil ryzyka dostawcy lub produktu/komponentu oraz głębokość monitorowania w oparciu o poziom łańcucha dostaw, na którym odbywa się monitorowanie. Jeśli jest dostępny, wykaz komponentów (np. urządzeń, oprogramowania) może pomóc podmiotom w określeniu zakresu i głębokości monitorowania i skanowania produktów i komponentów stanowiących część ich łańcuchów dostaw pod kątem podatności.

Poziom(y): 2, 3

2. *MONITOROWANIE I SKANOWANIE PODATNOŚCI | AUTOMATYCZNA ANALIZA TRENDÓW*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny śledzić trendy dotyczące podatności komponentów w ramach łańcucha dostaw w czasie. Informacje te mogą pomóc im w opracowaniu strategii zamówień, które zmniejszą narażenie na ryzyko w ramach łańcucha dostaw.

Poziom(y): 2, 3

RA-7 REAKCJA NA RYZYKO

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny włączyć zdolności reagowania na zagrożenia związane

z cyberbezpieczeństwem w całym łańcuchu dostaw do ogólnej strategii reagowania na ryzyko, upewniając się, że reakcje te są dostosowane do tolerancji ryzyka podmiotu i mieszczą się w jej granicach. Reakcja na ryzyko powinna obejmować określenie reakcji na ryzyko, ocenę rozwiązań alternatywnych oraz działania decyzyjne w zakresie reakcji.

Poziom(y): 1, 2, 3

RA-9 ANALIZA KRYTYCZNOŚCI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny przeprowadzić analizę krytyczności, która stanowi podstawę oceny działań związanych z zarządzaniem ryzykiem w zakresie cyberbezpieczeństwa w całym łańcuchu dostaw. W pierwszej kolejności podmioty powinny przeprowadzić analizę krytyczności w ramach etapu ujmowania ryzyka będącego częścią procesu zarządzania ryzykiem związanym z obszarem C-SCRM. Następnie ustalenia uzyskane w ramach działań na etapie oceny (np. analiza krytyczności, analiza podatności, analiza zagrożeń czy strategie ograniczania ryzyka) wpływają na aktualizację oraz dostosowanie analizy krytyczności. Między analizą krytyczności a innymi działaniami w ramach etapu oceny istnieje relacja symbiozy z racji tego, że wpływają na siebie nawzajem. W celu uzyskania wysokiej jakości analizy krytyczności, podmioty powinny stosować ją w sposób powtarzalny w całym cyklu życia systemu i realizować ją równolegle na trzech poziomach. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się także z treścią załącznika F.

Poziom(y): 1, 2, 3

RA-10 WYSZUKIWANIE ZAGROŻEŃ

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Działania w obszarze C-SCRM związane z poszukiwaniem zagrożeń powinny uzupełniać

wewnętrzne działania podmiotu związane z tym zagadnieniem. Podmioty powinny aktywnie monitorować zagrożenia dla swojego łańcucha dostaw, co stanowi kluczową część procesu zarządzania ryzykiem dotyczącego cyberbezpieczeństwa w łańcuchu dostaw. Wymaga to współpracy pomiędzy jednostkami odpowiedzialnymi za działania w obszarze C-SCRM oraz innymi jednostkami podmiotu zajmującymi się cyberbezpieczeństwem. Możliwości w zakresie poszukiwania zagrożeń mogą być także realizowane z pomocą podmiotu świadczącego usługi wspólne, zwłaszcza gdy dany podmiot nie posiada zasobów pozwalających na samodzielne prowadzenie tego rodzaju działań. Typowe działania obejmują wymianę informacji z innymi podmiotami oraz aktywne korzystanie ze źródeł informacji o zagrożeniach (np. dostępnych w Centrach Zapewniania i Analiz Informacji [*ang. Information Assurance and Analysis Centers - ISAC*] oraz Organizacjach Zapewniania i Analiz Informacji [*ang. Information Assurance and Analysis Organizations - ISAO*]). Działania te mogą pomóc w określeniu oraz dostrzeżeniu wskaźników zwiększonego ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw, takich jak incydenty związane z cyberbezpieczeństwem, fuzje i przejęcia, a także zagraniczną własność, kontrolę lub wpływy (*ang. Foreign Ownership, Control, or Influence – FOCI*). Osoby odpowiedzialne za poszukiwanie zagrożeń w łańcuchu dostaw powinny skupić się na zagrożeniach dla dostawców podmiotu, a także systemów informacyjnych, komponentów systemu oraz dostarczanych przez nich danych. Zebrane dane umożliwiają podmiotom proaktywne identyfikowanie i reagowanie na zagrożenia płynące z łańcucha dostaw.

Poziom(y): 1, 2, 3

Tłumaczenie

RODZINA SA: NABYWANIE SYSTEMU I USŁUG

Dokument [NSC 200] określa minimalne wymagania bezpieczeństwa w zakresie nabywania systemów oraz usług w następujący sposób:

> *Organizacje powinny: (I) alokować wystarczające zasoby, zapewniające odpowiednią ochronę organizacyjnych systemów informacyjnych; (II) stosować procesy cyklu życia rozwoju systemu, które uwzględniają względy bezpieczeństwa informacji; (III) stosować ograniczenia dotyczące używania oprogramowania i instalacji; oraz (IV) zapewnić, aby dostawcy zewnętrzni stosowali adekwatne środki bezpieczeństwa w celu ochrony informacji, aplikacji i/lub usług zleconych przez organizację.*

Podmioty nabywają produkty i usługi ICT/OT poprzez zakup systemów i usług. Opisane środki bezpieczeństwa dotyczą działań nabywców, dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych, innych dostawców usług związanych z ICT/OT oraz powiązanych jednostek w ramach łańcucha dostaw. Dotyczą one zarówno fizycznych, jak i logicznych aspektów bezpieczeństwa łańcucha dostaw, od wykrywania po kwestie cyklu życia SDLC (*ang. System Development Life Cycle*) systemu i zasady inżynierii bezpieczeństwa. Zagadnienia związane z obszarem C-SCRM zostały szeroko omówione w dokumencie [NSC 800-53]. Niniejszy dokument uzupełnia te informacje o dodatkowe szczegóły oraz rozwija opisane środki bezpieczeństwa.

SA-1 POLITYKA I PROCEDURY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Zasady i procedury nabywania systemów i usług powinny uwzględniać zagadnienia związane z obszarem C-SCRM w całym procesie cyklu życia zamówienia. Działania dotyczące obszaru C-SCRM iw zamówieniach oraz wynikające z nich umowy powinny obejmować wymagania oraz klauzule, które dotyczą obowiązkowych i pożądanych środków bezpieczeństwa. Mogą obejmować specyfikacje wdrożeniowe, akceptowalne potwierdzenia spełnienia wymogów, a także informacje na temat weryfikacji i zatwierdzania zgodności z wymogami. Zagadnienia dotyczące obszaru C-SCRM powinny być włączone w proces oceny dostawcy.

Zamówienia, których dotyczą powyższe zasady, nie powinny być ograniczone wyłącznie do tych, które są bezpośrednio związane z pozyskaniem produktu lub usługi ICT/OT. Choć zagadnienia dotyczące obszaru C-SCRM wiążą się w szczególności z takimi zamówieniami, kwestie dotyczące tego obszaru powinny być także brane pod uwagę w przypadku wszelkich zamówień produktów lub usług, w których może istnieć niedopuszczalne ryzyko, że dostarczony produkt lub wykonawca usługi naruszy integralność, dostępność lub poufność informacji podmiotu. Ta wstępna ocena powinna mieć miejsce podczas fazy planowania nabycia i być w pewnym stopniu oparta na określeniu i zrozumieniu krytyczności misji podmiotu, jego zasobów o wysokiej wartości oraz wrażliwości informacji, do których może mieć dostęp dostawca produktu lub usług.

Ponadto podmioty powinny opracować zasady i procedury dotyczące ryzyka związanego z łańcuchem dostaw, które może pojawić się w trakcie realizacji umowy, np. w przypadku zmiany właściciela, przejęcia kontroli nad danym podmiotem, lub sytuacji uzyskania informacji, które wskazują, że dostawca lub produkt jest celem ataku na łańcuch dostaw. Łańcuchy dostaw stale się zmieniają w wyniku przejęć i fuzji, tworzenia spółek joint venture oraz zawierania umów partnerskich. Zasady i polityki powinny pomagać podmiotom w zrozumieniu zmian oraz wykorzystaniu zdobytych informacji do rozwoju swoich działań w zakresie C-SCRM. Podmioty mogą uzyskać informacje o takich zmianach między innymi poprzez śledzenie publicznych ogłoszeń dotyczących działalności podmiotów oraz wszystkich komunikatów i informacji przekazywanych przez dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych i innych dostawców usług związanych z ICT/OT.

Dodatkowe wytyczne dotyczące działań związanych z obszarem C-SCRM w ramach procesów zamówień znajdują się w rozdziale 3. Organizacje powinny ponadto zapoznać się z treścią załącznika F.

Poziom(y): 1, 2, 3

SA-2 PRZYDZIAŁ ZASOBÓW

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien uwzględnić wymagania dotyczące obszaru C-SCRM przy przydzielaniu zasobów.

Poziom(y): 1, 2

SA-3 CYKL ŻYCIA SYSTEMU

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Istnieje silny związek pomiędzy cyklem życia systemów a działaniami związanymi z obszarem C-SCRM. Podmiot powinien zapewnić, że działania związane z obszarem C-SCRM są włączone do cyklu życia systemu zarówno po stronie podmiotu, jak i po stronie dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT. Oprócz tradycyjnych działań związanych z cyklem życia systemu, takich jak wymagania i projektowanie, cykl życia systemu obejmuje takie działania jak zarządzanie zapasami, zamówienia i zaopatrzenie oraz dostarczanie systemów i ich komponentów. Dodatkowe wytyczne dotyczące cyklu życia systemu znajdują się w rozdziale 2 oraz Załączniku C. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 1, 2, 3

SA-4 PROCES NABYCIA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty włączają wymogi, opisy i kryteria dotyczące obszaru C-SCRM do odpowiednich umów:

1. Zobowiązane są ustanowić bazowe (podstawowe) i dostosowywane do indywidualnych potrzeb wymogi dotyczące obszaru C-SCRM, które będą stosowane i włączane do umów podczas nabywania produktów lub usług od dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych i innych dostawców usług związanych z ICT/OT. Powinny one obejmować między innymi:

a. Wymogi w zakresie C-SCRM, które obejmują obowiązujące prawo (np. zakaz stosowania wybranych technologii lub korzystania z usług wybranych dostawców), dotyczą określonych oraz wybranych środków bezpieczeństwa, których celem jest zmniejszenie ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw związanego z zamawianym produktem lub zamawianą usługą, a także zapewnienie, że wykonawca jest wystarczająco odpowiedzialny, godny zaufania i dysponuje odpowiednimi możliwościami.

b. Wymogi dotyczące krytycznych elementów łańcucha dostaw w celu wykazania zdolności do usuwania podatności w oparciu o uzyskane informacje z rożnych źródeł.

c. Wymogi dotyczące zarządzania własnością intelektualną i odpowiedzialnością za takie elementy jak kod oprogramowania, dane i informacje, środowisko produkcyjne, rozwojowe lub integracyjne, projekty oraz zastrzeżone procesy, gdy są one udostępniane podmiotowi do wglądu lub wykorzystania.

d. Wymogi dotyczące oczekiwanego okresu eksploatacji produktu lub systemu, wszelkich elementów, które mogą zostać uznane za krytyczne ze względu na ich przewidziany okres eksploatacji, a także wymogi związane z zakończeniem rozwoju lub eksploatacji rozwiązania. Podmioty powinny przeprowadzić badania lub zwrócić się o informacje do oferentów lub obecnych dostawców w ramach umowy, aby dowiedzieć się więcej na temat dostępnych rozwiązań w przypadku zakończenia rozwoju lub eksploatacji (np. wymiana, modernizacja, migracja do nowego systemu itp.)

e. Należy uwzględnić wszelkie okoliczności, w których dopuszczalne jest zastosowanie komponentów pochodzących z rynku wtórnego.

f. Wymagania dotyczące cech funkcjonalnych, konfiguracji i wdrożenia, a także metod, technik oraz praktyk rozwojowych, które mogą być istotne dla procesu. Określenie kryteriów oceny C-SCRM, w tym wagi takich kryteriów.

2. Powinny:

a. Opracować plan nabywania części zamiennych w celu zapewnienia odpowiednich zapasów oraz zrealizować go, gdy będzie to konieczne;

b. Opracować plan zdobywania alternatywnych źródeł dostaw, które mogą być niezbędne podczas zdarzeń zagrażających ciągłości działalności lub w przypadku wystąpienia zakłóceń w łańcuchu dostaw;

c. Współpracować z dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych i innymi dostawcami usług związanych z ICT/OT w celu określenia istniejących i akceptowalnych procesów reagowania na incydenty i wymiany informacji, w tym informacji o podatnościach pochodzących od innych podmiotów w ich łańcuchach dostaw.

3. Ustanawiają i utrzymują procedury weryfikacji i kryteriów akceptacji dla dostarczonych produktów i usług, które obejmują m.in.:

a. Przyjmowanie produktów komercyjnych i rządowych bez weryfikacji, zgodnie z upoważnieniem podmiotu (np. według listy zatwierdzonych produktów)

b. Weryfikację przez dostawcę podatności sprzętowych i programowych systemów informacyjnych dostępnych w obrocie komercyjnym.

4. Zapewniają, że kryteria planu ciągłego monitorowania obejmują aspekty łańcucha dostaw, takie jak uwzględnienie monitorowania

funkcji, portów i stosowanych protokołów. Więcej informacji znajduje się w rozdziale 2 i załączniku C.

5. Zapewniają, że umowa obejmuje monitorowanie systemów informacyjnych dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT znajdujących się w infrastrukturze łańcucha dostaw. W stosownych przypadkach zapewniają monitorowanie i oceny nabytych efektów pracy oraz procesów. Wymóg ten dotyczy między innymi monitorowanie infrastruktury rozwoju oprogramowania pod kątem podatności (np. procedur DevSecOps [*ang. development, security, and operations*], kontenerów i repozytoriów kodu).
6. Informują o procesach zgłaszania podatności w zakresie bezpieczeństwa informacji wykrytych podczas korzystania z produktów lub usług ICT/OT oraz zapewniają zgłaszania ich odpowiednim interesariuszom, w tym w stosownych przypadkach producentom.
7. Przeglądają oraz potwierdzają przestrzeganie warunków umowy na bieżąco.

Organizacje powinny zapoznać się z treścią załącznika.

Poziom(y): 1, 2, 3

Powiązane środki bezpieczeństwa: SA-4 (1), (2), (3), (6) i (7)

Zabezpieczenia rozszerzone:

1. *PROCES NABYCIA | KONFIGURACJA SYSTEMÓW, KOMPONENTÓW I USŁUG*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Jeśli podmiot chce dokonać zakupu komponentów, musi upewnić się, że specyfikacje produktu są odpowiednie i spełniają jego wymagania, niezależnie od tego, czy zakup odbywa się bezpośrednio od producenta, partnerów handlowych czy na rynku wtórnym.

Poziom(y): 3

2. *PROCES NABYCIA | PROFILE OCHRONY ZATWIERDZONE PRZEZ NIAP*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: To zabezpieczenie rozszerzone wymaga, aby podmiot opracowywał, pobierał oraz korzystał z certyfikowanych komponentów, zapewniających bezpieczeństwo informacji. Przykładowo certyfikat NIAP dotyczy oprogramowania komercyjnego i rządowego.

Poziom(y): 2, 3

3. *PROCES NABYCIA | PLAN CIĄGŁEGO MONITOROWANIA ŚRODKÓW BEZPIECZEŃSTWA*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: To zabezpieczenie rozszerzone jest istotne z punktu widzenia działań w obszarze C-SCRM i planów ciągłego monitorowania skuteczności zabezpieczeń i dlatego powinno być rozszerzone na dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych i innych dostawców usług związanych z ICT/OT.

Poziom(y): 2, 3

SA-5 DOKUMENTACJA SYSTEMU

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Dokumentacja systemu informacyjnego powinna zawierać odpowiednie zagadnienia związane z obszarem C SCRM (np. plan C-SCRM). Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 3

SA-8 ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Poniższe techniki inżynierii bezpieczeństwa są pomocne w zarządzaniu ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw.

a. Podmioty powinny przewidzieć, w jaki sposób produkt lub usługa ICT/OT mogą zostać nadużyte lub wykorzystane, aby określić możliwości ochrony produktu lub systemu przed takim wykorzystaniem. Należy przy tym odnieść się do zamierzonych i niezamierzonych scenariuszy użycia w architekturze i projektowaniu.

b. Projektowanie architektur sieci i bezpieczeństwa, systemów i komponentów powinno opierać się na tolerancji ryzyka podmiotu, określonej na podstawie ocen ryzyka (patrz rozdział 2 i załącznik C).

c. Należy udokumentować i uzyskać akceptację kierownictwa dla ryzyka, którego zakres nie jest w pełni ograniczony.

d. Należy ograniczyć liczbę, zakres oraz poziom uprawnień elementów krytycznych. Należy przeprowadzić ocenę krytyczności w celu określenia, które elementy lub funkcje są krytyczne. Więcej informacji na temat analizy krytyczności znajduje się w Załączniku C i dokumencie NISTIR 8179, *Criticality Analysis Process Model*: *Prioritizing Systems and Components*.

e. Należy stosować mechanizmy bezpieczeństwa, które pomagają ograniczyć możliwości wykorzystania podatności w zabezpieczeniach łańcucha dostaw, takie jak szyfrowanie, kontrola dostępu, zarządzanie tożsamością oraz wykrywanie złośliwego oprogramowania lub manipulacji.

f. Należy projektować komponenty i elementy systemu informacyjnego tak, aby były trudne do wyłączenia (np. Stosując techniki zabezpieczania przed manipulacją), a jeśli zostaną wyłączone, należy uruchomić metody powiadamiania, takie jak ścieżki audytu, informacje o manipulacji lub alarmy.

g. Należy zaprojektować mechanizmy dostarczania (np. pobieranie oprogramowania) w taki sposób, aby uniknąć niepotrzebnego narażenia lub dostępu do łańcucha dostaw oraz systemów/komponentów przemieszczających się przez łańcuch dostaw w czasie procesu.

h. Należy zaprojektować odpowiednie mechanizmy weryfikacji, które będą stosowane podczas wdrażania i eksploatacji.

Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 1, 2, 3

SA-9 USŁUGI SYSTEMU ZEWNĘTRZNEGO

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Dodatkowe wytyczne dotyczące obszaru C-SCRM zostały przedstawione w formie zabezpieczeń rozszerzonych.

Zabezpieczenia rozszerzone:

1. *USŁUGI SYSTEMU ZEWNĘTRZNEGO | OCENY RYZYKA I ZATWIERDZENIA*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Więcej informacji znajduje się w załącznikach C i D. Organizacje powinny ponadto zapoznać się z treścią załącznika F.

Poziom(y): 2, 3

2. *USŁUGI SYSTEMU ZEWNĘTRZNEGO | USTANOWIENIE I UTRZYMANIE RELACJI OPARTYCH NA ZAUFANIU Z DOSTAWCAMI*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Relacje z dostawcami[46] powinny spełniać następujące wymogi związane z bezpieczeństwem łańcucha dostaw:

[46] W kontekście niniejszego zabezpieczenia rozszerzonego pojęcie „dostawcy" może obejmować podmioty takie jak dostawcy, deweloperzy, integratorzy systemów, dostawcy zewnętrznych usług systemowych oraz dostawców innych usług dotyczących ICT/OT.

a. Określenie kompleksowych wymagań oraz poddanie ich przeglądowi pod kątem dokładności i kompletności, w tym przypisanie poziomów krytyczności różnym komponentom oraz zdefiniowanie koncepcji operacyjnych i związanych z nimi scenariuszy zamierzonego i niezamierzonego użycia.

b. Wymagania powinny opierać się na potrzebach, odpowiednich czynnikach zgodności, analizie krytyczności oraz ocenie ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw.

c. Należy zidentyfikować i udokumentować zagrożenia dotyczące cyberbezpieczeństwa w całym łańcuchu dostaw, podatności oraz związane z nimi ryzyko.

d. Wymogi dotyczące integralności, poufności i dostępności danych i informacji w podmiocie powinny zostać określone i przekazane dostawcom, deweloperom, integratorom systemów, dostawcom zewnętrznych usług systemowych oraz innym dostawcom usług związanych z ICT/OT.

e. Należy określić i zawrzeć w dokumentach konsekwencje niezgodności z wymaganiami C-SCRM i wymaganiami bezpieczeństwa systemu informacyjnego.

f. Należy ustalić jasne rozgraniczenie odpowiedzialności, ról i obowiązków pomiędzy wykonawcami, gdy wielu różnych dostawców jest zaangażowanych we wspieranie systemu lub misji i funkcji biznesowej.

g. Wymagania powinny określać stan realizacji umowy o świadczenie usług oraz zakończenie współpracy z dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych lub innymi dostawcami usług związanych z ICT/OT. Jest to ważne z punktu widzenia

konkurencji, możliwości zmiany dostawcy oraz zarządzania procesami związanymi z zakończeniem eksploatacji systemu.

h. Należy wynegocjować oraz uwzględnić zapisy umowne dotyczące zakończenia relacji w celu zapewnienia bezpiecznego zakończenia współpracy, obejmującego na przykład usunięcie danych ze środowisk chmurowych.

Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 1, 2, 3

1. *USŁUGI SYSTEMU ZEWNĘTRZNEGO | SPÓJNE INTERESY KONSUMENTÓW I DOSTAWCÓW*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: W kontekście niniejszego zabezpieczenia rozszerzonego pojęcie „dostawcy” może obejmować podmioty takie jak dostawcy, deweloperzy, integratorzy systemów, dostawcy zewnętrznych usług systemowych oraz dostawców innych usług dotyczących ICT/OT.

Poziom(y): 3

2. *USŁUGI SYSTEMU ZEWNĘTRZNEGO | PRZETWARZANIE, PRZECHOWYWANIE I LOKALIZACJA USŁUG*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Lokalizacja usług może być pod kontrolą dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT. Podmioty powinny ocenić ryzyko związane z obszarem C-SCRM dotyczące danej lokalizacji geograficznej i odpowiednio zareagować na ryzyko, na przykład poprzez określenie nieakceptowalnych lokalizacji oraz wprowadzenie odpowiednich środków bezpieczeństwa w celu ograniczenia związanego z nimi ryzyka dotyczącego obszaru C-SCRM.

Poziom(y): 3

SA-10 ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Zarządzanie konfiguracją przez deweloperów stanowi klucz do ograniczania ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw. Prowadząc działania związane z zarządzaniem konfiguracją, deweloperzy eliminują wady i prawdopodobieństwo ich wystąpienia, jednocześnie zwiększając odpowiedzialność za zmiany. Zarządzanie konfiguracją powinno być wykonywane zarówno przez deweloperów wewnętrznych w organizacjach, jak i przez integratorów lub dostawców zewnętrznych usług systemowych. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

Powiązane środki bezpieczeństwa: SA-10 (1), (2), (3), (4), (5), (6)

SA-11 TESTOWANIE I OCENA PRZEZ DEWELOPERA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: W zależności od pochodzenia komponentów, ten środek bezpieczeństwa może być realizowany w różny sposób. W przypadku komponentów komercyjnych i rządowych, podmiot nabywający powinien przeprowadzić badania (np. na podstawie publicznie dostępnych materiałów) lub zażądać dowodów na potwierdzenie, czy dostawca (producent) przeprowadził rzeczone testy w ramach swoich procesów zapewnienia jakości lub bezpieczeństwa. Gdy podmiot nabywający ma kontrolę nad aplikacją i procesami rozwojowymi, powinien wymagać przeprowadzania tych testów w ramach cyklu życia systemu. Oprócz konkretnych rodzajów testów opisanych w zabezpieczeniach rozszerzonych, przykłady testów istotnych z punktu widzenia działań w obszarze C-SCRM obejmują testowanie autentyczności produktu, weryfikację pochodzenia komponentów, weryfikację konfiguracji przed jej zastosowaniem oraz testowanie interfejsów. Tego typu testy mogą wymagać przeznaczenia na ich realizację znaczących zasobów,

w związku z czym należy przeprowadzać je według priorytetu krytyczności na podstawie analiz krytyczności, zagrożeń i podatności (opisanych w rozdziale 2 i Załączniku C), a także skuteczności technik testowania. Podmioty mogą również wymagać testów przeprowadzonych przez podmioty zewnętrzne w ramach tego zabezpieczenia. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 1, 2, 3

Powiązane środki bezpieczeństwa: SA-11 (1), (2), (3), (4), (5), (6), (7), (8), (9)

SA-15 PROCES ROZWOJU, STANDARDY I NARZĘDZIA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Zapewnienie udokumentowanych i sformalizowanych procesów rozwoju w celu kierowania działaniami deweloperów wewnętrznych oraz integratorów systemów ma kluczowe znaczenie dla działań podmiotu w zakresie skutecznego ograniczania ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw. Podmiot powinien stosować krajowe i międzynarodowe normy/standardy oraz najlepsze praktyki podczas wdrażania tego środka bezpieczeństwa. Stosowanie istniejących norm sprzyja spójności wdrażania, niezawodności i możliwości obrony procesów oraz interoperacyjności. Środek bezpieczeństwa powinien dotyczyć wszystkich środowisk podmiotu – programistycznych, utrzymaniowych, testowych i wdrożeniowych. Narzędzia wchodzące w skład tego środka bezpieczeństwa mogą być ręczne lub zautomatyzowane. Zastosowanie zautomatyzowanych narzędzi zwiększa dokładność, efektywność i skalę analizy, co pomaga w rozwiązywaniu problemów związanych z zagrożeniami dla cyberbezpieczeństwa, które pojawiają się w związku z procesem rozwoju oprogramowania w całym łańcuchu dostaw. Dodatkowo, dane wyjściowe z takich działań i narzędzi stanowią użyteczny wkład dla procesów C-SCRM, jak opisano w rozdziale 2 i Załączniku C. Ten środek bezpieczeństwa ma zastosowanie do wewnętrznych procesów

podmiotu, systemów informacyjnych i sieci, jak również do procesów, systemów i sieci integratorów systemów. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

Powiązane środki bezpieczeństwa: Zabezpieczenia rozszerzone SA-15 (1), (2), (5), (6) i (7)

Zabezpieczenia rozszerzone:

1. *PROCES ROZWOJU, STANDARDY I NARZĘDZIA | ANALIZA KRYTYCZNOŚCI*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: To zabezpieczenie rozszerzone wskazuje krytyczne komponenty w ramach systemu informacyjnego, co pomaga w określeniu konkretnych działań w zakresie C-SCRM, które należy wdrożyć dla tych komponentów. Więcej informacji na ten temat znajduje się w sekcji Analiza Krytyczności na potrzeby procesów C-SCRM w Załączniku G.

Poziom(y): 2, 3

2. *PROCES ROZWOJU, STANDARDY I NARZĘDZIA | MODELOWANIE ZAGROŻEŃ I ANALIZY PODATNOŚCI*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: To zabezpieczenie rozszerzone zapewnia modelowanie zagrożeń i analizę podatności dla odpowiednich produktów, aplikacji, systemów informacyjnych i sieci organizacyjnych i wykonawców. Przeprowadzenie tej analizy pomoże włączyć działania związane z obszarem C-SCRM w prace związane z udoskonalaniem i modyfikacją kodu. Więcej informacji na ten temat znajduje się w sekcji poświęconej analizom zagrożeń i podatności na potrzeby procesów C-SCRM w Załączniku C.

Poziom(y): 2, 3

Powiązane środki bezpieczeństwa: SA-15(5), SA-15(6), SA-15(7)

3. *PROCES ROZWOJU, STANDARDY I NARZĘDZIA | PONOWNE WYKORZYSTANIE INFORMACJI O ZAGROŻENIACH I PODATNOŚCIACH*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: To zabezpieczenie rozszerzone zachęca programistów do ponownego wykorzystania informacji o zagrożeniach i podatnościach uzyskanych w wyniku wcześniejszych prac rozwojowych oraz wniosków wyciągniętych z użytkowania narzędzi w celu wykorzystania ich w bieżących pracach rozwojowych. Przeprowadzenie tego procesu pomoże w określeniu działań w zakresie C-SCRM opisanych w rozdziale 2 i Załączniku C.

Poziom(y): 3

SA-16 SZKOLENIA PROWADZONE PRZEZ DEWELOPERA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Szkolenia organizowane przez deweloperów dla zewnętrznych i wewnętrznych deweloperów są kluczowe z punktu widzenia obszaru C-SCRM. Środek bezpieczeństwa dotyczy szkolenia osób odpowiedzialnych za systemy i sieci organizacyjne, w tym ich środowiska rozwojowe. Zapewnione przez dewelopera szkolenie w zakresie tego środka bezpieczeństwa dotyczy również osób, które są odpowiedzialne za dobór komponentów systemu i sieci. Szkolenie powinno obejmować zagadnienia dotyczące obszaru C-SCRM, aby zapewnić, że 1) deweloperzy są świadomi potencjalnych zagrożeń i podatności podczas tworzenia, testowania i utrzymywania sprzętu i oprogramowania oraz że 2) osoby odpowiedzialne za wybór komponentów systemu i sieci uwzględniają zagadnienia dotyczące obszaru C-SCRM przy ich wyborze. Szkolenie powinno obejmować również wiedzę z zakresu bezpiecznych praktyk programistycznych oraz korzystania z narzędzi do wyszukiwania podatności w oprogramowaniu. Dodatkowe wytyczne dotyczące bezpieczeństwa oprogramowania krytycznego znajdują się w Załączniku F.

Poziom(y): 2, 3

Powiązane środki bezpieczeństwa: AT-3

SA-17 ARCHITEKTURA ORAZ PROJEKT BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI DEWELOPERA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Ten środek bezpieczeństwa ułatwia wykorzystanie zagadnień z obszaru C-SCRM do wpływania na architekturę systemu, projektowanie i decyzje dotyczące wyboru komponentów, w tym funkcji dotyczących bezpieczeństwa. Przykłady obejmują określenie komponentów składających się na architekturę i projekt systemu lub wybór określonych komponentów w celu zapewnienia dostępności poprzez wybór zróżnicowanych dostawców lub komponentów. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

Powiązane środki bezpieczeństwa: SA-17 (1) i (2)

SA-20 NIESTANDARDOWA (NA ZAMÓWIENIE) ROZBUDOWA KOMPONENTÓW KRYTYCZNYCH

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Na podstawie oceny ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw podmiot może zdecydować, że konieczne jest opracowanie niestandardowych wariantów wybranych krytycznych komponentów. Ten środek bezpieczeństwa zawiera dodatkowe wytyczne dotyczące tego działania. Podmioty powinny współpracować z dostawcami i partnerami, aby określić wykaz krytycznych komponentów. Organizacje powinny zadbać o ciągłą zdolność do utrzymywania opracowanych na zamówienie krytycznych komponentów oprogramowania. Uzyskanie kodu źródłowego, skryptów kompilacyjnych oraz testów dla komponentu oprogramowania może pozwolić organizacji na przekazanie innej jednostce zadania utrzymania tego komponentu, jeśli zajdzie taka potrzeba.

Poziom(y): 2, 3

SA-21 DOBÓR DEWELOPERÓW

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien wdrożyć procesy weryfikacji swoich wewnętrznych deweloperów. W przypadku integratorów systemów, którzy mogą dostarczać kluczowych deweloperów zajmujących się krytycznymi komponentami, podmiot powinien zapewnić, że zastosowano odpowiednie procesy weryfikacji. Weryfikacja i kontrola deweloperów powinna stanowić wymóg umowny, który zostanie przekazany stosownym podwykonawcom niższego szczebla, którzy świadczą usługi programistyczne lub mają dostęp do środowiska rozwojowego.

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *DOBÓR DEWELOPERÓW | POTWIERDZENIE DOBORU*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Wewnętrzne kontrole i weryfikacje deweloperów powinny zostać zatwierdzone. Podmioty mogą zatwierdzić weryfikację dewelopera przez integratora systemu, żądając od niego danych podsumowujących, które zostaną dostarczone po zatwierdzeniu.

Poziom(y): 2, 3

SA-22 KOMPONENTY SYSTEMU BEZ WSPARCIA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Nabywanie produktów bezpośrednio od producentów oryginalnego sprzętu lub ich autoryzowanych dystrybutorów i sprzedawców zmniejsza ryzyko związane z cyberbezpieczeństwem w łańcuchu dostaw. W przypadku niedostępnych komponentów systemu, podmiot powinien korzystać z usług autoryzowanych sprzedawców lub dystrybutorów, którzy posiadają stałe relacje z ich dostawcą.

Przy dokonywaniu zakupu z alternatywnych źródeł, podmiot powinien nabyć rozwiązanie bezpośrednio u producenta lub jego autoryzowanych dystrybutorów i sprzedawców. Decyzje o wykorzystaniu alternatywnych źródeł wymagają komunikacji z inżynierami, aby ustalić zakres różnic między komponentami. Na przykład, jeśli alternatywą jest nabycie otwartoźródłowego komponentu oprogramowania, podmiot powinien określić procesy rozwoju, testowania, akceptacji i wydania oprogramowania przez społeczność skupioną wokół projektu. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

KATEGORIA SI: INTEGRALNOŚĆ SYSTEMU I INFORMACJI

Dokument [NSC 200] określa minimalne wymagania bezpieczeństwa w zakresie integralności systemów i informacji w następujący sposób:

> *Organizacje powinny: (I) w odpowiednim czasie identyfikować, zgłaszać i korygować błędy informacji i systemów informacyjnych; (II) zapewnić ochronę przed złośliwym kodem w stosownych lokalizacjach w ramach organizacyjnych systemów informacyjnych; oraz (III) monitorować ostrzeżenia i porady systemu informacyjnego oraz w odpowiedzi na to podejmować odpowiednie działania.*

Integralność systemów i informacji w przypadku systemów i komponentów przemieszczających się w łańcuchu dostaw ma kluczowe znaczenie dla zarządzania ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw. Wprowadzanie złośliwego kodu oraz podrobionych produktów to dwa podstawowe przykłady zagrożeń dla cyberbezpieczeństwa w całym łańcuchu dostaw, z których oba można przynajmniej częściowo wyeliminować poprzez wdrożenie zabezpieczeń zapewniających integralność systemów i informacji. Podmioty powinny zapewnić, że odpowiednie zabezpieczenia integralności systemu i informacji są częścią działań związanych z obszarem C-SCRM.

SI-1 POLITYKA I PROCEDURY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien włączyć działania w zakresie C-SCRM do polityki i procedur zapewniania integralności systemów i informacji, zapewniając tym samym, że wymagania dotyczące stosowania różnych narzędzi i technik weryfikacji integralności są jasno określone. Integralność systemu i informacji w odniesieniu do systemów informacyjnych i ich komponentów oraz sieci ma kluczowe znaczenie z punktu widzenia zarządzania ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw. Wprowadzanie złośliwego kodu oraz podrobionych produktów to dwa podstawowe przykłady zagrożeń dla cyberbezpieczeństwa w całym łańcuchu dostaw, z których oba można przynajmniej częściowo wyeliminować poprzez wdrożenie zabezpieczeń zapewniających integralność systemów i informacji.

Poziom(y): 1, 2, 3

Powiązane środki bezpieczeństwa: SR-1, 9, 10, 11

SI-2 USUWANIE USTEREK

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Wyniki działań związanych z usuwaniem wad stanowią użyteczny wkład w procesy zarządzania ryzykiem w łańcuchu dostaw rozwiązań ICT/OT opisane w rozdziale 2 i Załączniku C. Dodatkowe informacje znajdują się w rozdziale 2 oraz załączniku C. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *USUWANIE USTEREK | AUTOMATYCZNE AKTUALIZACJE OPROGRAMOWANIA I OPROGRAMOWANIA SPRZĘTOWEGO*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien opracować listę oprogramowania w ramach swoich systemów informacyjnych i sieci, które wymagają automatycznej aktualizacji – zarówno pośredniej, jak i bezpośredniej. Lista ta powinna zostać opracowana na podstawie wyników analizy krytyczności, która dostarcza informacji o krytycznych i niekrytycznych funkcjach i komponentach (więcej informacji znajduje się w rozdziale 2 i Załączniku C). Do oceny aktualizacji oraz zarządzania nimi przed instalacją można zastosować scentralizowany proces zarządzania poprawkami. Oprogramowanie, które wymaga bezpośrednich aktualizacji przekazywanych przez dostawcę powinno akceptować wyłącznie aktualizacje pochodzące bezpośrednio od producenta, chyba że inne rozwiązanie zostało wdrożone przez podmiot nabywający, na przykład w ramach scentralizowanego procesu zarządzania poprawkami. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2

SI-3 ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Z racji tego, że większość kodu wykorzystywanego w systemach podmiotów publicznych nie jest opracowywana przez rząd, zagrożenia związane ze złośliwym kodem często pochodzą z łańcucha dostaw. Ten środek bezpieczeństwa ma zastosowanie do podmiotów publicznych oraz wykonawców realizujących zadania związane z kodem (np. opracowywanie kodu, instalowanie poprawek, przeprowadzanie aktualizacji systemów itp.), jak również do odpowiednich systemów informacyjnych i sieci wykonawcy. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

Powiązane środki bezpieczeństwa: SA-11; SI-7(15); SI-3(4), (6), (8), (10); SR-3(3)

SI-4 MONITOROWANIE SYSTEMU

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Ten środek bezpieczeństwa obejmuje monitorowanie podatności, które wynikają z wcześniejszych naruszeń zasad ochrony w zakresie cyberbezpieczeństwa łańcucha dostaw, takich jak złośliwy kod dodany podczas tworzenia oprogramowania i ustawiony na aktywację po jego instalacji. Usługi związane z monitorowaniem systemów są często realizowane przez zewnętrznych usługodawców. Umowy gwarancji świadczenia usług z tymi dostawcami powinny być skonstruowane tak, aby uwzględniały niniejszy środek bezpieczeństwa. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 1, 2, 3

Zabezpieczenia rozszerzone:

1. *MONITOROWANIE SYSTEMU | WŁĄCZENIE ŚWIADOMOŚCI SYTUACYJNEJ*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Informacje dotyczące monitorowania systemu mogą w stosownych przypadkach być skorelowane z informacjami pochodzącymi od dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT. Wyniki korelacji informacji mogą wskazywać na podatności dotyczące cyberbezpieczeństwa łańcucha dostaw, które wymagają usunięcia lub ograniczenia.

Poziom(y): 2, 3

2. *MONITOROWANIE SYSTEMU | RYZYKO DLA OSÓB*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Do osób o podwyższonym ryzyku można zaliczyć pracowników podmiotu, wykonawców oraz inne osoby trzecie (w tym wolontariuszy, gości), którzy mogą mieć potrzebę lub możliwość dostępu do systemu, sieci lub środowiska podmiotu. Podmiot może wdrożyć zwiększony nadzór nad osobami o podwyższonym ryzyku zgodnie z zasadami, procedurami i – jeśli to możliwe – warunkami umowy oraz w koordynacji z odpowiednimi kierownikami wyższego szczebla.

Poziom(y): 2, 3

SI-5 ALERTY BEZPIECZEŃSTWA, PORADY I DYREKTYWY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien zapoznawać się alertami, informacjami i dyrektywami na temat bezpieczeństwa związanymi z cyberbezpieczeństwem łańcucha dostaw oraz w razie potrzeby podejmować działania następcze. CERT, CSIRT i inne podmioty wydają alerty i informacje dotyczące bezpieczeństwa, które mogą

być związane z obszarem C-SCRM. Dodatkowe ustawy i rozporządzenia będą miały wpływ na to, jakie podmioty będą wydawały takie informacje oraz w jaki sposób będą to robiły. Podmioty powinny zapewnić, aby ich protokoły i procesy wymiany informacji obejmowały udostępnianie informacji, alertów i dyrektyw odpowiednim stronom, z którymi zawarły umowę na dostawę produktów lub świadczenie usług. Podmioty powinny przekazać wytyczne lub wskazówki dotyczące działań, które należy podjąć w odpowiedzi na udostępnienie alertu, informacji lub dyrektywy. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F

Poziom(y): 1, 2, 3

SI-7 APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Ten środek bezpieczeństwa dotyczy organizacji i odpowiednich produktów, aplikacji, systemów informacyjnych i sieci dostawców. Integralność wszystkich systemów i sieci powinna być systematycznie testowana i weryfikowana w celu zapewnienia, że pozostaje zgodna z wymaganiami, tak aby nieprzewidziane zmiany nie miały wpływu na systemy/komponenty przemieszczające się w łańcuchu dostaw. Należy również przetestować i zweryfikować integralność systemów i komponentów. Odpowiednie narzędzia weryfikacji obejmują weryfikację podpisu cyfrowego lub sumy kontrolnej; testy akceptacyjne komponentów fizycznych; ograniczenie oprogramowania do środowisk o ograniczonych uprawnieniach, takich jak piaskownice; wykonywanie przed użyciem kodu w środowiskach o ograniczonych uprawnieniach; a także zapewnienie, że jeśli dostępny jest tylko kod binarny lub źródłowy, to został on uzyskany bezpośrednio od producenta, zweryfikowanego dostawcy lub dystrybutora. Mechanizmy

działania tego środka bezpieczeństwa zostały szczegółowo omówione w dokumencie [NSC 800-53]. Ten środek bezpieczeństwa dotyczy podmiotów publicznych oraz odpowiednich systemów informacyjnych i sieci dostawców. Przy zakupie produktu ICT/OT podmiot powinien przeprowadzić analizę due diligence, aby zrozumieć jakie praktyki stosuje dostawca w zakresie zapewniania integralności. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

Powiązane środki bezpieczeństwa: SR-3(3)

Zabezpieczenia rozszerzone:

1. *APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI| KOD BINARNY LUB WYKONYWALNY MASZYNOWO*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien uzyskać kod binarny lub kod źródłowy bezpośrednio od producenta, dewelopera lub z innego zweryfikowanego źródła.

Poziom(y): 2, 3

2. *APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI| UWIERZYTELNIANIE KODU*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien zapewnić, że mechanizmy uwierzytelniania kodu, takie jak podpisy cyfrowe, zostały wdrożone w celu zapewnienia integralności oprogramowania, oprogramowania sprzętowego i informacji.

Poziom(y): 3

SI-12 ZARZĄDZANIE I RETENCJA DANYCH

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Zagadnienia związane z obszarem C-SCRM powinny być uwzględnione w wymaganiach dotyczących zarządzania informacjami oraz ich przechowywania, zwłaszcza gdy chodzi o wrażliwe i zastrzeżone informacje integratora systemu, dostawcy lub dostawcy usług zewnętrznych.

Poziom(y): 3

SI-20 SKAŻENIE

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Dostawcy, deweloperzy, integratorzy systemów, dostawcy zewnętrznych usług systemowych oraz inni dostawcy usług związanych z ICT/OT mogą mieć dostęp do wrażliwych informacji organizacji. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Poziom(y): 2, 3

Powiązane środki bezpieczeństwa: SR-9

KATEGORIA SC: OCHRONA SYSTEMÓW I SIECI TELEKOMUNIKACYJNYCH

Dokument [NSC 200] określa minimalne wymagania bezpieczeństwa w zakresie ochrony systemów i sieci telekomunikacyjnych w następujący sposób:

> *Organizacje powinny: (I) monitorować, kontrolować i chronić komunikację organizacyjną (tj. informacje przekazywane lub odbierane przez organizacyjne systemy informacyjne) na zewnętrznych granicach i kluczowych granicach wewnętrznych systemów informacyjnych; oraz (II) stosować projekty architektoniczne, techniki tworzenia oprogramowania i zasady inżynierii systemów, które promują skuteczne bezpieczeństwo informacji przetwarzanych w organizacyjnych systemach informacyjnych.*

Infrastruktura komunikacyjna podmiotu składa się z komponentów i systemów ICT/OT, które mają swoje własne łańcuchy dostaw. Łączność ta umożliwia użytkownikom lub administratorom dostęp zdalny do systemów podmiotu oraz łączenie się z Internetem, innymi usługami ICT/OT w ramach podmiotu, systemami wykonawców oraz okazjonalnie z systemami dostawców. Infrastruktura łączności podmiotu może być dostarczana i wspierana przez dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT.

SC-1 POLITYKA I PROCEDURY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Polityki i procedury ochrony systemów i łączności powinny uwzględniać ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw w odniesieniu do procesów, systemów i sieci podmiotu. Polityki na poziomie podmiotu i programu pomagają określić i wyjaśnić te wymogi, a odpowiednie procedury dostarczają instrukcji dotyczących ich realizacji. Polityki i procedury powinny obejmować koordynację komunikacji pomiędzy wieloma jednostkami organizacyjnymi w podmiocie oraz pomiędzy nimi, jak również metody komunikacji, łączności oraz procesy pomiędzy podmiotem a jego dostawcami, deweloperami, integratorami systemów, zewnętrznymi dostawcami usług systemowych oraz innymi dostawcami usług związanych z ICT/OT.

Poziom(y): 1, 2, 3

SC-4 INFORMACJE NA WSPÓŁDZIELONYCH ZASOBACH SYSTEMOWYCH

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot może udostępniać zasoby systemu informacyjnego dostawcom, deweloperom, integratorom systemów, dostawcom zewnętrznych usług systemowych oraz innym dostawcom usług związanych z ICT/OT. Ochrona informacji w zasobach współdzielonych w ramach różnych działań łańcucha dostaw stanowi wyzwanie w przypadku outsourcingu kluczowych operacji. Podmioty mogą udostępnić zbyt wiele informacji, co zwiększa poziom ryzyka, lub udostępniać ich zbyt mało i utrudniać dostawcom, deweloperom, integratorom systemów, dostawcom zewnętrznych usług systemowych i innym dostawcom usług związanych z ICT/OT efektywne świadczenie usług. Podmiot powinien współpracować z deweloperami w celu zdefiniowania struktury lub procesu udostępniania informacji, w tym udostępnianych danych, metody udostępniania oraz ról, które otrzymują dostęp do informacji. W procesie wymiany informacji należy uwzględnić odpowiednie wymogi w zakresie ochrony prywatności, rozpowszechniania, przetwarzania i dostępu.

Poziom(y): 2, 3

SC-5 OCHRONA PRZED BLOKADĄ USŁUG (DOS)

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Dodatkowe wytyczne dotyczące wyłącznie obszaru C-SCRM zostały przedstawione w formie zabezpieczenia rozszerzonego SC-5 (2) w publikacji NSC 800-53.

Zabezpieczenia rozszerzone:

1. *OCHRONA PRZED BLOKADĄ USŁUG (DOS) | PRZEPUSTOWOŚĆ I REDUNDANCJA*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien uwzględnić wymogi dotyczące nadmiarowej przepustowości i redundancji w umowach z dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych i innymi dostawcami usług związanych z ICT/OT.

Poziom(y): 2

SC-7 OCHRONA POŁĄCZEŃ BRZEGOWYCH

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien wdrożyć odpowiednie mechanizmy i procesy monitorowania na granicach systemu, pomiędzy systemami organizacji a systemami dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych systemów dostawców usług związanych z ICT/OT. Postanowienia dotyczące ochrony granic systemu powinny być włączone do umów z dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych i innymi dostawcami usług związanych z ICT/OT. W całym podmiocie, w systemach i sieciach dostawców oraz w cyklu życia systemu może istnieć wiele punktów styku między systemami. Należy przeprowadzić odpowiednie oceny podatności, zagrożeń i ryzyka w celu zapewnienia właściwej ochrony elementów łańcucha dostaw i przepływu informacji w łańcuchu dostaw. Ocena podatności, zagrożenia i ryzyka może pomóc w ustaleniu zakresu ochrony granic systemu na podstawie odpowiedniego zestawu kryteriów i pomóc w zarządzaniu związanymi z tym kosztami. W przypadku umów z zewnętrznymi dostawcami usług, podmiotu powinny zapewnić, że dostawca spełnia wymogi zabezpieczeń dotyczące środowisk i sieci znajdujących się w ich zakresie zabezpieczeń. Dodatkowe informacje znajdują się w rozdziale 2 oraz załączniku C. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2

Zabezpieczenia rozszerzone:

1. *OCHRONA POŁĄCZEŃ BRZEGOWYCH | IZOLACJA NARZĘDZI BEZPIECZEŃSTWA, MECHANIZMÓW I ELEMENTÓW WSPIERAJĄCYCH*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien zapewnić oddzielenie i izolację narzędzi programistycznych, testowych oraz oceny bezpieczeństwa oraz środowisk operacyjnych i odpowiednich narzędzi monitorujących w ramach systemów informacyjnych i sieci podmiotu. Ten środek bezpieczeństwa dotyczy podmiotu odpowiedzialnego za tworzenie oprogramowania i sprzętu, w tym organizacji i głównych wykonawców. W związku z tym niniejsze środki bezpieczeństwa mają zastosowanie do systemów informacyjnych i sieci podmiotu publicznego i odpowiednich dostawców. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Jeśli nastąpi naruszenie zasad ochrony lub wyciek informacji z któregokolwiek środowiska, pozostałe środowiska nadal powinny być chronione poprzez mechanizmy lub techniki separacji i izolacji.

Poziom(y): 3

Powiązane środki bezpieczeństwa: SR-3(3)

2. *OCHRONA POŁĄCZEŃ BRZEGOWYCH | OCHRONA PRZED NIEAUTORYZOWANYMI POŁĄCZENIAMI FIZYCZNYMI*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Ten środek bezpieczeństwa jest istotny z punktu widzenia C-SCRM, ponieważ dotyczy dostawców zewnętrznych usług.

Poziom(y): 2,3

Powiązane środki bezpieczeństwa: SR-3(3)

3. *OCHRONA POŁĄCZEŃ BRZEGOWYCH | BLOKOWANIE KOMUNIKACJI SPOZA ORGANIZACJI*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Ten środek bezpieczeństwa jest istotny z punktu widzenia C-SCRM, ponieważ dotyczy dostawców zewnętrznych usług.

Poziom(y): 3

SC-8 POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Wymogi dotyczące poufności i integralności transmisji powinny zostać włączone do umów z dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych oraz innymi dostawcami usług związanych z ICT/OT. Nabywcy, dostawcy, deweloperzy, integratorzy systemów, dostawcy zewnętrzni usług systemowych oraz inni dostawcy usług związanych z ICT/OT mogą ponownie wykorzystać istniejące mechanizmy bezpieczeństwa (np. uwierzytelnianie, autoryzację lub szyfrowanie) w celu spełnienia wymogów podmiotu w zakresie poufności i integralności. Stopień ochrony powinien być uzależniony od wrażliwości przekazywanych informacji oraz relacji pomiędzy organizacją a dostawcami, twórcami, integratorami systemów, dostawcami zewnętrznych usług systemowych oraz innymi dostawcami usług związanych z ICT/OT. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

SC-18 KOD MOBILNY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien stosować ten środek bezpieczeństwa w różnych obszarach, w których następuje przemieszczanie kodu w systemach informacyjnych i sieciach.

Przykładem mogą być procesy nabywania, takie jak elektroniczna transmisja informacji o łańcuchu dostaw (np. przez e-mail), odbiór komponentów oprogramowania, zarządzanie informacjami logistycznymi lub infrastruktura czujników.

Poziom(y): 3

Zabezpieczenia rozszerzone:

1. *KOD MOBILNY | NABYCIE, ROZWÓJ I WYKORZYSTANIE*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien stosować rygorystyczne techniki ochrony łańcucha dostaw przy nabywaniu, opracowywaniu i wykorzystywaniu kodu, który ma być wdrożony w systemie informacyjnym. Przykłady obejmują zapewnienie, że kod w momencie nabycia pochodzi ze sprawdzonych źródeł, że sprawdzeni integratorzy systemów są wykorzystywani do opracowania niestandardowego kodu, a także że istnieją procesy weryfikacji kryteriów akceptacji przed instalacją w celu sprawdzenia źródła i integralności kodu. Należy pamiętać, że kod może dotyczyć zarówno podstawowych systemów informacyjnych i sieci (np. aplikacji na urządzenia RFID) jak i samych systemów informacyjnych i ich komponentów.

Poziom(y): 3

SC-27 WIELOPLATFORMOWOŚĆ APLIKACJI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Wykorzystanie zaufanych aplikacji niezależnych od platformy jest kluczowym zagadnieniem związanym z obszarem C-SCRM. Większa przenośność aplikacji niezależnych od platformy umożliwia podmiotom łatwiejszą zmianę dostawców zewnętrznych usług w przypadku, gdy nastąpi kompromitacja jednego z nich, co zmniejsza ryzyko związane z cyberbezpieczeństwem zależne od dostawcy. Jest to szczególnie istotne w przypadku krytycznych aplikacji, na których może opierać się wiele systemów.

Poziom(y): 2, 3

SC-28 OCHRONA DANYCH W SKŁADOWANIU

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien uwzględnić postanowienia dotyczące ochrony informacji w stanie spoczynku do swoich umów z dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych oraz innymi dostawcami usług związanych z ICT/OT. Podmiot powinien również zapewnić odpowiednią ochronę w ramach systemów informacyjnych i sieci dla danych w stanie spoczynku dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT, takich jak kody źródłowe, dane testowe, projekty oraz informacje dotyczące własności intelektualnej. Ten środek bezpieczeństwa powinien być stosowany w całym cyklu życia systemu, w tym w procesie określania wymagań, w czasie rozwoju, produkcji, testowania, zarządzania zapasami, utrzymania i utylizacji. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

Powiązane środki bezpieczeństwa: SR-3(3)

SC-29 HETEROGENICZNOŚĆ SYSTEMU

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Zabezpieczenie to obejmuje wykorzystanie różnych systemów operacyjnych, technik wirtualizacji oraz wielu dostawców. Dywersyfikacja źródeł dostaw może zwiększyć dostępność komponentów i zmniejszyć wpływ potencjalnej kompromitacji cyberbezpieczeństwa łańcucha dostaw. W przypadku naruszenia zasad ochrony cyberbezpieczeństwa w łańcuchu dostaw, alternatywne źródło dostaw pozwoli podmiotom na szybsze przejście na alternatywny system/komponent, którego nie dotyczyła kompromitacja.

Różnorodność komponentów zmniejsza także powierzchnię ataku poprzez ograniczenie wpływu do części infrastruktury, która używa podatnych komponentów.

Poziom(y): 2, 3

SC-30 MASKOWANIE I DEZINFORMACJA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Techniki ukrywania i przekierowania związane z obszarem C-SCRM obejmują między innymi określenie losowych czasów omówień, ukrycie lokalizacji, losową zmianę używanej fałszywej lokalizacji oraz losową zmianę lub przesunięcie przechowywania informacji na alternatywne serwery lub zmianę rozwiązań.

Poziom(y): 2, 3

Zabezpieczenia rozszerzone:

1. *MASKOWANIE I DEZINFORMACJA | LOSOWOŚĆ*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Procesy w łańcuchu dostaw mają z konieczności przewidywalną, mierzalną oraz powtarzalną strukturę, co pozwala na osiągnięcie efektywności i redukcji kosztów. To otwiera możliwość potencjalnego naruszenia bezpieczeństwa. W celu ochrony przed kompromitacją, podmiot powinien stosować techniki wprowadzające losowość do działań w systemach lub sieciach (np. zmiany przedsiębiorstw spedycyjnych i tras, zmiany czasu lub daty otrzymywania aktualizacji oprogramowania, jeżeli wcześniej były zaplanowane w przewidywalny sposób).

Poziom(y): 2, 3

2. *MASKOWANIE I DEZINFORMACJA | ZMIANA MIEJSCA PRZETWARZANIA I PRZECHOWYWANIA*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Zmiany lokalizacji przetwarzania lub przechowywania danych mogą być wykorzystane do ochrony pobieranych informacji, dostaw lub powiązanych

metadanych łańcucha dostaw. Podmiot może wykorzystywać takie techniki w swoich systemach i sieciach informacyjnych, aby zasiać wśród potencjalnych atakujących niepewność w stosunku do swoich działań. Wprowadzenie kilku zmian w procesach i ich losowe stosowanie – niezależnie od tego, czy dotyczy to odbioru, testów akceptacyjnych, magazynowania czy innych działań w łańcuchu dostaw – może pomóc w zmniejszeniu prawdopodobieństwa wystąpienia incydentów w łańcuchu dostaw.

Poziom(y): 2, 3

3. *MASKOWANIE I DEZINFORMACJA | WPROWADZAJĄCE W BŁĄD INFORMACJE*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot może przekazywać informacje wprowadzające w błąd w ramach działań mających na celu ukrywanie informacji oraz zwodzenie napastników w celu ochrony opracowywanego systemu informacyjnego oraz systemów i sieci podmiotu. Przykładem takich działań w zakresie bezpieczeństwa są sieci - pułapki czy środowiska zwirtualizowane. Wdrożenie takich rozwiązań może być wykorzystywane do przekazywania wprowadzających w błąd informacji. Takie działania mogą być uznawane za zaawansowane techniki, które wymagają doświadczonych pracowników oraz odpowiednich zasobów do skutecznego wdrożenia. Jeśli podmiot decyduje się na wykorzystanie takich rozwiązań, powinno to się odbyć w porozumieniu z działem prawnym oraz zgodnie z polityką podmiotu.

Poziom(y): 2, 3

4. *MASKOWANIE I DEZINFORMACJA | UKRYWANIE KOMPONENTÓW SYSTEMU*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot może stosować różne techniki ukrywania i wprowadzania w błąd w celu

ochrony informacji o opracowywanym systemie informacyjnym oraz systemach informacyjnych i sieciach podmiotu. Na przykład dostarczenie krytycznych komponentów do centralnego lub zaufanego magazynu podmiotu zewnętrznego może zostać wykorzystane do ukrycia wszelkich informacji dotyczących wykorzystania komponentu lub podmiotu korzystającego z komponentu. Rozdzielenie komponentów i związanych z nimi informacji pomiędzy różne kanały fizyczne i cyfrowe oraz ukrycie informacji za pomocą różnych technik może być wykorzystane do ukrycia informacji i zmniejszenia możliwości potencjalnego ujawnienia komponentu, sposobu jego wykorzystania, stanu lub innych cech.

Poziom(y): 2, 3

SC-36 PRZETWARZANIE I PRZECHOWYWANIE ROZPROSZONE

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Przetwarzanie i przechowywanie mogą być rozproszone zarówno w systemach i sieciach podmiotu, jak i w całym cyklu życia systemu. Podmiot powinien zapewnić, że techniki te są stosowane w obu kontekstach. Rozwój, produkcja, zarządzanie konfiguracją, testowanie, konserwacja i operacje mogą wykorzystywać rozproszone przetwarzanie i przechowywanie danych. Ten środek bezpieczeństwa dotyczy podmiotów odpowiedzialnych za funkcje przetwarzania i przechowywania lub związaną z nimi infrastrukturę, w tym organizacje i wykonawców. W związku z tym ma on zastosowanie do systemów informacyjnych i sieci organizacyjnych i odpowiednich dostawców. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla.

Poziom(y): 2, 3

Powiązane środki bezpieczeństwa: SR-3(3)

SC-37 KANAŁY POZAPASMOWE

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Dodatkowe wytyczne dotyczące wyłącznie obszaru C-SCRM zostały przedstawione w formie zabezpieczenia rozszerzonego SC-37 (1).

Zabezpieczenia rozszerzone:

1. *KANAŁY POZAPASMOWE | ZAPEWNIANIE DOSTAW I TRANSMISJI*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien zastosować zabezpieczenia w celu zapewnienia, że tylko określone osoby lub systemy informacyjne otrzymają informacje o systemie informacyjnym lub jego środowisku i procesach rozwojowych. Przed wydaniem krytycznych komponentów, takich jak niestandardowe układy scalone, oprogramowanie lub informacje, należy zażądać odpowiednich dokumentów uwierzytelniających i autoryzacyjnych oraz zweryfikować ich autentyczność.

Poziom(y): 2, 3

SC-38 BEZPIECZEŃSTWO OPERACJI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien zapewnić, że odpowiednie informacje o zagrożeniach i podatnościach w łańcuchu dostaw są uzyskiwane i przekazywane w celu realizacji procesów bezpieczeństwa operacyjnego.

Poziom(y): 2, 3

Powiązane środki bezpieczeństwa: SR-7

SC-47 ALTERNATYWNE ŚCIEŻKI KOMUNIKACJI

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Jeśli to konieczne i wymagane, dostawcy, deweloperzy, integratorzy systemów, dostawcy zewnętrznych usług systemowych oraz inni dostawcy usług związanych z ICT/OT powinni zostać włączeni do alternatywnych sposobów komunikacji wymienionych w opisie niniejszego środka zabezpieczeń.

Poziom(y): 1, 2, 3

KATEGORIA SR: ZARZĄDZANIE RYZYKIEM W ŁAŃCUCHU DOSTAW

Dokument [NSC 200] określa minimalne wymagania bezpieczeństwa w zakresie zarządzania ryzykiem w łańcuchu dostaw w następujący sposób:

> *Organizacje powinny: (I) opracowywać polityki i procedury w zakresie zarządzania ryzykiem w łańcuchu dostaw; (II) opracowywać programy bezpieczeństwa i ochrony prywatności uwzględniające polityki i procedury zarządzania ryzykiem w łańcuchu dostaw; (III) aktualizować polityki i procedury zarządzania ryzykiem w łańcuchu dostaw w oparciu o zaistniałe zdarzenia obejmujące wyniki oceny lub audytu, incydenty lub naruszenia bezpieczeństwa, lub zmiany w przepisach prawa, zarządzeniach, dyrektywach, rozporządzeniach, zasadach, standardach i wytycznych.*

Dokument [NSC 800-53] ustanawia nową rodzinę środków zabezpieczających: *Zarządzanie ryzykiem w łańcuchu dostaw (ang. Supply chain risk management - SR)*. Poniższe wytyczne uzupełniające rozszerzają zakres środków zabezpieczających SR oraz obejmują dodatkowe informacje i kontekst dotyczący ich stosowania. Poniższe środki zabezpieczające stanowią nową rodzinę w dokumencie NSC 800-53, który zawiera stosowne wytyczne. Niniejszy dokument obejmuje wszystkie zabezpieczenia rozszerzone należące do rodziny SR opisane w dokumencie NSC 800-53, a poniższe środki bezpieczeństwa SR i zabezpieczenia rozszerzone zostały dodane do treści dokumentu NSC 800-53 [SR-13]. Czytelnicy powinni zapoznać się z opisami środków bezpieczeństwa SR w dokumencie NSC 800-53, a także środkami opisanymi w niniejszym rozdziale.

SR-1 POLITYKA I PROCEDURY

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Polityki C-SCRM są opracowywane na poziomie 1 dla całego podmiotu oraz na poziomie 2 dla poszczególnych misji i funkcji. Polityki C-SCRM mogą być wdrażane na poziomach 1, 2 i 3, w zależności od poziomu głębokości i szczegółowości. Procedury C-SCRM są opracowywane na poziomie 2 dla konkretnych misji i funkcji oraz na poziomie 3 dla konkretnych systemów. Poszczególne piony działające w podmiocie, obejmujące między innymi bezpieczeństwo

informacji, dział prawny, zarządzanie ryzykiem i dział zamówień, powinny dokonywać przeglądu i uzgadniać opracowanie polityk i procedur C-SCRM lub dostarczać osobom odpowiedzialnym za systemy wytyczne do opracowania procedur C-SCRM specyficznych dla danego systemu.

Poziom(y): 1, 2, 3

SR-2 PLAN ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Plany C-SCRM opisują wdrożenia, wymagania, ograniczenia i założenia dotyczące poszczególnych systemów. Na plany C-SCRM wpływają inne działania podmiotu w zakresie oceny ryzyka, w związku z którymi mogą dziedziczyć i dostosowywać wspólne zabezpieczenia bazowe zdefiniowane na poziomach 1 oraz 2. Plany C-SCRM opracowane na poziomie 3 są zgodne ze strategią i polityką C-SCRM podmiotu (poziomy 1 i 2) oraz planem wdrożenia C-SCRM (poziomy 1 i 2) w celu zapewnienia systematycznego i holistycznego podejścia do zarządzania ryzykiem związanym z cyberbezpieczeństwem łańcucha dostaw w całym podmiocie.

Plany C-SCRM powinny być opracowywane w formie samodzielnych dokumentów i włączane do istniejących planów bezpieczeństwa systemu tylko wtedy, gdy wymagają tego ograniczenia dotyczące danego podmiotu.

Poziom(y): 3

Powiązane środki bezpieczeństwa: PL-2

SR-3 ZABEZPIECZENIA I PROCESY W ŁAŃCUCHU DOSTAW

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Rozdział 2 i załącznik C do niniejszego dokumentu zawierają szczegółowe wytyczne dotyczące wdrażania tego środka bezpieczeństwa. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 1, 2, 3

Zabezpieczenia rozszerzone:

1. *ZABEZPIECZENIA I PROCESY W ŁAŃCUCHU DOSTAW | ZRÓŻNICOWANA BAZA DOSTAWCÓW*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny zdywersyfikować swoją bazę dostawców, zwłaszcza w przypadku krytycznych produktów i usług ICT/OT. W ramach tego działania podmiot powinien podjąć próbę określenia obszarów, w których awaria grozi przerwaniem ciągłości działania, a także ryzyka związanego z głównymi dostawcami oraz kolejnymi poziomami w łańcuchu dostaw. Wskazówki dotyczące przeprowadzania analizy krytyczności znajdują się w rozdziale 2, Załączniku C oraz wytycznej RA-9.

Poziom(y): 2, 3

Powiązane środki bezpieczeństwa: RA-9

2. *ZABEZPIECZENIA I PROCESY W ŁAŃCUCHU DOSTAW | KASKADOWANIE ŚRODKÓW BEZPIECZEŃSTWA*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa w całym cyklu życia systemu i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla. Wykorzystanie procesu zamówień oraz zaopatrzenia stanowi ważne narzędzie związane z ochroną łańcucha dostaw. W ramach wymagań dotyczących zamówień podmioty powinny uwzględnić konieczność włączania środków bezpieczeństwa u podwykonawców przez dostawców w całym cyklu życia systemu. W ramach działań związanych z badaniem i analizą rynku podmioty powinny przeprowadzać szeroko zakrojone analizy due diligence potencjalnych dostawców lub produktów, a także podmiotów, z którymi współpracują w ramach własnych łańcuchów dostaw, co może pomóc podmiotom uniknąć sytuacji, w których w łańcuchach dostaw będą występowały punkty, których podatność zagrozi stabilności całego

łańcucha. Wyniki tych analiz mogą być pomocne w kształtowaniu podejścia do zamówień oraz dopracowaniu wymagań. Ocenę ryzyka związanego z cyberbezpieczeństwem dostawcy, produktu lub usługi należy przeprowadzić przed podjęciem decyzji o udzieleniu zamówienia, aby zapewnić dobre zrozumienie całościowego profilu ryzyka oraz uwzględnienie go w roli ważnego czynnika przy podejmowaniu decyzji. W okresie realizacji, dostawcy powinni być monitorowani pod kątem zgodności z określonymi środkami bezpieczeństwa i wymaganiami, a także zmian w warunkach ryzyka. Dodatkowe wytyczne dotyczące roli działań związanych z obszarem C-SCRM w ramach procesów zamówień znajdują się w rozdziale 3.

Poziom(y): 2, 3

SR-4 POCHODZENIE

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Pochodzenie powinno być udokumentowane w przypadku systemów, komponentów systemów i powiązanych danych w całym cyklu życia systemu. Podmioty powinny rozważyć sporządzenie specyfikacji materiałowych komponentów oprogramowania w przypadku stosownych klas oprogramowania, w tym oprogramowania komercyjnego, oprogramowania otwartoźródłowego oraz oprogramowania opracowanego wewnątrz podmiotu. Specyfikacje materiałowe komponentów oprogramowania powinny być opracowywane w formatach spełniających wymagania w [Cyber Resilience Act – CRA]. Podmioty opracowujące specyfikacje materiałowe komponentów oprogramowania powinny stosować wymogi minimalne CRA w celu uwzględnienia podstawowych komponentów. Specyfikacje materiałowe komponentów oprogramowania powinny być podpisane cyfrowo przy użyciu weryfikowalnego i zaufanego klucza. Specyfikacje materiałowe komponentów oprogramowania mogą stanowić niezwykle ważne narzędzie, które pozwoli organizacjom na utrzymywanie informacji o pochodzeniu komponentów. W miarę ich rozbudowywania, organizacje

powinny upewnić się, że nie wpływają one na ograniczanie priorytetu działań dotyczących obszaru C-SCRM (np. praktyk w zakresie zarządzania podatnościami, ocen ryzyka dostawców) na podstawie błędnego założenia, że specyfikacje materiałowe komponentów oprogramowania zastępują te działania. Specyfikacje materiałowe komponentów oprogramowania i zwiększona przejrzystość, którą mają zapewnić organizacjom, stanowią jedynie uzupełnienie działań – nie powinny ich zastępować. Organizacje, które nie są w stanie odpowiednio analizować oraz wykorzystywać danych zawartych w specyfikacjach materiałowych komponentów oprogramowania, prawdopodobnie nie będą w stanie poprawić swoich działań w zakresie C-SCRM na ich podstawie. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

SR-5 STRATEGIE, NARZĘDZIA I METODY NABYCIA

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Rozdział 3 i środki bezpieczeństwa SA zawierają dodatkowe wytyczne dotyczące strategii, narzędzi i metod wykorzystywanych w procesie zamówień. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 1, 2, 3

Powiązane środki bezpieczeństwa: Środki bezpieczeństwa należące do rodziny SA

SR-6 OCENY I RECENZJE DOSTAWCÓW

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmiot powinien uwzględnić wszelkie informacje dotyczące bezpieczeństwa, integralności, odporności, jakości, wiarygodności oraz autentyczności dostawcy lub świadczonych przez niego usług, a także oferowanych produktów. Podmioty powinny rozważyć zastosowanie tych informacji w odniesieniu do spójnego zestawu podstawowych czynników bazowych i kryteriów

oceny, aby ułatwić sprawiedliwe porównanie dostawców, a także ich obserwację w czasie. W zależności od konkretnego kontekstu i celu przeprowadzenia oceny, podmiot może wybrać dodatkowe czynniki. Ważną kwestią jest również jakość informacji, na których opiera się ocena, w tym ich istotność, kompletność, a także dokładność. Należy również udokumentować źródła informacji wpływających na ocenę. Biuro zarządzania programem C-SCRM może pomóc w określeniu wymagań, metod i narzędzi do oceny dostawców. Organizacje zapoznać się z załącznikiem E w celu uzyskania dalszych wytycznych dotyczących podstawowych czynników ryzyka i dokumentacji ocen oraz załącznikiem F.

Poziom(y): 2, 3

SR-7 BEZPIECZEŃSTWO OPERACJI W RAMACH ŁAŃCUCHA DOSTAW

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Biuro zarządzania programem C-SCRM może pomóc w określeniu środków bezpieczeństwa operacyjnego związanych z wybranymi misjami oraz pionami. Środki bezpieczeństwa operacyjnego są szczególnie ważne, gdy istnieją uzasadnione obawy dotyczące zagrożenia ze strony łańcucha dostaw lub zagrożenia dla samego łańcucha dostaw bądź jego elementu, a także gdy charakter misji lub operacji biznesowych podmiotu, jego informacji i/lub oferty usług i produktów czyni go bardziej atrakcyjnym celem.

Poziom(y): 2, 3

SR-8 UMOWY DOTYCZĄCE POWIADOMIEŃ

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny wymagać od swoich dostawców co najmniej zawarcia umów dotyczących powiadamiania z jednostkami wchodzącymi w skład ich łańcuchów dostaw, które są związane z usługami lub produktami o znaczeniu krytycznym lub ponoszą za nie odpowiedzialność. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

Powiązane środki bezpieczeństwa: RA-9

SR-9 ODPORNOŚĆ NA MANIPULACJE I WYKRYWANIE SABOTAŻU

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny stosować zabezpieczenia przeciwko manipulacji oraz środki pozwalające na wykrywanie manipulacji co najmniej w przypadku krytycznych komponentów. Analiza krytyczności może pomóc w określeniu, które komponenty powinny zostać uznane za krytyczne. Wskazówki dotyczące przeprowadzania analizy krytyczności znajdują się w rozdziale 2, Załączniku C oraz wytycznej RA-9. Biuro zarządzania programem C-SCRM może pomóc w identyfikacji krytycznych komponentów, zwłaszcza tych, które są wykorzystywane przez wiele misji, funkcji i systemów w podmiocie. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 2, 3

Powiązane środki bezpieczeństwa: RA-9

SR-10 KONTROLA SYSTEMÓW / KOMPONENTÓW

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny dokonywać kontroli krytycznych systemów i komponentów w celu upewnienia, się, że zastosowano środki zabezpieczające przed manipulacją oraz w celu sprawdzenia, czy występują jakiekolwiek oznaki manipulacji. Produkty lub komponenty powinny być kontrolowane przed użyciem, a następnie okresowo. Postanowienia dotyczące kontroli powinny być włączone do umów z dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych i innymi dostawcami usług związanych z ICT/OT. Podmioty powinny wymagać od swoich kluczowych wykonawców wdrożenia tego środka bezpieczeństwa i przekazania tego wymogu odpowiednim wykonawcom niższego szczebla, jeśli jest to konieczne.

Analiza krytyczności może pomóc w określeniu, które systemy i komponenty powinny zostać uznane za krytyczne i poddane kontroli. Wskazówki dotyczące przeprowadzania analizy krytyczności znajdują się w rozdziale 2, Załączniku C

oraz wytycznej RA-9. Biuro zarządzania programem C-SCRM może pomóc w identyfikacji krytycznych systemów i komponentów, zwłaszcza tych, które są wykorzystywane przez wiele misji, funkcji i systemów w podmiocie.

Poziom(y): 2, 3

Powiązane środki bezpieczeństwa: RA-9

SR-11 AUTENTYCZNOŚĆ KOMPONENTU

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Opracowanie polityki i procedur przeciwdziałania podróbkom wymaga koordynacji z działem zamówień i zaopatrzenia, działem IT, działem prawnym oraz biurem zarządzania programem C-SCRM. Polityka i procedury powinny uwzględniać wymogi zgodności z przepisami, wymogi lub klauzule umów oraz procesy zgłaszania fałszerstw do właściwych podmiotów. W stosownych przypadkach polityka powinna również obejmować opracowanie i stosowanie wykazu kwalifikowanych oferentów lub wykazu kwalifikowanych producentów. Pomaga to zapobiegać fałszerstwom poprzez korzystanie z autoryzowanych dostawców, jeśli tylko jest to możliwe, oraz ich integrację z łańcuchem dostaw organizacji]. Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Poziom(y): 1, 2, 3

Zabezpieczenia rozszerzone:

1. *AUTENTYCZNOŚĆ KOMPONENTU | SZKOLENIE W ZAKRESIE WYKRYWANIA PODRÓBEK*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Biuro zarządzania programem C-SCRM może pomóc w identyfikacji podmiotów, które mogą przeprowadzić szkolenie w zakresie wykrywania podróbek lub mogą zaoferować takie szkolenia podmiotowi. Biuro zarządzania programem C-SCRM może również pomóc w ustaleniu, którzy pracownicy powinni odbyć takie szkolenie.

Poziom(y): 2, 3

2. *AUTENTYCZNOŚĆ KOMPONENTU | ZABEZPIECZENIA KONFIGURACYJNE W PRZYPADKU SERWISU I NAPRAWY KOMPONENTÓW*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Dział IT, dział bezpieczeństwa lub biuro zarządzania programem C-SCRM powinny być odpowiedzialne za ustanowienie i wdrożenie procesów zabezpieczeń konfiguracji w przypadku serwisu i naprawy komponentów, w tym – jeśli to stosowne – włączenie serwisu i naprawy komponentów do ogólnych procesów zabezpieczeń konfiguracji podmiotu. Autentyczność komponentu powinna być uwzględniona w umowach dotyczących obsługi i naprawy komponentów.

Poziom(y): 2, 3

3. *AUTENTYCZNOŚĆ KOMPONENTU | SKANOWANIE W CELU WYKRYWANIA PODRÓBEK*

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty powinny przeprowadzać skanowanie w celu wykrywania podróbek co najmniej w przypadku komponentów krytycznych. Analiza krytyczności może pomóc w określeniu, które systemy i komponenty powinny zostać uznane za krytyczne i poddane kontroli. Wytyczne dotyczące przeprowadzania analizy krytyczności znajdują się w rozdziale 2, Załączniku C oraz środku bezpieczeństwa RA-9. Biuro zarządzania programem C-SCRM może pomóc w identyfikacji krytycznych komponentów, zwłaszcza tych, które są wykorzystywane przez wiele misji, funkcji i systemów w podmiocie.

Poziom(y): 2, 3

Powiązane środki bezpieczeństwa: RA-9

SR-12 USUWANIE KOMPONENTÓW

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Dział bezpieczeństwa IT w połączeniu z biurem zarządzania programem C-SCRM może pomóc w ustanowieniu odpowiednich polityk, procedur, mechanizmów i technik utylizacji komponentów.

Poziom(y): 2, 3

SR-13 WYKAZ DOSTAWCÓW (NOWY)

Zabezpieczenie:

a. Opracowanie, udokumentowanie i utrzymywanie wykazu dostawców, który:

1. Stanowi dokładną listę głównych dostawców organizacji, którzy mogą być źródłem ryzyka związanego z cyberbezpieczeństwem w łańcuchu dostaw [Zadanie: Określenie przez organizację parametrów ustalania głównych dostawców];

2. Jest wystarczająco szczegółowy, by umożliwić ocenę krytyczności oraz ryzyka łańcucha dostaw, śledzenia i raportowania;

3. Uwzględnia następujące informacje dla każdego głównego dostawcy (np. głównego wykonawcy): przegląda i aktualizuje wykaz dostawców [Zadanie: Określenie częstotliwości przez podmiot].

I Zawiera unikalny identyfikator dla instrumentu zamówienia (tj. umowy, zadania lub zamówienia dostawy).

II Zawiera opis dostarczanych produktów bądź usług.

III Zawiera informację o projekcie, programie lub systemie, który wykorzystuje produkty i/lub usługi dostawcy.

IV Zawiera poziom krytyczności, który odpowiada krytyczności programu, projektu bądź systemu (lub komponentu systemu).

b. Przegląd i aktualizacja wykazu dostawców [Zadanie: Określenie częstotliwości przeglądu przez podmiot].

Dodatkowe wytyczne dotyczące obszaru C-SCRM: Podmioty korzystają z usług licznych dostawców w realizacji swoich misji oraz działalności. Dostawcy dostarczają produkty i usługi wspierające realizację misji, działań, funkcji, programów, projektów i systemów. Niektórzy dostawcy są bardziej kluczowi niż inni ze względu na krytyczny charakter misji, działań, programów, projektów, systemów wykorzystujących ich produkty i usługi,

a także poziom zależności podmiotu od dostawcy. Podmioty powinny stosować analizy krytyczności, aby pomóc w określeniu, które produkty i usługi mają charakter krytyczny, aby na ich podstawie określić charakter dostawców, który należy udokumentować w wykazie dostawców. Wytyczne dotyczące przeprowadzania analizy krytyczności znajdują się w rozdziale 2, Załączniku C oraz środku bezpieczeństwa RA-9.

Poziom(y): 2, 3

Powiązane środki bezpieczeństwa: RA-9

ZAŁĄCZNIK B PODSUMOWANIE ŚRODKÓW BEZPIECZEŃSTWA ZWIĄZANYCH Z OBSZAREM C-SCRM

Niniejszy załącznik zawiera listę środków bezpieczeństwa C-SCRM opisanych w niniejszej publikacji oraz ich zestawienie z odpowiadającymi im środkami bezpieczeństwa opisanymi w dokumencie [NSC 800-53]. W tabeli B-1 zostały opisane środki bezpieczeństwa określone w dokumencie [NSC 800-53]. Wymagania bazowe o niskim poziomie uznaje się za istotne z punktu widzenia działań związanych z obszarem C-SCRM. Do tego zbioru środków bezpieczeństwa dodano szereg środków bezpieczeństwa związanych z obszarem C-SCRM, co pozwoliło na ustalenie poziomu bazowego C-SCRM. Dodatkowo, środki bezpieczeństwa, które powinny być przekazywane kaskadowo przez głównych dostawców podwykonawcom są opisane jako kaskadowalne środki bezpieczeństwa. Biorąc pod uwagę fakt, że działania związane z obszarem C-SCRM są działaniami obejmującymi kompleksowo cały podmiot, które wymagają wyboru i wdrożenia środków zabezpieczających na wszystkich poziomach podmiotu, misji oraz operacyjnym (poziomach 1, 2 i 3 podmiotu według dokumentu [NSC 800-39]), tabela B-1 zawiera także informację na temat poziomów podmiotu, na których powinny być wdrożone poszczególne środki bezpieczeństwa. Środki bezpieczeństwa związane z obszarem C-SCRM i zabezpieczenia rozszerzone, które nie zostały zawarte w dokumencie [NSC 800-53] są oznaczone gwiazdką obok identyfikatora zabezpieczeń, np. w przypadku środków zabezpieczeń MA-8 i SR-13.

Tabela B-1. Podsumowanie środków bezpieczeństwa związanych z obszarem C-SCRM

				Poziomy		
Identyfikator środka bezpieczeństwa	**Nazwa środka bezpieczeństwa lub zabezpieczenia rozszerzonego**	**Poziom bazowy C-SCRM**	**Kaskadowalny środek bezpieczeństwa**	**1**	**2**	**3**
AC-1	**Polityka i procedury**	x	x	x	x	x
AC-2	**Zarządzanie kontami**	x	x		x	x

Tłumaczenie

				Poziomy		
Identyfikator środka bezpieczeństwa	**Nazwa środka bezpieczeństwa lub zabezpieczenia rozszerzonego**	**Poziom bazowy C-SCRM**	**Kaskadowalny środek bezpieczeństwa**	**1**	**2**	**3**
AC-3	**Egzekwowanie uprawnień dostępu**	x	x		x	x
AC-3(8)	*Egzekwowanie uprawnień dostępu | Wycofanie uprawnień dostępu*				x	x
AC-3(9)	*Egzekwowanie uprawnień dostępu | Kontrolowane udostępnianie informacji*				x	x
AC-4	**Kontrola przepływu informacji**		x		x	x
AC-4(6)	*Kontrola przepływu informacji | metadane*				x	x
AC-4(17)	*Kontrola przepływu informacji | Uwierzytelnianie domeny*				x	x
AC-4(19)	*Kontrola przepływu informacji | Walidacja metadanych*				x	x
AC-4(21)	*Kontrola przepływu informacji | Fizyczne lub logiczne oddzielenie przepływów informacji*					x
AC-5	*Podział obowiązków*		x		x	x
AC-6(6)	*Zasada minimalnych uprawnień | Uprzywilejowany dostęp dla użytkowników spoza organizacji*				x	x
AC-17	**Dostęp zdalny**	x	x		x	x
AC-17(6)	*Dostęp zdalny | Ochrona informacji o mechanizmach*				x	x
AC-18	**Dostęp bezprzewodowy**	x		x	x	x
AC-19	**Kontrola dostępu do urządzeń przenośnych**	x			x	x

				Poziomy		
Identyfikator środka bezpieczeństwa	**Nazwa środka bezpieczeństwa lub zabezpieczenia rozszerzonego**	**Poziom bazowy C-SCRM**	**Kaskadowalny środek bezpieczeństwa**	**1**	**2**	**3**
AC-20	**Wykorzystanie zewnętrznych systemów**	x	x	x	x	x
AC-20(1)	*Wykorzystanie zewnętrznych systemów | Ograniczenia dotyczące dozwolonego użytkowania*				x	x
AC-20(3)	*Wykorzystanie zewnętrznych systemów | Ograniczone wykorzystanie systemów nienależących do organizacji*				x	x
AC-21	**Udostępnianie informacji**			x	x	
AC-22	**Publicznie dostępne treści**	x			x	x
AC-23	**Ochrona danych przed wydobywaniem**		x		x	x
AC-24	**Decyzje dotyczące kontroli dostępu**		x	x	x	x
AT-1	**Polityka i procedury**	x		x	x	
AT-2(1)	*Szkolenie w zakresie uświadamiania bezpieczeństwa | Ćwiczenia praktyczne*				x	
AT-2(2)	*Szkolenie w zakresie uświadamiania bezpieczeństwa | Zagrożenia wewnętrzne*	x	x		x	
AT-2(3)	*Szkolenie w zakresie uświadamiania bezpieczeństwa | Inżynieria społeczna oraz wydobywanie*				x	

				Poziomy		
Identyfikator środka bezpieczeństwa	**Nazwa środka bezpieczeństwa lub zabezpieczenia rozszerzonego**	**Poziom bazowy C-SCRM**	**Kaskadowalny środek bezpieczeństwa**	**1**	**2**	**3**
AT-2(4)	*Szkolenie w zakresie uświadamiania bezpieczeństwa | Podejrzane komunikaty i nietypowe zachowania systemu*				x	
AT-2(5)	*Szkolenie w zakresie uświadamiania bezpieczeństwa | Zaawansowane trwałe zagrożenia*				x	
AT-2(6)	*Szkolenie w zakresie uświadamiania bezpieczeństwa | Środowiska zagrożeń związanych z cyberbezpieczeństwem*				x	
AT-3	**Szkolenie w zakresie bezpieczeństwa opartego na rolach**	x	x		x	
AT-3(2)	*Szkolenie w zakresie bezpieczeństwa opartego na rolach | Fizyczne środki bezpieczeństwa*				x	
AT-4	**Dokumentacja szkoleń**	x			x	
AU-1	**Polityka i procedury**	x		x	x	x
AU-2	**Rejestrowanie zdarzeń**	x	x	x	x	x
AU-3	**Zawartość dokumentacji kontroli**	x	x	x	x	x
AU-6	**Przegląd, analiza i sprawozdanie z kontroli**	x			x	x
AU-6(9)	*Przegląd, analiza i sprawozdanie z kontroli | Korelacja z informacjami ze źródeł nietechnicznych*					x

				Poziomy		
Identyfikator środka bezpieczeństwa	**Nazwa środka bezpieczeństwa lub zabezpieczenia rozszerzonego**	**Poziom bazowy C-SCRM**	**Kaskadowalny środek bezpieczeństwa**	**1**	**2**	**3**
AU-10	**Niezaprzeczalność**					x
AU-10(1)	*Niezaprzeczalność | Kojarzenie tożsamości*				x	
AU-10(2)	*Niezaprzeczalność | Potwierdzanie związku tożsamości twórcy informacji*				x	x
AU-10(3)	*Niezaprzeczalność | Łańcuch dowodowy*				x	x
AU-12	**Tworzenie dokumentacji kontroli**	x	x		x	x
AU-13	**Monitorowanie pod kątem ujawniania informacji**		x		x	x
AU-14	**Audyt sesji**		x		x	x
AU-16	**Dokumentacja kontroli międzyorganizacyjnych**				x	x
AU-16(2)	*Dokumentacja kontroli międzyorganizacyjnych | Udostępnianie informacji z kontroli*		x		x	x
CA-1	**Polityka i procedury**	x		x	x	x
CA-2	**Ocena zabezpieczeń**	x			x	x
CA-2(2)	*Ocena zabezpieczeń | Oceny specjalistyczne*					x
CA-2(3)	*Ocena zabezpieczeń | Wykorzystywanie wyników dostarczanych przez inne organizacje*					x
CA-3	**Wymiana informacji**	x	x			x

Tłumaczenie

				Poziomy		
Identyfikator środka bezpieczeństwa	**Nazwa środka bezpieczeństwa lub zabezpieczenia rozszerzonego**	**Poziom bazowy C-SCRM**	**Kaskadowalny środek bezpieczeństwa**	**1**	**2**	**3**
CA-5	**Plan i etapy działania**	x			x	x
CA-6	**Autoryzacja**	x		x	x	x
CA-7(3)	*Ciągłe monitorowanie | Analizy trendów*					x
CM-1	**Polityka i procedury**	x		x	x	x
CM-2	**Konfiguracja bazowa**	x	x		x	x
CM-2(6)	*Konfiguracja bazowa | Środowiska rozwojowe i testowe*				x	x
CM-3	**Zabezpieczanie zmian konfiguracji**		x		x	x
CM-3(1)	*Zabezpieczanie zmian konfiguracji | Automatyczna dokumentacja, powiadomienie i zakaz zmian*				x	x
CM-3(2)	*Zabezpieczanie zmian konfiguracji | Testowanie, walidacja i dokumentacja zmian*				x	x
CM-3(4)	*Zabezpieczanie zmian konfiguracji | Przedstawiciele ds. Bezpieczeństwa i prywatności*				x	x
CM-3(8)	*Zabezpieczanie zmian konfiguracji | Zapobieganie zmianom lub ograniczanie zmian w konfiguracji*				x	x
CM-4	**Analizy wpływu**	x				x
CM-4(1)	*Analizy wpływu | Oddzielne środowiska testowe*					x
CM-5	**Ograniczenia możliwości dokonywania zmian**	x			x	x

Tłumaczenie

				Poziomy		
Identyfikator środka bezpieczeństwa	**Nazwa środka bezpieczeństwa lub zabezpieczenia rozszerzonego**	**Poziom bazowy C-SCRM**	**Kaskadowalny środek bezpieczeństwa**	**1**	**2**	**3**
CM-5(1)	*Ograniczenia możliwości dokonywania zmian | Automatyczne Egzekwowanie uprawnień dostępu i dokumentacja*					x
CM-5(6)	*Ograniczenia możliwości dokonywania zmian | Ograniczenie dostępu do bibliotek*					x
CM-6	**Ustawienia konfiguracji**	x	x		x	x
CM-6(1)	*Ustawienia konfiguracji | Automatyczne zarządzanie, stosowanie i weryfikacja*					x
CM-6(2)	*Ustawienia konfiguracji | Reagowanie na nieautoryzowane zmiany*					x
CM-7	**Zasada minimalnej funkcjonalności**	x	x			x
CM-7(1)	*Zasada minimalnej funkcjonalności | Przegląd okresowy*				x	x
CM-7(4)	*Zasada minimalnej funkcjonalności | Nieautoryzowane oprogramowanie*				x	x
CM-7(5)	*Zasada minimalnej funkcjonalności | Autoryzowane oprogramowanie*					x
CM-7(6)	*Zasada minimalnej funkcjonalności | Środowiska z ograniczonymi uprawnieniami*				x	x

				Poziomy		
Identyfikator środka bezpieczeństwa	**Nazwa środka bezpieczeństwa lub zabezpieczenia rozszerzonego**	**Poziom bazowy C-SCRM**	**Kaskadowalny środek bezpieczeństwa**	**1**	**2**	**3**
CM-7(7)	*Zasada minimalnej funkcjonalności | Wykonywanie kodu w środowiskach chronionych*					x
CM-7(8)	*Zasada minimalnej funkcjonalności | Wykonywalny kod binarny lub maszynowy*				x	x
CM-7(9)	*Zasada minimalnej funkcjonalności | Zakaz używania nieautoryzowanego sprzętu*				x	x
CM-8	**Inwentaryzacja komponentów systemu**	x	x		x	x
CM-8(1)	*Inwentaryzacja komponentów systemu | Aktualizacje podczas instalacji i usuwania*					x
CM-8(2)	*Inwentaryzacja komponentów systemu | Automatyzacja utrzymania*					x
CM-8(4)	*Inwentaryzacja komponentów systemu | Informacje o rozliczalności*					x
CM-8(6)	*Inwentaryzacja komponentów systemu | Ocenione konfiguracje i zatwierdzone odchylenia*					x
CM-8(7)	*Inwentaryzacja komponentów systemu | Scentralizowane repozytorium*					x

				Poziomy		
Identyfikator środka bezpieczeństwa	**Nazwa środka bezpieczeństwa lub zabezpieczenia rozszerzonego**	**Poziom bazowy C-SCRM**	**Kaskadowalny środek bezpieczeństwa**	**1**	**2**	**3**
CM-8(8)	*Inwentaryzacja komponentów systemu | Automatyczne śledzenie lokalizacji*				x	x
CM-8(9)	*Inwentaryzacja komponentów systemu | Przypisanie komponentów do systemów*					x
CM-9	**Plan zarządzania konfiguracją**		x		x	x
CM-9(1)	*Plan zarządzania konfiguracją | Przypisanie odpowiedzialności*				x	x
CM-10	**Ograniczenia w użyciu oprogramowania**	x			x	x
CM-10(1)	*Ograniczenia w użyciu oprogramowania | Oprogramowanie otwartoźródłowe*				x	x
CM-11	**Oprogramowanie instalowane przez użytkownika**	x			x	x
CM-12	**Położenie (lokacja) informacji**				x	x
CM-12(1)	*Położenie (lokacja) informacji | Zautomatyzowane narzędzia wspierające lokalizację informacji*				x	x
CM-13	**Mapowanie działań na danych**				x	x
CM-14	**Podpisywanie komponentów**					x
CP-1	**Polityka i procedury**	x		x	x	x
CP-2	**Plan ciągłości działania**	x			x	x

				Poziomy		
Identyfikator środka bezpieczeństwa	**Nazwa środka bezpieczeństwa lub zabezpieczenia rozszerzonego**	**Poziom bazowy C-SCRM**	**Kaskadowalny środek bezpieczeństwa**	**1**	**2**	**3**
CP-2(1)	*Plan ciągłości działania | Koordynacja z powiązanymi planami*				x	x
CP-2(2)	*Plan ciągłości działania | Planowanie możliwości*				x	x
CP-2(7)	*Plan ciągłości działania | Koordynacja z dostawcami zewnętrznych usług*		x			x
CP-2(8)	*Plan ciągłości działania | Określenie krytycznych zasobów*					x
CP-3	**Szkolenie w zakresie planowania ciągłości działania**	x	x		x	x
CP-3(1)	*Szkolenie w zakresie planowania ciągłości działania | Symulowane zdarzenia*				x	x
CP-4	**Testowanie planu ciągłości działania**	x			x	x
CP-6	**Zapasowe miejsce przechowywania kopii**				x	x
CP-6(1)	*Zapasowe miejsce przechowywania kopii | Oddzielenie od głównego magazynu*				x	x
CP-7	**Zapasowe miejsce przetwarzania**				x	x
CP-8	**Usługi telekomunikacyjne**				x	x

				Poziomy		
Identyfikator środka bezpieczeństwa	**Nazwa środka bezpieczeństwa lub zabezpieczenia rozszerzonego**	**Poziom bazowy C-SCRM**	**Kaskadowalny środek bezpieczeństwa**	**1**	**2**	**3**
CP-8(3)	*Usługi telekomunikacyjne | Rozdzielenie dostawców głównych i alternatywnych*				x	x
CP-8(4)	*Usługi telekomunikacyjne | Plan ciągłości działania dostawcy*				x	x
CP-11	**Alternatywne protokoły komunikacji**				x	x
IA-1	**Polityka i procedury**	x		x	x	x
IA-2	**Identyfikacja i uwierzytelnianie (użytkownicy organizacyjni)**	x	x	x	x	x
IA-3	**Identyfikacja i uwierzytelnianie urządzenia**			x	x	x
IA-4	**Zarządzanie identyfikatorem**	x	x		x	x
IA-4(6)	*Zarządzanie identyfikatorem | Zarządzanie międzyorganizacyjne*			x	x	x
IA-5	**Zarządzanie metodami uwierzytelniania**	x	x		x	x
IA-5(5)	*Zarządzanie metodami uwierzytelniania | Zmiana danych uwierzytelniających przed dostawą*					x
IA-5(9)	*Zarządzanie metodami uwierzytelniania | Sfederowane zarządzanie poświadczeniami*					x
IA-8	**Identyfikacja i uwierzytelnianie (użytkownicy spoza organizacji)**	x			x	x
IA-9	**Identyfikacja i uwierzytelnianie usług**		x		x	x

				Poziomy		
Identyfikator środka bezpieczeństwa	**Nazwa środka bezpieczeństwa lub zabezpieczenia rozszerzonego**	**Poziom bazowy C-SCRM**	**Kaskadowalny środek bezpieczeństwa**	**1**	**2**	**3**
IR-1	**Polityka i procedury**	x	x	x	x	x
IR-2	**Szkolenie w zakresie reagowania na incydenty**	x	x		x	x
IR-3	**Testowanie reagowania na incydenty**				x	x
IR-4(6)	*Obsługa incydentów | Zagrożenia wewnętrzne*			x	x	x
IR-4(7)	*Obsługa incydentów | Zagrożenia wewnętrzne wewnątrz organizacji*			x	x	x
IR-4(10)	*Obsługa incydentów | Koordynacja łańcucha dostaw*		x		x	
IR-4(11)	*Obsługa incydentów | Zintegrowany zespół reagowania na incydenty*					x
IR-5	**Monitorowanie incydentów**	x			x	x
IR-6(3)	*Zgłaszanie incydentów | Koordynacja łańcucha dostaw*		x			x
IR-7(2)	*Pomoc w reagowaniu na incydenty | Koordynacja z dostawcami zewnętrznymi*		x			x
IR-8	**Plan reagowania na incydenty**	x	x		x	x
IR-9	**Reakcja na wyciek / ujawnienie informacji**		x			x
MA-1	**Polityka i procedury**	x	x	x	x	x
MA-2(2)	*Nadzór nad utrzymaniem | Zautomatyzowane działania związane z utrzymaniem*					x

				Poziomy		
Identyfikator środka bezpieczeństwa	**Nazwa środka bezpieczeństwa lub zabezpieczenia rozszerzonego**	**Poziom bazowy C-SCRM**	**Kaskadowalny środek bezpieczeństwa**	**1**	**2**	**3**
MA-3	**Narzędzia utrzymaniowe**				x	x
MA-3(1)	*Narzędzia utrzymaniowe | Kontrola narzędzi*					x
MA-3(2)	*Narzędzia utrzymaniowe | Kontrola nośników*					x
MA-3(3)	*Narzędzia utrzymaniowe | Zapobieganie nieautoryzowanemu usunięciu*					x
MA-4	**Utrzymanie zdalne**	x	x		x	x
MA-4(3)	*Utrzymanie zdalne | Porównywalne bezpieczeństwo i sanityzacja*				x	x
MA-5	**Personel utrzymaniowy**	x			x	x
MA-5(4)	*Personel utrzymaniowy | Cudzoziemcy*		x		x	x
MA-6	**Terminowość przeprowadzania konserwacji**					x
MA-7	**Konserwacja w terenie**					x
MA-8 *	**Monitorowanie konserwacji i wymiana informacji**					x
MP-1	**Polityka i procedury**	x		x	x	
MP-4	**Przechowywanie nośników danych**		x	x	x	
MP-5	**Transport nośników danych**			x	x	
MP-6	**Sanityzacja nośników danych**	x	x		x	x
PE-1	**Polityka i procedury**	x		x	x	x

				Poziomy		
Identyfikator środka bezpieczeństwa	**Nazwa środka bezpieczeństwa lub zabezpieczenia rozszerzonego**	**Poziom bazowy C-SCRM**	**Kaskadowalny środek bezpieczeństwa**	**1**	**2**	**3**
PE-2	**Zezwolenia na dostęp fizyczny**	x	x		x	x
PE-2(1)	*Zezwolenia na dostęp fizyczny | Dostęp na podstawie stanowiska lub roli*				x	x
PE-3	**Kontrola dostępu fizycznego**	x			x	x
PE-3(1)	*Kontrola dostępu fizycznego | Dostęp do systemu*				x	x
PE-3(2)	*Kontrola dostępu fizycznego | Obiekty i systemy*				x	x
PE-3(5)	*Kontrola dostępu fizycznego | Ochrona przed manipulacją*				x	x
PE-6	**Monitorowanie dostępu fizycznego**	x		x	x	x
PE-16	**Dostawa i usuwanie**	x				x
PE-17	**Zapasowe miejsce pracy**					x
PE-18	**Lokalizacja komponentów systemu**			x	x	x
PE-20	**Monitorowanie i śledzenie zasobów**				x	x
PE-23	**Lokalizacja obiektu**		x		x	x
PL-1	**Polityka i procedury**	x			x	
PL-2	**Plany bezpieczeństwa systemu i ochrony prywatności**	x	x			x
PL-4	**Zasady postępowania**	x			x	x
PL-7	**Koncepcja bezpieczeństwa działań operacyjnych**					x

Tłumaczenie

				Poziomy		
Identyfikator środka bezpieczeństwa	**Nazwa środka bezpieczeństwa lub zabezpieczenia rozszerzonego**	**Poziom bazowy C-SCRM**	**Kaskadowalny środek bezpieczeństwa**	**1**	**2**	**3**
PL-8	**Architektury bezpieczeństwa i ochrony prywatności**				x	x
PL-8(2)	*Architektury bezpieczeństwa i ochrony prywatności | Różnorodność dostawców*				x	x
PL-9	**Zarządzanie centralne**			x	x	
PL-10	**Wybór zabezpieczeń bazowych**	x			x	x
PM-2	**Role kierownicze programu bezpieczeństwa informacji**			x	x	
PM-3	**Zasoby w zakresie bezpieczeństwa informacji i ochrony prywatności**			x	x	
PM-4	**Plan działania i etapy wprowadzania zabezpieczeń**				x	x
PM-5	**Inwentaryzacja systemu**		x		x	x
PM-6	**Miary skuteczności**			x	x	
PM-7	**Struktura organizacyjna**			x	x	
PM-8	**Plan infrastruktury krytycznej**			x		
PM-9	**Strategia zarządzania ryzykiem**			x		
PM-10	**Proces autoryzacji**			x	x	
PM-11	**Definicja misji i procesu biznesowego**			x	x	x
PM-12	**Zagrożenia wewnętrzne**			x	x	x
PM-13	**Personel bezpieczeństwa i ochrony prywatności**			x	x	

				Poziomy		
Identyfikator środka bezpieczeństwa	**Nazwa środka bezpieczeństwa lub zabezpieczenia rozszerzonego**	**Poziom bazowy C-SCRM**	**Kaskadowalny środek bezpieczeństwa**	**1**	**2**	**3**
PM-14	**Testowanie, szkolenia i monitorowanie**			x	x	
PM-15	**Grupy i stowarzyszenia zajmujące się bezpieczeństwem i ochroną prywatności**			x	x	
PM-16	**Ostrzeganie o zagrożeniach**			x	x	
PM-17	**Ochrona nadzorowanych informacji jawnych przetwarzanych w systemach zewnętrznych**				x	
PM-18	**Plan programu ochrony prywatności**		x	x	x	
PM-19	**Role kierownicze programu ochrony prywatności**			x		
PM-20	**Rozpowszechnianie informacji o programie ochrony prywatności**			x	x	
PM-21	**Rejestrowanie ujawnień**			x	x	
PM-22	**Zarządzanie jakością danych osobowych**			x	x	
PM-23	**Organ zarządzania danymi**			x		
PM-25	**Minimalizacja danych osobowych wykorzystywanych w testach, szkoleniach i badaniach**				x	
PM-26	**Zarządzanie skargami**				x	x

Tłumaczenie

				Poziomy		
Identyfikator środka bezpieczeństwa	**Nazwa środka bezpieczeństwa lub zabezpieczenia rozszerzonego**	**Poziom bazowy C-SCRM**	**Kaskadowalny środek bezpieczeństwa**	**1**	**2**	**3**
PM-27	**Sprawozdawczość w zakresie ochrony prywatności**				x	x
PM-28	**Opracowywanie ram ryzyka**			x		
PM-29	**Role kierownicze programu zarządzania ryzykiem**			x		
PM-30	**Strategia zarządzania ryzykiem w łańcuchu dostaw**			x	x	
PM-31	**Strategia ciągłego monitorowania**			x	x	x
PM-32	**Przeznaczenie**				x	x
PS-1	**Polityka i procedury**	x	x	x	x	x
PS-3	**Dobór personelu**	x	x		x	x
PS-6	**Umowy dostępu / współpracy**	x	x		x	x
PS-7	**Bezpieczeństwo osobowe stron trzecich**	x			x	
PT-1	**Polityka i procedury**		x	x	x	x
RA-1	**Polityka i procedury**	x		x	x	x
RA-2	**Kategoryzacja bezpieczeństwa**	x		x	x	x
RA-3	**Szacowanie ryzyka**	x		x	x	x
RA-5	**Monitorowanie i skanowanie podatności**	x	x		x	x
RA-5(3)	*Monitorowanie i skanowanie podatności | Szerokość i głębokość pokrycia*				x	x

Tłumaczenie

				Poziomy		
Identyfikator środka bezpieczeństwa	**Nazwa środka bezpieczeństwa lub zabezpieczenia rozszerzonego**	**Poziom bazowy C-SCRM**	**Kaskadowalny środek bezpieczeństwa**	**1**	**2**	**3**
RA-5(6)	*Monitorowanie i skanowanie podatności | Automatyczna analiza trendów*				x	x
RA-7	**Reakcja na ryzyko**	x		x	x	x
RA-9	**Analiza krytyczności**		x	x	x	x
RA-10	**Wyszukiwanie zagrożeń**			x	x	x
SA-1	**Polityka i procedury**	x		x	x	x
SA-2	**Przydział zasobów**	x		x	x	
SA-3	**Cykl życia systemu**	x		x	x	x
SA-4	**Proces nabycia**	x		x	x	x
SA-4(5)	*Proces nabycia | Konfiguracja systemów, komponentów i usług*					x
SA-4(7)	*Proces nabycia | Profile ochrony zatwierdzone przez NIAP*				x	x
SA-4(8)	*Proces nabycia | Plan ciągłego monitorowania środków bezpieczeństwa*				x	x
SA-5	**Dokumentacja systemu**	x				x
SA-8	**Zasady inżynierii bezpieczeństwa i ochrony prywatności**	x		x	x	x
SA-9(1)	*Usługi systemu zewnętrznego | Oceny ryzyka i zatwierdzenia*				x	x

				Poziomy		
Identyfikator środka bezpieczeństwa	**Nazwa środka bezpieczeństwa lub zabezpieczenia rozszerzonego**	**Poziom bazowy C-SCRM**	**Kaskadowalny środek bezpieczeństwa**	**1**	**2**	**3**
SA-9(3)	*Usługi systemu zewnętrznego | Ustanowienie i utrzymanie relacji opartych na zaufaniu z dostawcami*			x	x	x
SA-9(4)	*Usługi systemu zewnętrznego | Spójne interesy konsumentów i dostawców*					x
SA-9(5)	*Usługi systemu zewnętrznego | Przetwarzanie, przechowywanie i lokalizacja usług*					x
SA-10	**Zarządzanie konfiguracją dewelopera**				x	x
SA-11	**Testowanie i ocena przez dewelopera**			x	x	x
SA-15	**Proces rozwoju, standardy i narzędzia**				x	x
SA-15(3)	*Proces rozwoju, standardy i narzędzia | Analiza krytyczności*				x	x
SA-15(4)	*Proces rozwoju, standardy i narzędzia | Modelowanie zagrożeń i analizy podatności*				x	x
SA-15(8)	*| Ponowne wykorzystanie informacji o zagrożeniach i podatnościach*					x
SA-16	**Szkolenia prowadzone przez dewelopera**				x	x

				Poziomy		
Identyfikator środka bezpieczeństwa	**Nazwa środka bezpieczeństwa lub zabezpieczenia rozszerzonego**	**Poziom bazowy C-SCRM**	**Kaskadowalny środek bezpieczeństwa**	**1**	**2**	**3**
SA-17	**Architektura oraz projekt bezpieczeństwa i ochrony prywatności dewelopera**				x	x
SA-20	**Niestandardowa (na zamówienie) rozbudowa komponentów krytycznych**				x	x
SA-21	**Dobór deweloperów**		x		x	x
SA-21(1)	*Dobór deweloperów | Potwierdzenie doboru*				x	x
SA-22	**Komponenty systemu bez wsparcia**	x			x	x
SC-1	**Polityka i procedury**	x		x	x	x
SC-4	**Informacje na współdzielonych zasobach systemowych**				x	x
SC-5(2)	*Ochrona przed blokadą usług (DoS) | Przepustowość i redundancja*				x	
SC-7	**Ochrona połączeń brzegowych**	x	x		x	
SC-7(13)	*Ochrona połączeń brzegowych | Izolacja narzędzi bezpieczeństwa, mechanizmów i elementów wspierających*		x			x
SC-7(14)	*Ochrona połączeń brzegowych | Ochrona przed nieautoryzowanymi połączeniami fizycznymi*				x	x

				Poziomy		
Identyfikator środka bezpieczeństwa	**Nazwa środka bezpieczeństwa lub zabezpieczenia rozszerzonego**	**Poziom bazowy C-SCRM**	**Kaskadowalny środek bezpieczeństwa**	**1**	**2**	**3**
SC-7(19)	*Ochrona połączeń brzegowych | Blokowanie komunikacji spoza organizacji*					x
SC-8	**Poufność i integralność transmisji**		x		x	x
SC-18	**Kod mobilny**					x
SC-18(2)	*Kod mobilny | Nabycie, rozwój i wykorzystanie*					x
SC-27	**Wieloplatformowość aplikacji**				x	x
SC-28	**Ochrona danych w składowaniu**		x		x	x
SC-29	**Heterogeniczność systemu**				x	x
SC-30	**Maskowanie i dezinformacja**				x	x
SC-30(2)	*Maskowanie i dezinformacja | Losowość*				x	x
SC-30(3)	*Maskowanie i dezinformacja | Zmiana miejsca przetwarzania i przechowywania*				x	x
SC-30(4)	*Maskowanie i dezinformacja | Wprowadzające w błąd informacje*				x	x
SC-30(5)	*Maskowanie i dezinformacja | Ukrywanie komponentów systemu*				x	x
SC-36	**Przetwarzanie i przechowywanie rozproszone**		x		x	x
SC-37(1)	*Kanały pozapasmowe | Zapewnianie dostaw i transmisji*				x	x
SC-38	**Bezpieczeństwo operacji**				x	x

				Poziomy		
Identyfikator środka bezpieczeństwa	**Nazwa środka bezpieczeństwa lub zabezpieczenia rozszerzonego**	**Poziom bazowy C-SCRM**	**Kaskadowalny środek bezpieczeństwa**	**1**	**2**	**3**
SC-47	**Alternatywne ścieżki komunikacyjne**			x	x	x
SI-1	**Polityka i procedury**	x		x	x	x
SI-2	**Usuwanie usterek**	x	x		x	x
SI-2(5)	*Usuwanie usterek | Automatyczne aktualizacje oprogramowania i oprogramowania sprzętowego*				x	
SI-3	**Zabezpieczenie przed złośliwym kodem**	x	x		x	x
SI-4	**Monitorowanie systemu**	x	x	x	x	x
SI-4(17)	*Monitorowanie systemu | Włączenie świadomości sytuacyjnej*				x	x
SI-4(19)	*Monitorowanie systemu | Ryzyko dla osób*				x	x
SI-5	**Alerty bezpieczeństwa, porady i dyrektywy**	x	x	x	x	x
SI-7	**Aplikacje, oprogramowanie układowe i integralność informacji**	x	x		x	x
SI-7(14)	*Aplikacje, oprogramowanie układowe i integralność informacji| Kod binarny lub wykonywalny maszynowo*				x	x
SI-7(15)	*Aplikacje, oprogramowanie układowe i integralność informacji| uwierzytelnianie kodu*					x

				Poziomy		
Identyfikator środka bezpieczeństwa	**Nazwa środka bezpieczeństwa lub zabezpieczenia rozszerzonego**	**Poziom bazowy C-SCRM**	**Kaskadowalny środek bezpieczeństwa**	**1**	**2**	**3**
SI-12	**Zarządzanie i retencja danych**	x				x
SI-20	**Skażenie**		x		x	x
SR-1	**Polityka i procedury**	x		x	x	x
SR-2	**Plan zarządzania ryzykiem w łańcuchu dostaw**	x				x
SR-3	**Zabezpieczenia i procesy w łańcuchu dostaw**	x		x	x	x
SR-3(1)	*Zabezpieczenia i procesy w łańcuchu dostaw | Zróżnicowana baza dostawców*				x	x
SR-3(3)	*Zabezpieczenia i procesy w łańcuchu dostaw | Kaskadowanie środków bezpieczeństwa*		x		x	x
SR-4	**Pochodzenie**				x	x
SR-5	**Strategie, narzędzia i metody nabycia**	x		x	x	x
SR-6	**Oceny i recenzje dostawców**				x	x
SR-7	**Bezpieczeństwo operacji w ramach łańcucha dostaw**				x	x
SR-8	**Umowy dotyczące powiadomień**	x			x	x
SR-9	**Odporność na manipulacje i wykrywanie sabotażu**				x	x
SR-10	**Kontrola systemów / komponentów**	x	x		x	x
SR-11	**Autentyczność komponentu**	x		x	x	x

				Poziomy		
Identyfikator środka bezpieczeństwa	**Nazwa środka bezpieczeństwa lub zabezpieczenia rozszerzonego**	**Poziom bazowy C-SCRM**	**Kaskadowalny środek bezpieczeństwa**	**1**	**2**	**3**
SR-11(1)	*Autentyczność komponentu | Szkolenie w zakresie wykrywania podróbek*	x			x	x
SR-11(2)	*Autentyczność komponentu | Zabezpieczenia konfiguracyjne w przypadku serwisu i naprawy komponentów*	x			x	x
SR-11(3)	*Autentyczność komponentu | Skanowanie w celu wykrywania podróbek*				x	x
SR-12	**Usuwanie komponentów**	x			x	x
SR-13 *	**Wykaz dostawców**				x	x

ZAŁĄCZNIK C RAMY NARAŻENIA NA RYZYKO[47]

Istnieje wiele możliwości celowego lub nieumyślnego wprowadzenia, stworzenia lub wykorzystania podatności, które mają wpływ na środowisko podmiotu lub wykorzystywane systemy i ich komponenty, w całym łańcuchu dostaw. Wykorzystanie tych podatności określamy mianem zdarzenia powodującego zagrożenie w łańcuchu dostaw. *Scenariusz zagrożenia to zbiór częściowo uporządkowanych w czasie zdarzeń związanych z określonym potencjalnym lub zidentyfikowanym istniejącym źródłem zagrożenia lub wieloma źródłami zagrożenia.* Opracowanie i analiza scenariuszy zagrożeń może pomóc podmiotom w pełniejszym zrozumieniu różnych rodzajów zagrożeń, które mogą wystąpić, oraz stworzyć podstawy do analizy prawdopodobieństwa i wpływu, jaki określone zdarzenie lub zdarzenia mogą mieć na podmiot. Przeprowadzenie tej analizy jest użytecznym sposobem na odkrycie luk w środkach bezpieczeństwa, a także określenie odpowiednich strategii łagodzących i wyznaczenie priorytetów w zakresie ich stosowania[48].

Scenariusze zagrożeń są zazwyczaj wykorzystywane na dwa sposoby:

1. Przełożenie nieuporządkowanych informacji uzyskanych z oceny ryzyka przeprowadzonej zgodnie z dokumentem [NSC 800-30] na scenariusze o węższym zakresie w celu dalszej oceny. Scenariusze te mogą pomóc podmiotom w odkryciu zależności oraz innych podatności, które wymagają poświęcenia uwagi oraz mogą zostać wykorzystane do celów szkoleniowych.
2. Określenie wpływu, jaki na podmiot miałoby udane wykorzystanie konkretnej podatności oraz określenie korzyści wynikających z zastosowania strategii łagodzących.

Scenariusze zagrożeń stanowią kluczowy element procesu zarządzania ryzykiem dotyczącego cyberbezpieczeństwa w łańcuchu dostaw, opisanego w Załączniku G niniejszej publikacji. Podmiot tworzy scenariusz zagrożeń w celu przeanalizowania

[47] Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

[48] Dodatkowe przykładowe scenariusze zagrożeń i listy zagrożeń można znaleźć w dokumencie ICT SCRM Task Force: Threat Scenarios Report (v3), August 2021, https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v3.pdf. Na potrzeby sprawozdania wykorzystano wersję dokumentu NIST SP 800-161 z 2015 roku.

zróżnicowanego zestawu zagrożeń i podatności, aby stworzyć spójną historię, która może być analizowana w ramach oceny ryzyka. Mając zdefiniowany scenariusz zagrożenia, podmiot może przeprowadzić ocenę ryzyka, aby zrozumieć, jak prawdopodobny jest ten scenariusz i co może się wydarzyć w jego wyniku. Analizowane elementy scenariusza zagrożeń są wykorzystywane do określenia ryzyka, które stanowi wniosek dotyczący poziomu narażenia podmiotu na ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw.

Po określeniu ryzyka podmiot określa sposób reagowania na ryzyko, korzystając w tym celu z ram narażenia na ryzyko. W ramach ram narażenia na ryzyko podmioty będą dokumentować scenariusz zagrożenia, analizę ryzyka, zidentyfikowaną strategię reakcji na ryzyko oraz wszelkie powiązane środki bezpieczeństwa związane z obszarem C-SCRM.

Niniejszy załącznik zawiera przykładowe ramy narażenia na ryzyko w obszarze C-SCRM, które mogą być wykorzystane przez podmiot w celu opracowania dopasowanych ram narażenia na ryzyko dla potencjalnych i zidentyfikowanych zagrożeń, które będą w większym stopniu odpowiadać ich potrzebom. Załącznik zawiera sześć przykładów ich wykorzystania. Przykłady różnią się nieco sposobem wykorzystania ram, aby zademonstrować możliwości dostosowania ich przez podmiot. Każdy przykład określa jedną lub więcej podatności, opisuje konkretne źródło zagrożenia, określa spodziewany wpływ na podmiot i proponuje środki bezpieczeństwa związane z obszarem C-SCRM opisane w dokumencie [NSC 800-161], które mogą ograniczyć ryzyko.

RAMY NARAŻENIA NA RYZYKO

Krok 1: Tworzenie planu opracowania i analizy scenariuszy zagrożeń

- Określenie celu analizy scenariusza zagrożeń w zakresie założeń, etapów (kamieni milowych) i oczekiwanych rezultatów.
- Określenie zakresu zastosowania w podmiocie, poziomu szczegółowości i innych ograniczeń.

- Określenie zasobów, które należy wykorzystać, w tym pracowników, czasu i sprzętu.
- Zdefiniowanie ram narażenia na ryzyko, które zostaną wykorzystane do analizy scenariuszy.

Krok 2: Charakteryzacja środowiska

- Zidentyfikowanie podstawowych misji i procesów biznesowych oraz kluczowych zależności podmiotu.
- Opisanie źródeł zagrożeń, które są istotne dla podmiotu. W stosownych przypadkach należy uwzględnić motywację i zasoby, jakimi dysponuje źródło zagrożenia.
- Wymienienie znanych podatności lub obszarów zagrożonych. (Uwaga: Obszary zagrożone mogą obejmować na przykład planowany outsourcing produkcji, zbliżające się rozwiązanie umowy dotyczącej utrzymania lub zaprzestanie produkcji elementu).
- Określenie istniejących i planowanych środków bezpieczeństwa.
- Określenie powiązanych przepisów, norm, polityk i procedur.
- Określenie dopuszczalnego poziomu ryzyka (progu ryzyka) w zależności od oceny taktyk, technik i procedur w podmiocie, krytyczności systemu oraz priorytetów w zakresie misji lub działalności jednostki odpowiedzialnej za ryzyko. Poziom ryzyka lub próg ryzyka może być okresowo weryfikowany i dostosowywany w celu odzwierciedlenia elastyczności globalnego łańcucha dostaw, zmian w podmiocie i nowych priorytetów w zakresie misji.

Krok 3: Opracowanie i wybór zdarzeń powodujących zagrożenie do analizy

- Wymienienie możliwych sposobów, w jakie źródła zagrożeń mogą wykorzystać znane podatności lub wpłynąć na obszary zagrożenia, aby opracować listę zdarzeń. (Uwaga: Do określenia tej informacji mogą okazać się użyteczne dane historyczne).
- Opisanie konsekwencji, które mogą wystąpić w wyniku każdego zdarzenia powodującego zagrożenie. Opis może być na tyle wyczerpujący lub szczegółowy, na ile jest to konieczne. W stosownych przypadkach należy ocenić prawdopodobieństwo i wpływ każdego zdarzenia.

- Wykluczenie zdarzeń, które wyraźnie wykraczają poza zdefiniowany cel i zakres analizy.
- Szczegółowe opisanie pozostałych zdarzeń powodujących zagrożenie. Należy uwzględnić taktyki, techniki i procedury, które źródło zagrożeń może wykorzystać do przeprowadzenia ataków. (Uwaga: Poziom szczegółowości opisu jest uzależniony od potrzeb podmiotu).
- Wybór do analizy zdarzeń, które są najlepiej dopasowane do zdefiniowanego celu i zakresu analizy. Bardziej prawdopodobne zdarzenia oraz zdarzenia skutkujące większym wpływem, poszczególne obszary oraz zdarzenia, które mogą reprezentować kilka z pozostałych wymienionych zdarzeń, są na ogół dobrymi propozycjami.

Krok 4: Przeprowadzenie analizy z wykorzystaniem ram narażenia na ryzyko

- W przypadku każdego zdarzenia zagrożenia należy odnotować wszelkie bezpośrednie konsekwencje zdarzenia oraz określić te jednostki organizacyjne i procesy, na które zdarzenie może mieć wpływ, uwzględniając obowiązujące przepisy, normy, polityki i procedury; istniejące i planowane środki bezpieczeństwa oraz zakres, w jakim środki bezpieczeństwa te są w stanie skutecznie zapobiegać, powstrzymać lub w inny sposób ograniczyć szkody, które mogłyby wyniknąć ze zdarzenia powodującego zagrożenie.
- Należy ocenić wpływ tych konsekwencji na misję i procesy biznesowe, informacje, aktywa, jednostki organizacyjne i interesariuszy. Najlepiej przeprowadzić to w kategoriach ilościowych na podstawie danych historycznych i z uwzględnieniem istniejących i planowanych środków bezpieczeństwa oraz obowiązujących przepisów, norm, zasad i procedur. (Uwaga: Korzystne może być określenie najbardziej prawdopodobnego poziomu wpływu oraz najgorszego możliwego scenariusza, a także scenariusza typu „atak stulecia").
- Określenie tych jednostek organizacyjnych, procesów, informacji (dostępu lub przepływu) oraz aktywów, które mogą być dotknięte w następstwie zdarzeń, a także konsekwencji i poziomów wpływu do momentu przeanalizowania

każdego elementu krytycznego, z uwzględnieniem istniejących i planowanych środków bezpieczeństwa oraz obowiązujących przepisów, standardów, zasad i procedur (np. w przypadku awarii krytycznego serwera jednym z pierwszych obszarów, które przystąpią do działania będzie dział wsparcia technologicznego, ale jeśli zespół stwierdzi, że do przywrócenia działania serwera potrzebna jest nowa część, może zostać zaangażowany dział zaopatrzenia).

Krok 5: Określenie środków bezpieczeństwa związanych z obszarem C-SCRM

- Określenie, czy i które zdarzenia scenariusza zagrożeń tworzą poziom ryzyka przekraczający akceptowalny przez jednostkę odpowiedzialną poziom (próg) ryzyka. (Uwaga: W niektórych przypadkach poziom akceptowalnego ryzyka może zależeć od możliwości wdrożenia lub kosztu strategii łagodzących). Określenie możliwości wzmocnienia istniejących środków bezpieczeństwa lub wdrożenia nowych zabezpieczeń. Korzystanie z listy norm lub zalecanych środków bezpieczeństwa może uprościć ten proces. Niniejszy załącznik wykorzystuje środki bezpieczeństwa wymienione w Załączniku A niniejszego dokumentu.
- Ocena skuteczności istniejących i planowanych zabezpieczeń w ograniczaniu ryzyka wystąpienia danego scenariusza.
- Ocena zdolności i zasobów (środków finansowych, pracowników i czasu) do wdrożenia potencjalnych nowych lub ulepszonych środków bezpieczeństwa.
- Określenie środków bezpieczeństwa związanych z obszarem C-SCRM lub połączenia środków bezpieczeństwa związanych z obszarem C-SCRM, które mogą spowodować, że ocena ryzyko szczątkowe zdarzenia zostanie obniżone do akceptowalnego poziomu w sposób najbardziej efektywny pod względem zasobów, z uwzględnieniem wszelkich zasad lub przepisów, które mogą mieć zastosowanie. (Uwaga: Należy uwzględnić możliwość, że jeden środek bezpieczeństwa pozwoli ograniczyć ryzyko więcej niż jednego zdarzenia lub że zwiększy ryzyko odrębnego zdarzenia).

Krok 6: Ocena/Przekazanie informacji zwrotnych

- Należy opracować plan wdrożenia wybranych środków bezpieczeństwa i ocenić ich skuteczność.
- Po ocenie skuteczności ram narażenia na ryzyko należy, w razie potrzeby, wprowadzić ulepszenia.

Tabela C-1: Przykładowe ramy narażenia na ryzyko

Zagrożenie		***Opis***
Scenariusz zagrożenia	**Opis zdarzenia powodującego zagrożenie**	*Opis możliwych sposobów, w jakie źródła zagrożeń mogą wykorzystać znane podatności lub wpłynąć na obszary zagrożenia, aby opracować listę zdarzeń.* Zdarzenie powodujące zagrożenie Zdarzenie lub sytuacja, które mogą potencjalnie spowodować niepożądane konsekwencje lub wpływ.
	Rezultat zdarzenia powodującego zagrożenie	*Opis rezultatu zdarzenia powodującego zagrożenie.* Rezultat zdarzenia powodującego zagrożenie: wpływ zagrożenia związanego z podatnością na poufność, integralność bądź dostępność działań, aktywów oraz pracowników podmiotu.
Jednostki podmiotu, procesy, informacje, aktywa lub interesariusze, których dotyczy zdarzenie		*Lista jednostek, procesów, informacji, aktywów lub interesariuszy podmiotu, których dotyczy zdarzenie.*
Ryzyko	**Wpływ**	*Opisać szacunkowy wpływ, stratę lub szkodę wynikające z urzeczywistnienia się zdarzenia powodującego zagrożenie i mogącego mieć wpływ na misję i procesy biznesowe, zasoby informacyjne lub interesariuszy. Szacunki powinny*

Zagrożenie		*Opis*
		być przedstawione w ujęciu ilościowym na podstawie danych historycznych i powinny uwzględniać istniejące i planowane środki bezpieczeństwa oraz obowiązujące przepisy, normy, polityki i procedury. (Uwaga: Korzystne może być określenie najbardziej prawdopodobnego poziomu wpływu oraz najgorszego możliwego scenariusza, a także scenariusza typu „atak stulecia"). Wpływ na działania organizacyjne, aktywa organizacyjne, osoby fizyczne, inne organizacje lub państwo – w tym interesy bezpieczeństwa narodowego lub utratę poufności, integralności lub dostępności informacji bądź systemu.
	Prawdopodobieństwo	*Opis prawdopodobieństwa wystąpienia określonego zdarzenia lub zdarzeń.* Prawdopodobieństwo: Szansa na wystąpienie danego zdarzenia.
	Narażenie na ryzyko (wpływ ryzyka x prawdopodobieństwo)	*Wynik ryzyka – iloczyn wpływu ryzyka i prawdopodobieństwa.* *Miara stopnia zagrożenia jednostki przez potencjalną okoliczność lub zdarzenie, zwykle stanowi wypadkową: (I) niekorzystnych skutków, które zaistniałyby w przypadku wystąpienia danej okoliczności lub danego zdarzenia; oraz (II) prawdopodobieństwa jego wystąpienia.*
	Dopuszczalny poziom ryzyka	*Określenie akceptowalnego poziomu ryzyka (progu ryzyka) w zależności od oceny taktyk, technik i procedur podmiotu, krytyczności systemu, apetytu na*

Zagrożenie		*Opis*
		ryzyko i tolerancji ryzyka oraz strategicznych celów jednostki odpowiedzialnej. Akceptowalne ryzyko: Poziom ryzyka szczątkowego dla operacji, aktywów lub pracowników podmiotu, który mieści się w ramach apetytu na ryzyko i deklarowanej tolerancji ryzyka ustalonych przez podmiot.
	Potencjalne strategie ograniczające ryzyko oraz środki bezpieczeństwa związane z obszarem C-SCRM	*Opis potencjalnych strategii ograniczenia ryzyka i wszelkie odpowiednie środki bezpieczeństwa związane z obszarem C-SCRM.* Ograniczanie ryzyka związanego z obszarem C-SCRM: Systematyczny proces zarządzania narażeniem na ryzyko związane z cyberbezpieczeństwem w łańcuchach dostaw, zagrożeniami i podatnościami w całym łańcuchu dostaw oraz opracowywanie strategii reagowania na ryzyko w odniesieniu do ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw.
	Szacunkowy koszt strategii ograniczających ryzyko	*Określenie szacunkowych kosztów strategii ograniczania ryzyka.*
	Zmiana prawdopodobieństwa	*Określenie potencjalnych zmian prawdopodobieństwa wystąpienia zdarzenia.*
	Zmiana wpływu	*Określenie potencjalnych zmian dotyczących wpływu ryzyka.*

Zagrożenie		*Opis*
	Wybrane strategie	*Określenie wybranych strategii ograniczania wpływu.*
	Szacowane ryzyko szczątkowe	*Określenie szacunkowego poziomu ryzyka szczątkowego.* Ryzyko szczątkowe: Część ryzyka, która pozostaje po wdrożeniu środków bezpieczeństwa.

PRZYKŁADOWE SCENARIUSZE

Niniejszy załącznik obejmuje sześć przykładowych scenariuszy zagrożeń wykorzystujących fikcyjną spółkę ABC oraz opisane powyżej ramy narażenia na ryzyko. Przykłady celowo różnią się poziomem szczegółowości i precyzji, aby pokazać, że scenariusze zagrożeń mogą być tak szczegółowe i rozbudowane, jak to konieczne. Choć podane scenariusze wykorzystują wartości procentowe oraz podstawowe oceny prawdopodobieństwa, wpływu i ryzyka (tj. wysokie, umiarkowane, niskie), podmioty mogą używać dowolnych i zróżnicowanych jednostek i skal (*np. Common Vulnerability Scoring System - CVSS*). Ponadto scenariusze te różnią się nieznacznie pod względem wdrożenia ram reakcji na ryzyko, co demonstruje, że ramy narażenia na ryzyko można dostosować w razie potrzeby.

SCENARIUSZ 1: WPŁYW NA DOSTAWCÓW LUB KONTROLA NAD DOSTAWCAMI PRZEZ RZĄDY OBCYCH PAŃSTW[49]

Informacje ogólne

Pewien podmiot postanowił przeprowadzić analizę scenariuszy zagrożeń dla swoich dostawców obwodów drukowanych (*ang. printed circuit board - PCB*). Scenariusz skupia się na wrażliwości podmiotu na nieprzewidziane wahania kosztów komponentów.

Źródło zagrożenia

Spółka ABC projektuje, montuje i dostarcza 3,5 miliona komputerów osobistych rocznie. Korzysta z usług dostawców z całego świata, a jej produkty są nabywane przez klientów z wielu obszarów świata. Pięć lat temu, dążąc do obniżenia kosztów sprzedawanych towarów, Spółka ABC przeniosła większość swoich zamówień na obwody drukowane do Azji Południowo-Wschodniej. Aby uniknąć zaopatrywania się u jednego dostawcy, spółka ABC podpisała umowy z pięcioma różnymi dostawcami w kraju i przez cały czas cieszyła się sprawną współpracą z każdym z nich.

Podatność

Chociaż spółka ABC zaopatruje się u wielu dostawców, polega na dostawcach z jednego kraju w Azji Południowo-Wschodniej. W wyniku tego wyboru spółka ABC jest narażona na zagrożenia geopolityczne ze względu na możliwość drastycznego wpływu polityki jednego rządu na dostępność dostarczanych materiałów i produktów.

Opis zdarzenia powodującego zagrożenie

Podmiot ustalił następujące fikcyjne zagrożenia na potrzeby przeprowadzenia analizy: W ubiegłym roku władzę w kraju, w którym spółka ABC prowadzi większość swoich interesów związanych z obwodami drukowanymi, przejęło nowe ugrupowanie. Nowy rząd skupił się na usprawnieniu prowadzenia działalności gospodarczej i finansowej w kraju, umożliwiając większym spółkom lokującym siedziby oraz zakłady w kraju czerpanie korzyści z łatwiejszego i tańszego prowadzenia interesów z dostawcami w tym samym regionie. Jednak w lutym 2019 roku skorumpowany rząd uchwalił nowe

[49] Treść Scenariusza 1 stanowi nieznacznie zmodyfikowany scenariusz (np. zmienione nazwy firm) zamieszczony w dokumencie ICT SCRM Task Force: Threat Scenarios Report (v3), August 2021, https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v3.pdf. Na potrzeby sprawozdania wykorzystano wersję dokumentu NIST SP 800-161 z 2015 roku.

przepisy, które spowodowały nałożenie dodatkowego 20-procentowego podatku na wszystkie komponenty elektroniczne i towary sprzedawane poza granice kraju. Nowe prawo miało wejść w życie 1 czerwca 2019 roku.

Kiedy ogłoszono nowe prawo, spółka ABC posiadała zapasy obwodów drukowanych wynoszące około 10% rocznego zapotrzebowania, co było typowym poziomem zapasów i nie stanowiło powodu do obaw. W miesiącach poprzedzających czerwiec spółka ABC skontaktowała się ze wszystkimi dostawcami, aby zamówić dodatkowe produkty, jednak pojawiły się niedobory z powodu zwiększonego zapotrzebowania wielu zagranicznych odbiorców na produkty. Do 1 czerwca, czyli do dnia wejścia w życie nowego prawa podatkowego, spółka ABC osiągnęła poziom zapasów w wysokości do 15% rocznego zapotrzebowania.

Rezultat

Od lutego do czerwca 2019 roku spółka ABC rozważała partnerstwo z nowymi dostawcami, jednak pojawił się szereg problemów. Co dziesiąty z dostawców, z którymi kontaktowała się spółka ABC, wymagał czasu na zwiększenie produkcji do oczekiwanego poziomu, wynoszącego od 6 do 18 miesięcy. Wymagałoby to dodatkowej pracy ze strony spółki ABC, w tym analizy próbek produktów dostawcy, finalizowania szczegółów logistycznych i monitorowania działań po stronie dostawcy niezbędnych do zaspokojenia nowego popytu, takich jak zakup surowców, zatrudnianie dodatkowych pracowników czy poszerzanie przestrzeni produkcyjnej.

Drugą kwestią było to, że obecne umowy ze wszystkimi pięcioma dostawcami w Azji Południowo-Wschodniej obejmowały minimalne ilości zamawianych produktów – w ich wyniku spółka ABC była zobowiązana do zakupu co najmniej 100 000 sztuk obwodów drukowanych miesięcznie przez okres obowiązywania umów, który wynosił od 3 do 24 miesięcy. Oznaczałoby to, że spółka ABC nie była w stanie łatwo uniknąć kosztu nowego podatku. Czy spółka ABC mogła ponieść wyższe koszty? Przy wzroście kosztów o 20% doprowadziło to do obniżenia marży na jednym komputerze z 13,5% do średnio 4,5%. W przypadku niektórych produktów o niższej marży pojawiała się konieczność zawieszenia produkcji oraz wykorzystanie droższych obwodów w modelach z wyższej półki, które można było sprzedawać z wyższą marżą.

Jednostki organizacyjne i procesy, których dotyczą skutki ryzyka

Brak

Potencjalne strategie ograniczające ryzyko oraz środki bezpieczeństwa związane z obszarem C-SCRM

- Przeprowadzanie regularnych ocen i przeglądów ryzyka związanego z dostawcami[50].
- Dywersyfikacja dostawców według lokalizacji, a także kraju, regionu i innych czynników.
- Uwzględnienie wpływu kosztów w umowach z dostawcami, co ułatwi rozwiązanie umów w przypadku nadmiernego wzrostu kosztów z winy dostawcy lub z innych powodów.
- Dostosowanie poziomów zapasów, aby lepiej uwzględnić nieoczekiwany niedobór produktów w krytycznych momentach.
- Zatrudnienie większej liczby pracowników w krajach lub regionach, w których działają kluczowi dostawcy, aby uzyskiwać wcześniejsze informacje o nowych przepisach, które mogą mieć negatywny wpływ na działalność.

Tabela C-2: Scenariusz 1

Scenariusz zagrożenia	**Źródło zagrożenia**	Dynamiczne warunki geopolityczne, które wpływają na dostawy komponentów do produkcji komputerów PC.
	Podatność	Geograficzna koncentracja dostawców kluczowych komponentów.
	Opis zdarzenia powodującego zagrożenie	Spółka ABC przeniosła większość swoich zamówień na obwody drukowane (PCB) do Azji Południowo-Wschodniej, aby obniżyć koszty sprzedawanych towarów. Starając się uniknąć korzystania z jednego źródła, spółka ABC zawarła umowy z pięcioma różnymi dostawcami w kraju. W kraju, w którym spółka ABC produkuje większość wykorzystywanych obwodów drukowanych, władzę

[50] Regularna ocena i przegląd strategii ograniczania ryzyka związanego z dostawcami zostały dodane do oryginalnego tekstu scenariusza 1 znajdującego się w dokumencie ICT SCRM Task Force: Threat Scenarios Report (v3), August 2021, https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios- report-v3.pdf. Na potrzeby sprawozdania wykorzystano wersję dokumentu NIST SP 800-161 z 2015 roku.

		przejęło nowe ugrupowanie. W lutym 2019 roku skorumpowany rząd uchwalił nowe przepisy, które spowodowały nałożenie dodatkowego 20-procentowego podatku na wszystkie komponenty elektroniczne i towary sprzedawane poza granice kraju. Nowa ustawa miała wejść w życie 1 czerwca 2019 roku. Kiedy ogłoszono nowe prawo, spółka ABC posiadała zapasy obwodów drukowanych wynoszące około 10% rocznego zapotrzebowania, co było typowym poziomem zapasów i nie stanowiło dla niej powodu do obaw. W miesiącach poprzedzających wejście w życie nowych przepisów, spółka ABC skontaktowała się ze wszystkimi dostawcami, aby zamówić dodatkowe produkty, jednak pojawiły się niedobory z powodu zwiększonego zapotrzebowania na produkty. Do 1 czerwca, czyli do dnia wejścia w życie nowego prawa podatkowego, spółka ABC osiągnęła poziom zapasów w wysokości do 15% rocznego zapotrzebowania.
	Rezultat zdarzenia powodującego zagrożenie	Spółka ABC rozważała nawiązanie współpracy z nowymi dostawcami, jednak natrafiła na wiele problemów. Co dziesiąty z dostawców, z którymi kontaktowała się spółka ABC, wymagał czasu na zwiększenie produkcji do oczekiwanego poziomu, wynoszącego od 6 do 18 miesięcy. Drugim problemem był fakt, że istniejące umowy z dostawcami w Azji Południowo-Wschodniej obejmowały minimalne ilości zamawianych produktów – w ich wyniku spółka ABC była zobowiązana do zakupu co najmniej 100 000 sztuk obwodów drukowanych miesięcznie przez okres obowiązywania umów, który wynosił od 3 do 24 miesięcy. Oznaczałoby to, że spółka ABC nie była w stanie łatwo uniknąć kosztu nowego podatku. Przy 20-procentowym wzroście kosztów marże na wytwarzanych i sprzedawanych komputerach spadły średnio z 13,5% do 4,5%.

Jednostki podmiotu / procesy, których to dotyczy		Brak	
Ryzyko	**Wpływ**	Wysoki: Obniżenie zysku ze sprzedaży komputerów PC o 40 000 000 dolarów.	
	Prawdopodobieństwo	Umiarkowane: Uśrednione roczne prawdopodobieństwo wystąpienia: 10%.	
	Narażenie na ryzyko (wpływ ryzyka x prawdopodobieństwo)	Wysokie: Wartość narażenia na ryzyko wynosi około 4 000 000 dolarów zysków ze sprzedaży.	
	Dopuszczalny poziom ryzyka	Prawdopodobieństwo poniżej 10% dla ryzyka spadku zysków ze sprzedaży o więcej niż 10 000 000 dolarów.	
Ograniczanie ryzyka	**Potencjalne strategie ograniczające ryzyko oraz środki bezpieczeństwa związane z obszarem C-SCRM**	Ocena oraz przegląd ryzyka związanego z dostawcą, aby uwzględnić FOCI [SR-6(1)], zastosowanie wymogów dotyczących różnorodności dostawców [C-SCRM_PL-3(1)], zapewnienie różnorodności dostawców [SCRM_PL-8(2)] i dostosowanie poziomów zapasów [CM-8].	Przeprowadzanie regularnych ocen i przeglądów ryzyka związanego z dostawcami. Dywersyfikacja dostawców według lokalizacji, a także kraju, regionu i innych czynników. Uwzględnienie wpływu kosztów w umowach z dostawcami, co ułatwi rozwiązanie umów w przypadku ich nadmiernego wzrostu z winy dostawcy lub z innych powodów. Dostosowanie poziomów zapasów,

			aby lepiej uwzględnić nieoczekiwany niedobór produktów w krytycznych momentach. Zatrudnienie większej liczby pracowników w krajach lub regionach, w których działają kluczowi dostawcy, aby uzyskiwać wcześniejsze informacje o nowych przepisach, które mogą mieć negatywny wpływ na działalność.
	Szacunkowy koszt strategii ograniczających ryzyko	Brak	
	Zmiana prawdopodobieństwa	Niskie: 10% prawdopodobieństwo wystąpienia.	
	Zmiana wpływu	Umiarkowane: 2 000 000 dolarów zysku ze sprzedaży produktów.	
	Wybrane strategie	Kombinacja strategii ograniczania ryzyka.	
	Szacowane ryzyko szczątkowe	Niskie: Ekspozycja na ryzyko szczątkowe wynosi 0,02% marży ze sprzedaży komputerów PC.	

SCENARIUSZ 2: PODRÓBKI PRODUKTÓW TELEKOMUNIKACYJNYCH

Informacje ogólne

Duża spółka ABC opracowała system, którego utrzymaniem zajmuje się zewnętrzny integrator na podstawie umowy. System wykorzystuje popularny komponent telekomunikacyjny, który nie jest już wytwarzany przez producenta. Producent zaoferował nowszy produkt jako zamiennik, jednak jego zastosowanie wymaga modyfikacji systemu kosztem około 1 miliona dolarów. Jeśli element nie zostanie zmodernizowany, spółka i integrator systemu będą musieli polegać na dostawcach z rynku wtórnego w kwestii części zamiennych. Nowszy produkt nie zapewnia znaczącej poprawy osiągów w stosunku do obecnie stosowanego komponentu.

Spółka ABC postanowiła przeprowadzić analizę scenariusza zagrożeń, aby określić czy zmodyfikować system, aby zastosować nowy produkt, czy też zaakceptować ryzyko dalszego korzystania z produktu, który nie jest już produkowany.

Środowisko

Środowisko charakteryzują następujące cechy:

- Istnieje oczekiwanie, że system będzie działał jeszcze przez 10 lat bez większych modernizacji lub modyfikacji, w dodatku wymaga czasu sprawności wynoszącego 99,9% czasu działania.
- Cały system opiera się na ponad 1000 komponentach o wartości 200 dolarów, a około 10% z nich jest wymienianych co roku z powodu zużycia, awarii lub innych przyczyn. W każdej chwili integrator dysponuje 3-miesięcznym zapasem komponentów.
- Komponent jest stale monitorowany pod kątem funkcjonalności, a ponadto istnieją skuteczne procedury umożliwiające przekierowanie ruchu i jego wymianę w przypadku nieoczekiwanej awarii.
- Przerwy w pracy wynikające z niespodziewanej awarii komponentu są rzadkie, lokalne i trwają zaledwie kilka minut. Gdy element ulegnie awarii, funkcjonalność systemu jest poważnie ograniczona przez około jedną do

czterech godzin, podczas gdy problem jest diagnozowany i naprawiany lub gdy komponent jest wymieniany.

- Produkty takie jak omawiany komponent były często podrabiane.
- Integrator wdrożył politykę ograniczającą zakup towarów podrabianych oraz procedurę postępowania w przypadku wykrycia podróbki [patrz SR-11].
- Integrator i agencja wdrożyły ograniczone procedury testowania, aby zapewnić funkcjonalność elementu przed jego przyjęciem [patrz SR-5(2)].

Zdarzenie powodujące zagrożenie

W ramach prac nad scenariuszem zagrożenia, spółka stworzyła fikcyjne źródło zagrożenia, które opisała jako grupę motywowaną zyskiem z ogromnym doświadczeniem w tworzeniu podrobionych produktów. Takie podmioty są w stanie uzyskać olbrzymie zyski tworząc i sprzedając podróbki, które są wizualnie identyczne z ich oryginalnymi odpowiednikami, ale wykorzystują materiały niższej jakości. Dysponują zasobami umożliwiającymi kopiowanie większości znaków towarowych i innych cech identyfikacyjnych oraz wprowadzanie podróbek do łańcucha dostaw powszechnie wykorzystywanego przez podmiot przy niewielkim lub zerowym ryzyku wykrycia. Podrobiony produkt jest atrakcyjny dla nieświadomych kupujących, ponieważ jest zazwyczaj oferowany z rabatem i sprzedawany jako nadwyżka magazynowa.

Gdyby do systemu wprowadzono element gorszej jakości, prawdopodobnie ulegałby on awarii częściej niż zgodnie z oczekiwaniami, ograniczając funkcjonalność systemu. W przypadku dużej liczby podrobionych produktów pomieszanych z oryginalnymi komponentami w systemie, liczba i dotkliwość niespodziewanych przestojów mogą znacznie wzrosnąć. Spółka i integrator zdecydowali, że ryzyko zakupu podrobionego produktu w celu konserwacji systemu oraz szacowany potencjalny wpływ takiego zdarzenia są wystarczająco wysokie, aby uzasadnić przeprowadzenie bardziej kompleksowej oceny.

Analiza scenariusza zagrożeń

W pierwszej kolejności wpływ ryzyka nabycia podrobionego produktu dotknąłby osób odpowiedzialnych za ich zakup. Polityka wymaga, aby starali się kupować oryginalne

produkty od sprawdzonych dostawców. Osoby te musiałyby zostać przekonane, że produkt jest autentyczny. Ponieważ przedmiotowa podróbka jest wizualnie identyczna z poszukiwanym komponentem i oferowana z rabatem, istnieje duże prawdopodobieństwo, że zostanie zakupiona. Jeden z produktów zostanie przetestowany pod kątem funkcjonalności, a następnie cały zapas trafi do magazynu.

Gdy jeden z elementów systemu będzie wymagał wymiany, obsługa techniczna zainstaluje podróbkę, przetestuje ją pod kątem prawidłowego działania i udokumentuje wymianę. Zanim podrobiony produkt ulegnie awarii, mogą minąć dwa lata, a do systemu może trafić nawet 200 podrobionych komponentów, zanim nastąpi pierwsza awaria. Jeśli wszystkie regularnie wymieniane elementy zostaną zastąpione podróbkami, a każda podróbka ulegnie awarii po dwóch latach, koszt obsługi systemu wzrośnie o 160 000 dolarów w ciągu 10 lat. Wymagany czas konserwacji oznaczałby także konieczność zatrudnienia dodatkowych pracowników oraz poniesienie innych wydatków przez integratora systemu.

Gdy podróbka ulegnie awarii, diagnostyka i wymiana elementu zajmie około jednej do czterech godzin, w tym czasie wydajność systemu jest mocno ograniczona. Jeśli więcej niż jeden z elementów ulegnie awarii w tym samym czasie, system może ulec całkowitej awarii. Może to spowodować znaczące problemy w działalności spółki i naruszyć określone w umowie gwarancje czasu pracy wynoszące 99,9%. Co więcej, jeśli podmiot ustali, że element uległ awarii ze względu na to, że został podrobiony, będzie musiał ponieść dodatkowe koszty związane ze zgłoszeniem podróbki.

Strategia ograniczająca ryzyko

Podmiot ustalił następujące działania ograniczające ryzyko (na podstawie Załącznika A do dokumentu NSC 800-161):

- Wymaganie od deweloperów przeprowadzania testów/oceny bezpieczeństwa we wszystkich fazach cyklu życia systemu po zakończeniu projektowania [patrz SA-11].
- Weryfikacja, że otrzymany system informacyjny lub komponent systemu jest autentyczny oraz że nie został zmanipulowany [patrz SR-11].

- Włączenie wymagań bezpieczeństwa do projektowania systemów informacyjnych (inżynieria bezpieczeństwa) [patrz PL-8, SC-36].
- Stosowanie wymagań dotyczących różnorodności dostawców [PL-8(2)].

Na podstawie tych środków bezpieczeństwa spółka była w stanie opracować strategię obejmującą:

- Testy akceptacyjne: Badanie komponentów w celu zapewnienia, że są nowe, oryginalne i że wszystkie związane z nimi licencje są ważne. Metody badań obejmują kontrolę fizyczną przeprowadzaną przez przeszkolonych pracowników z wykorzystaniem obrazowania cyfrowego, weryfikację podpisu cyfrowego, weryfikację numeru seryjnego oraz numeru części, a także badanie elektryczne próbek.
- Zwiększenie wymagań bezpieczeństwa w projekcie systemu poprzez dodanie elementów redundantnych wzdłuż bardziej krytycznych ścieżek (określonych w analizie krytyczności) w celu zminimalizowania wpływu awarii komponentu.
- Znalezienie alternatywnych, sprawdzonych dostawców komponentów.

Po przeprowadzeniu analiz ustalono, że zastosowanie tej strategii będzie kosztowało mniej niż akceptacja ryzyka wprowadzenia do systemu podróbek lub zmodyfikowanie systemu w celu zastosowania nowego elementu. Szacowany koszt wdrożenia bardziej rygorystycznego programu zamówień oraz testowania komponentów wyniósł 80 000 dolarów. Koszt zwiększenia wymagań w zakresie bezpieczeństwa wyniósł 100 000 dolarów.

Tabela C-3: Scenariusz 2

Scenariusz zagrożenia	**Źródło zagrożenia**	Podrobiony komponent telekomunikacyjny wprowadzony do łańcucha dostaw
	Podatność	Element nie jest już produkowany przez producenta. Nabywcy nie są w stanie lub nie chcą znaleźć oraz zakupić wyłącznie oryginalnych komponentów.
	Opis zdarzenia powodującego zagrożenie	Czynnik zagrożenia wprowadza swój podrobiony element do zaufanego łańcucha dystrybucji. Organizacje kupują podrobiony komponent. Podrobione komponenty są instalowane w systemie.
	Rezultat zdarzenia powodującego zagrożenie	Komponent ulega awarii częściej niż dotychczas, zwiększając liczbę przestojów.
Jednostki podmiotu, procesy, informacje, aktywa lub interesariusze, których dotyczy zdarzenie		Dział zamówień Dział utrzymania Dział odpowiedzialny za relacje z producentami / dostawcami Funkcje kluczowego działania
Ryzyko	**Wpływ**	Umiarkowane: Awaria elementu prowadzi do 1-4 godzinnego przestoju systemu.
	Prawdopodobieństwo	Wysokie: Znacząca motywacja ze strony podmiotu stwarzającego zagrożenie oraz wysoka podatność na zagrożenia ze względu na niezdolność spółki do wykrywania podróbek z 25% prawdopodobieństwem przedwczesnej awarii komponentów w ciągu roku.
	Narażenie na ryzyko (wpływ ryzyka x prawdopodobieństwo)	Średnie: Znaczące krótkotrwałe utrudnienia, które sprawią, że czas przestoju może spaść poniżej progu określonego w umowie o 0,5% (np. 99,4% < 99,9%).

	Dopuszczalny poziom ryzyka	Niskie: Mniejsze niż 10% prawdopodobieństwo czasu przestoju doprowadzającego do spadku poniżej progu 99%.	
Ograniczanie ryzyka	**Potencjalne strategie ograniczające ryzyko oraz środki bezpieczeństwa związane z obszarem C-SCRM**	Zwiększenie możliwości w zakresie testów akceptacyjnych [C-SCRM_SA-9; C-SCRM_SA-10] i wymagań dotyczące bezpieczeństwa w projektowaniu systemów [C-SCRM_PL-2], a także stosowanie wymagań dotyczących zróżnicowania dostawców [C-SCRM_PL-8(2)].	Zmodyfikowanie systemu w celu instalacji nowych komponentów.
	Szacunkowy koszt strategii ograniczających ryzyko	180 000 dolarów	1 milion dolarów
	Zmiana prawdopodobieństwa	Niskie: 8% prawdopodobieństwo awarii komponentu w skali roku.	
	Zmiana wpływu	Niski: Awaria elementu powoduje przekierowanie do nadmiarowych komponentów systemu – koszt jest ograniczony do konserwacji i wymiany.	
	Wybrane strategie	Badanie i testowanie na poziomie spółki. Umieszczenie komponentów w depozycie do czasu spełnienia ustalonych kryteriów testów akceptacyjnych. Zwiększenie poziomu inżynierii bezpieczeństwa. Znalezienie wielu dostawców komponentu.	
	Szacowane ryzyko szczątkowe	Niskie: 8% prawdopodobieństwo awarii komponentu prowadzącej do przestoju systemu i spadku dostępności poniżej 99,9%.	

SCENARIUSZ 3: SZPIEGOSTWO PRZEMYSŁOWE

Informacje ogólne

Spółka ABC produkująca półprzewodniki, wykorzystywana przez podmiot do produkcji systemów wojskowych i lotniczych, rozważa partnerstwo ze spółką KXY. – W ramach współpracy chce wykorzystywać jej zakłady produkcyjne. Stanowiłoby to znaczącą zmianę w łańcuchu dostaw związanym z krytycznym elementem systemu. Utworzono komitet, w skład którego weszli przedstawiciele podmiotu, spółki ABC oraz integratora, aby pomóc w określeniu wpływu, jaki nowe partnerstwo będzie miało na podmiot oraz odpowiednich praktyk ograniczających ryzyko, które należy wprowadzić po jego ustanowieniu.

Środowisko

Systemy, których dotyczy analiza, mają zasadnicze znaczenie dla bezpieczeństwa misji wojskowych i lotniczych. Element, który ma być wytwarzany przez spółkę KXY, jest wyjątkowy, opatentowany i krytyczny dla działania systemów. Utrata dostępności elementu podczas działania systemu mogłaby mieć znaczące, natychmiastowe skutki dla wielu organizacji i ludności cywilnej - w tym śmierć wielu osób i szkody liczone w milionach dolarów. Przeprowadzono wstępną ocenę ryzyka na podstawie dokumentu [NSC 800-30], która doprowadziła do ustalenia poziomu ryzyka na „Umiarkowany”.

Spółka KXY wykorzystuje najnowocześniejszą, tanią technologię wytwarzania płytek krzemowych na potrzeby komercyjne. Państwo, w którym działa KXY, w przeszłości uciekało się do wykorzystywania szpiegostwa przemysłowego w celu zdobycia własności intelektualnej oraz technologii. Władze wykazują zainteresowanie technologią półprzewodnikową i przekazały znaczące dofinansowania spółce KXY na rozwój na rynku wojskowym i lotniczym. Choć spółka KXY nie dysponuje obecnie infrastrukturą badawczą umożliwiającą spełnienie wymagań przemysłu wiodących państw, zasoby państwa narodowego są znaczące i obejmują zdolność do zapewnienia zarówno ustępstw, jak i zachęt, aby pomóc KXY w spełnieniu tych wymagań. Najważniejsze obawy dotyczą faktu, że państwo, w którym działa spółka KXY, może wykorzystać swoje wpływy, aby uzyskać dostęp do komponentu lub jego projektu.

Komitet dokonał przeglądu istniejących strategii ograniczania ryzyka i ustalił, że spółka ABC, integrator oraz podmiot wdrożyły szereg praktyk w celu zapewnienia, że system i wszystkie krytyczne elementy, ustalone w ramach analizy krytyczności, spełniają określone wymagania dotyczące funkcjonalności. Na przykład, system i elementy krytyczne są badane pod kątem zgodności z odpowiednimi normami branżowymi. W ramach wymagań opartych na dokumencie [NSC 800-53], spółka zastosowała szereg wymagań dotyczących ochrony informacji (patrz PM-11). Ponadto spółka ABC wdrożyła zaawansowany system śledzenia zapasów, który wymagał, aby większość elementów była jednoznacznie oznakowana przy użyciu technologii RFID lub w inny sposób oznaczona w celu ich śledzenia (patrz SR-4).

Scenariusz zagrożenia

Na podstawie wcześniejszych doświadczeń spółka uznała, że państwo, w którym spółka KXY ma siedzibę, prawdopodobnie zrobiłoby jedną z dwóch rzeczy, gdyby uzyskało dostęp do technologii: 1) sprzedało ją zainteresowanym podmiotom lub 2) wprowadziłoby podatności lub poszukało podatności w celu późniejszego wykorzystania. Aby którekolwiek z tych zdarzeń powodujących zagrożenie mogło ulec materializacji, kraj działalności spółki KXY musiałby znać przeznaczenie komponentu oraz mieć dostęp do komponentu lub jego projektu. Było to możliwe poprzez współpracę z działem kadr KXY, oszustwo, kradzież fizyczną lub wyciek informacji. Kradzież fizyczna byłaby trudna ze względu na istniejące zabezpieczenia i środki bezpieczeństwa fizycznego, a także procedury zabezpieczania zapasów. Aby zmodyfikowany element mógł zostać zakupiony i zintegrowany z systemem, musiałby przejść różne procedury testowe zarówno na poziomie integratora, jak i spółki. Stosowane metody badawcze obejmują badania radiograficzne, analizy materiałowe, testy elektryczne oraz badania trwałości i wytrzymałości. Modyfikacje etykiet oraz rozwiązań identyfikacyjnych musiałyby być niewykrywalne w badaniu podstawowym. Ponadto spółka KXY miała przechodzić regularne kontrole sprawdzające jej procesy w zakresie zapewnienia jakości i funkcjonalności komponentów.

Komitet uznał, że pomimo istniejących praktyk, istnieje 30-procentowa szansa, że państwo będące siedzibą spółki KXY będzie miało potrzebę, możliwość i zdolność do wprowadzenia złośliwych modyfikacji elementu bez wykrycia, wykorzystania nieznanych wcześniej podatności lub zapewnienia jednemu ze swoich sojuszników możliwości realizacji takiego działania. Może to spowodować utratę dostępności lub integralności systemu, powodując znaczne szkody. Wykorzystując informacje ze wstępnej oceny ryzyka przeprowadzonej na podstawie dokumentu [NSC 800-30], komitet określił to jako najgorszy scenariusz i uznał jego wpływ jako wysoki.

Ponadto stwierdzono 40-procentową szansę, że kraj docelowy mógłby sprzedać technologię zainteresowanym stronom, co spowodowałoby utratę przewagi technologicznej. Gdyby taki scenariusz uległ materializacji, życie wojskowych i cywilów w krajach sojuszniczych mogłoby być zagrożone, działania wywiadowcze zostałyby narażone na szwank, a w dodatku konieczne byłoby opracowanie nowego rozwiązania, co będzie wiązało się z dodatkowymi kosztami. Komitet uznał, że wpływ takiego scenariusza jest umiarkowany.

Komitet ustalił, że ogólna łączna ekspozycja na ryzyko dla tych podatności jest wysoka.

Strategie ograniczania ryzyka

Korzystając z załącznika A do dokumentu NSC 800-161, komitet określił trzy szeroko zakrojone strategie działania: (1) zwiększanie identyfikowalności, (2) zwiększenie wymagań dotyczących pochodzenia i informacji oraz (3) wybór innego dostawcy. Te trzy warianty zostały przeanalizowane dogłębnie w celu określenia konkretnych strategii wdrożeniowych, ich wpływu na scenariusze oraz szacunkowego kosztu wdrożenia. (W tym przypadku nie opisano konkretnych technik ani technologii, jednak ich opis byłby użyteczny w przypadku oceny rzeczywistego scenariusza zagrożenia).

Poprawa identyfikowalności i możliwości monitorowania:

- CM-8 – Inwentaryzacja komponentów systemu
- IA-1 – Polityka i procedury

- SA-10 – Zarządzanie konfiguracją dewelopera
- SR-8 – Umowy dotyczące powiadomień
- SR-4 – Pochodzenie

Koszt = wzrost o 20%

Wpływ = zmniejszenie o 10%

Zwiększenie wymagań dotyczących pochodzenia oraz zabezpieczeń informacji:

- AC-21 – Udostępnianie informacji
- SR-4 – Pochodzenie

Koszt = wzrost o 20%

Wpływ = zmniejszenie o 20%

Wybór innego dostawcy:

- SR-6 – Oceny i recenzje dostawców

Koszt = wzrost o 40%

Wpływ = zmniejszenie o 80%

Na podstawie tej analizy komitet zdecydował się na wdrożenie połączenia szeregu działań:

- Opracowanie i wymaganie wyjątkowych, trudnych do skopiowania etykiet lub zmiana etykiety, aby zniechęcić do klonowania lub modyfikacji komponentu [patrz SR-3(2)].
- Minimalizacja ilości informacji udostępnianych dostawcom. Wymagania w zakresie zabezpieczenia informacji [patrz AC-21].
- Wymagania dotyczące pochodzenia oraz aktualizacji informacji na temat pochodzenia w całym cyklu życia systemu [patrz SR-4].

Przy takim połączeniu zabezpieczeń oszacowane ryzyko szczątkowe zostało określone jako równoważne istniejącemu ryzyku, a wzrost kosztów okazał się mniejszy niż w przypadku zmiany dostawcy.

Tabela C-4: Scenariusz 3

Scenariusz zagrożenia	**Źródło zagrożenia**	Państwo narodowe dysponujące znacznymi zasobami, które może chcieć ukraść własność intelektualną podmiotu.	
	Podatność	Dostawca rozważa partnerstwo z firmą, która ma związek ze źródłem zagrożenia.	
	Opis zdarzenia powodującego zagrożenie	Państwo narodowe pomaga spółce KXY spełnić wymagania dotyczące zgodności z przepisami branżowymi. Spółka ABC współpracuje z KXY w zakresie rozwoju układów scalonych.	
	Istniejące działania	Wymagania w umowach dotyczące funkcjonalności systemu i elementów. Kompleksowy system śledzenia zapasów w Spółce ABC. Wymagania dotyczące zgodności z normami branżowymi.	
	Rezultat zdarzenia powodującego zagrożenie	Państwo narodowe uzyskuje technologię, modyfikuje technologię lub wykorzystuje wcześniej nieznaną podatność.	
Jednostki podmiotu, procesy, informacje, aktywa lub interesariusze, których dotyczy zdarzenie		Dostawca spółki KXY Integrator spółki ABC przeprowadzający testy funkcjonalne Użytkownicy technologii Inne agencje federalne / klienci	
Ryzyko	**Wpływ**	Modyfikacja technologii / wykorzystanie luk w zabezpieczeniach - wysoki.	Sprzedaż technologii zainteresowanym podmiotom – Umiarkowany
	Prawdopodobieństwo	Umiarkowany	Umiarkowany
	Narażenie na ryzyko (Wpływ ryzyka x Prawdopodobieństwo)	Wysokie	

	Dopuszczalny poziom ryzyka	Umiarkowany		
Ograniczanie ryzyka	**Potencjalne strategie ograniczające ryzyko oraz środki bezpieczeństwa związane z obszarem C-SCRM**	(1) Poprawa identyfikowalności i możliwości monitorowania	(2) Zwiększenie wymagań dotyczących pochodzenia oraz zabezpieczeń informacji	(3) Wybór innego dostawcy
	Szacunkowy koszt strategii ograniczających ryzyko	wzrost o 20%	wzrost o 20%	wzrost o 40%
	Zmiana prawdopodobieństwa	Umiarkowane → Niskie		
	Zmiana wpływu	Wysoki → Umiarkowany		
	Wybrane strategie	Opracowanie i wymaganie wyjątkowych, trudnych do skopiowania etykiet lub zmiana etykiety, aby zniechęcić do klonowania lub modyfikacji komponentu [C-SCRM_PE-3]. Minimalizacja ilości informacji udostępnianych dostawcom. Wymagania w zakresie zabezpieczenia informacji [C-SCRM AC-21]. Wymagania dotyczące pochodzenia oraz aktualizacji informacji na temat pochodzenia w całym cyklu życia systemu [C-SCRM_SR-4].		
	Szacowane ryzyko szczątkowe	Umiarkowane - ryzyko szczątkowe zostało określone jako równoważne z istniejącym ryzykiem, jeśli partnerstwo nie zostanie zawarte.		

Tłumaczenie

SCENARIUSZ 4: DODANIE ZŁOŚLIWEGO KODU

Informacje ogólne

Spółka ABC postanowiła przeprowadzić analizę scenariusza zagrożeń dotyczących systemu sterowania ruchem. Scenariusz ma skupiać się na podatnościach dotyczących oprogramowania i powinien zawierać ogólne zalecenia dotyczące działań ograniczających ryzyko.

Środowisko

System działa niemal automatycznie i wykorzystuje komputery, na których działa ogólnodostępny system operacyjny, a także scentralizowane serwery. Oprogramowanie zostało stworzone przez podmiot, jest regularnie utrzymywane i aktualizowane przez integratora na podstawie umowy zawartej na kolejne pięć lat. Integrator to duża spółka, regularnie współpracująca ze spółką ABC przy różnych projektach, dysponująca znaczącymi zasobami – to pozwala na realizację wymagań dotyczących dostępności i integralności systemu.

Zagrożeniem dla systemu może być utrata zasilania, utrata funkcjonalności lub utrata integralności powodująca przetwarzanie nieprawidłowych poleceń. Niektóre źródła zagrożeń mogą obejmować naturę, złośliwe podmioty oraz złośliwych pracowników. System jest wyposażony w pewne środki bezpieczeństwa, takie jak generator zapasowy, nadmiarowe rozwiązania w projekcie oraz plany awaryjne na wypadek awarii systemu.

Zdarzenie powodujące zagrożenie

Spółka ABC zdecydowała, że najbardziej groźne zdarzenie związane z zagrożeniem będzie wynikiem naruszenia integralności systemu przez złośliwego pracownika. Możliwe ataki mogą polegać na tym, że atakujący wprowadzi do systemu robaka lub wirusa, ograniczając jego zdolność do funkcjonowania, lub też będzie mógł ręcznie kontrolować system z jednego z centralnych serwerów, na przykład wprowadzając tylne drzwi w serwerze, do których będzie miał dostęp zdalny. W zależności od zaawansowania ataku, taka osoba może przejąć kontrolę nad systemem, wyłączyć pewne zabezpieczenia przed awarią i spowodować znaczne szkody.

Na podstawie tych informacji Spółka ABC przygotowała szereg następujących fikcyjnych zagrożeń w celu przeprowadzenia analiz:

> John Poindexter, niezadowolony pracownik integratora, postanawia wprowadzić do jednego z komponentów systemu pewne złośliwe oprogramowanie otwartoźródłowe. Następnie rezygnuje z pracy nie pozostawiając po sobie żadnych śladów. Złośliwe oprogramowanie ma możliwość komunikacji z Johnem i zapewnia mu dostęp do opcji wyłączenia lub zezwolenia na ruch sieciowy w dowolnej spośród 50 stacji transportowych. Rezultatem takiego działania będą trudne do zdiagnozowania zakłócenia, powodujące znaczne straty pieniężne i zagrożenia dla bezpieczeństwa.

Po przeprowadzeniu oceny ryzyka na podstawie dokumentu [NSC 800-30,] kierownictwo zdecydowało, że akceptowalny poziom ryzyka dla tego scenariusza można opisać jako Umiarkowany.

Analiza scenariusza zagrożeń

Gdyby plan Johna zakończył się powodzeniem, potencjalny przebieg wydarzeń mógłby wyglądać następująco:

> John przeprowadza próbę, wyłączając na krótki czas usługi jednej stacji. Takie zdarzenie zostałoby uznane jako przypadkowe i miałoby minimalny wpływ. Następnie John powoduje coraz częstsze zakłócenia na różnych stacjach. Skutkiem byłoby niezadowolenie pracowników i klientów, a także pewne obawy o bezpieczeństwo. Integrator zostałby poinformowany o problemie i zacząłby badać jego przyczynę. W rezultacie powstałoby rozwiązanie tymczasowe, a pracownicy stwierdziliby, że przyczyną problemu jest błąd w systemie. Ze względu na dobre ukrycie złośliwego kodu, integrator nie będzie w stanie go wykryć. W tym momencie John spowodowałby poważne zakłócenia w kilku systemach transportowych jednocześnie. Rozwiązanie opracowane przez integratora zawiodłoby ze względu na rozmiar ataku, a wszystkie usługi transportowe zostałyby wstrzymane. Podróżni dotkliwie odczuliby skutki awarii, a media zaczęłyby informować o problemie. Metoda ataku zostałaby wykryta,

a system zmodyfikowany tak, aby uniemożliwić Johnowi ponowny dostęp. W systemie nadal pozostałby złośliwy kod. Przez kilka miesięcy dochody uległyby znaczącemu zmniejszeniu. Pojawiłyby się także problemy natury prawnej. Spółka musiałaby zainwestować duże środki w przekonanie społeczeństwa, że system jest bezpieczny.

Działania ograniczające ryzyko

Spółka ABC zidentyfikowała następujące potencjalne obszary do poprawy:

- Stworzenie i utrzymanie wykazu elementów, procesów i uczestników łańcucha dostaw [SR-4].
- Kontrola dostępu i zmian w konfiguracji w ramach cyklu życia systemu oraz wymaganie okresowych przeglądów kodu (np. ręcznych recenzji) [AC-1, AC-2, CM-3].
- Wymóg statycznego testowania kodu [RA-9].
- Ustanowienie procedur obsługi incydentów [IR-4].

Tabela C-5: Scenariusz 4

Scenariusz zagrożenia	**Źródło zagrożenia**	Integrator – dodanie złośliwego kodu.
	Podatność	Minimalny nadzór nad działalnością integratora; brak zabezpieczeń i środków kontroli osób dodających niewielkie fragmenty kodu.
	Opis zdarzenia powodującego zagrożenie	Niezadowolony pracownik integratora wprowadza złośliwą funkcjonalność do oprogramowania, a następnie odchodzi ze Spółki ABC.
	Istniejące działania	Integrator – recenzje kodu. Nabywca: Umowa określająca wymagania dotyczące czasu, kosztów i funkcjonalności.
	Rezultat zdarzenia powodującego zagrożenie	50 dużych miast i 500 instancji dotkniętych złośliwym oprogramowaniem. Po aktywacji złośliwe oprogramowanie powoduje poważne zakłócenia komunikacyjne.

Jednostki podmiotu, procesy, informacje, aktywa lub interesariusze, których dotyczy zdarzenie		Podmiot, system sterowania ruchem, integrator, dział prawny. Dział PR.
Ryzyko	**Wpływ**	Wysoki – Zakłócenia w ruchu są poważne i trwają dwa tygodnie, gdy integrator pracuje nad rozwiązaniem problemu. Złośliwy kod nie zostaje wykryty i podatność nadal istnieje w systemie.
	Prawdopodobieństwo	Wysokie
	Narażenie na ryzyko (Wpływ ryzyka x Prawdopodobieństwo)	Wysokie
	Dopuszczalny poziom ryzyka	Umiarkowany
Ograniczanie ryzyka	**Potencjalne strategie ograniczające ryzyko oraz środki bezpieczeństwa związane z obszarem C-SCRM**	C-SCRM_AC-1; C-SCRM_AC-2; C-SCRM_CM-3; C-SCRM_IR-2; C-SCRM_SA-10; C-SCRM_SA-11
	Szacunkowy koszt strategii ograniczających ryzyko	2,5 miliona dolarów
	Zmiana prawdopodobieństwa	Wysokie → Niskie
	Zmiana wpływu	Wysoki (bez zmian)
	Wybrane strategie	Kombinacja strategii ograniczania ryzyka.
	Szacowane ryzyko szczątkowe	Umiarkowane

SCENARIUSZ 5: NIEZAMIERZONA KOMPROMITACJA

Informacje ogólne

Nieświadomi pracownicy wymieniają komponenty na bardziej ekonomiczne rozwiązania, nie rozumiejąc ich wpływu na wydajność, bezpieczeństwo i długoterminowe koszty.

Spółka ABC ma wątpliwości dotyczące swoich zasad nabywania, dlatego postanowiła przeprowadzić analizę scenariusza zagrożeń w celu zidentyfikowania działań ograniczających ryzyko. Wybrane działania muszą mieć zastosowanie do różnych projektów i przełożyć się na znaczące sukcesy w ciągu roku.

Środowisko

Spółka ABC nabywa wiele różnych systemów objęte zróżnicowanymi wymaganiami. Ze względu na złożoność środowiska dyrektorzy Spółki ABC decydują, że powinni wykorzystać scenariusz oparty na rzeczywistym zdarzeniu z przeszłości.

Zdarzenie powodujące zagrożenie

Wykorzystując rzeczywiste zdarzenie jako podstawę, spółka tworzy następujący opis zdarzenia zagrożenia:

> Gill, nowo zatrudniony menadżer programu, ma za zadanie zredukować koszty zakupu systemu o wartości 5 milionów dolarów, kupowanego w celu wspierania złożonych zadań badawczych w unikalnym środowisku fizycznym. System ma być odpowiedzialny za przekazywanie informacji dotyczących temperatury, wilgotności, toksycznych substancji chemicznych, a także za magazynowanie i analizowanie różnych zestawów danych. System nie może doświadczać żadnych nieplanowanych przerw w pracy dłuższych niż 10 sekund, w przeciwnym razie wystąpią poważne zagrożenia bezpieczeństwa, a także zagrożenie dla całego projektu badawczego. Komitet oceny zagrożeń Spółki ABC określił akceptowalny poziom ryzyka dla takiego zdarzenia na poziomie 2/10.
>
> Gill widzi, że wiele komponentów w projekcie systemu ma wysokie ceny w porównaniu z podobnymi komponentami, które nabywał wcześniej na potrzeby podmiotów komercyjnych. Gill prosi Johna, młodszego inżyniera

zatrudnionego przez integratora, o zastąpienie kilku load balancerów i routerów w projekcie systemu, aby obniżyć łączny koszt.

Analiza scenariusza zagrożeń

Spółka ABC decyduje, że istnieją trzy potencjalne rezultaty:

1. Stwierdzenie, że modyfikacje są nieodpowiednie przed zakupem jakichkolwiek produktów (30% szans, brak wpływu).
2. Stwierdzenie, że modyfikacje są nieodpowiednie w czasie przeprowadzanych testów (40% szans, brak wpływu).
3. Brak wykrycia nieodpowiednich modyfikacji, instalacja routerów w systemie, awarie oraz zdarzenia typu DoS (30% szans, duży wpływ).

Strategie ograniczania ryzyka

Określono trzy potencjalne strategie ograniczania ryzyka:

- Udoskonalenie istniejącego programu szkoleń [patrz AT-1], a także dodanie środków bezpieczeństwa w zakresie zarządzania konfiguracją w celu monitorowania wszystkich proponowanych zmian w systemach krytycznych [patrz CM-1];
- Poprawa wymagań dotyczących testowania [patrz SA-11]; oraz
- Wymaganie redundancji i różnorodności w projektach systemów [patrz SC-29, SC-36].

Wprowadzenie środków bezpieczeństwa dotyczących zarządzania konfiguracją zwiększyłoby prawdopodobieństwo odrzucenia zmian na etapie początkowym lub podczas testów, ale ustalono, że inwestycja o wartości 200 000 dolarów w same szkolenia nie będzie w stanie sprowadzić ryzyka do akceptowalnego poziomu w wymaganym czasie.

Poprawa wymagań dotyczących testowania zwiększyłaby prawdopodobieństwo odrzucenia modyfikacji podczas testów, ale ustalono, że żadna ilość samych testów nie będzie w stanie sprowadzić ryzyko do akceptowalnego poziomu.

Wymaganie redundancji i różnorodności w projekcie systemu znacznie zmniejszyłoby wpływ tego i innych zdarzeń, ale mogłoby podwoić koszty projektu. W ramach scenariusza ustalono, że aby sprowadzić ryzyko do akceptowalnego poziomu, należałoby zainwestować 2 miliony dolarów.

W wyniku tej analizy Spółka ABC decyduje się na wdrożenie połączenia szeregu praktyk:

- Obowiązkowy jednodniowy program szkoleniowy dla osób zajmujących się nabywaniem systemów krytycznych oraz dodanie zabezpieczeń w zakresie zarządzania konfiguracją, w wyniku których zmiany muszą być zatwierdzane przez radę zarządzania konfiguracją (koszt początkowej inwestycji – 80 000 dolarów).
- Inwestycje w sprzęt oraz oprogramowanie do testowania krytycznych systemów i komponentów o wartości 60 000 dolarów.
- Redundancja i różnorodność wymagań projektowych, odpowiednio dla każdego projektu.

Ustalono, że takie połączenie działań będzie najbardziej efektywne kosztowo dla różnorodnych projektów i pomoże ograniczyć ryzyko związane z różnymi zagrożeniami.

Tabela C-6: Scenariusz 5

Scenariusz zagrożenia	**Źródło zagrożenia**	Pracownik wewnętrzny – niezamierzona kompromitacja
	Podatność	Niedostateczne praktyki szkoleniowe
	Opis zdarzenia powodującego zagrożenie	Nowy kierownik odpowiedzialny za zamówienia z doświadczeniem w zamówieniach dla podmiotów komercyjnych otrzymuje zadanie ograniczenia kosztów sprzętu. Pracownik widzi wysoką cenę szeregu komponentów i współpracuje z inżynierem, aby zmienić zamówienie.

	Istniejące działania	Minimalny program szkoleń, który nie jest uważany za obowiązkowy. Podstawowe wymagania dotyczące testowania elementów systemu.		
	Rezultat zdarzenia powodującego zagrożenie	Zmiana zostaje uznana za nieodpowiednią przed zakupem.	Zmiana zostaje uznana za nieodpowiednią w czasie testów.	Zmiana przechodzi testy, a routery zostają zainstalowane i zaczynają szwankować, co prowadzi do odmowy świadczenia usług.
Jednostki podmiotu, procesy, informacje, aktywa lub interesariusze, których dotyczy zdarzenie.		Brak	Dział zamówień	Dział zamówień, System, Użytkownicy
Ryzyko	**Wpływ**	Brak	Niski	Wysoki
	Prawdopodobieństwo	Umiarkowane: 30%	Wysokie: 40%	Umiarkowane: 30%
	Narażenie na ryzyko (wpływ ryzyka x prawdopodobieństwo)	Brak	Umiarkowany	Umiarkowany
	Dopuszczalny poziom ryzyka	Niski	Umiarkowany	Wysoki

Ograniczanie ryzyka	**Potencjalne strategie ograniczające ryzyko oraz środki bezpieczeństwa związane z obszarem SCRM**	Usprawnienie programu szkoleniowego oraz wymóg zatwierdzania zmian.	Usprawnienie testów związanych z nabywanymi produktami.	Usprawnienie konstrukcji systemu.
	Szacunkowy koszt strategii ograniczających ryzyko	200 000 dolarów	—	2 miliony dolarów
	Zmiana wpływu	Brak - bez zmian	Niski - bez zmian	Wysoki → Niski
	Zmiana prawdopodobieństwa	30% → 10%	40% → 20%	30% → Bez zmian
	Poziom narażenia na nowe ryzyko	Brak	Niski	Umiarkowany
	Wybrane strategie	Wymóg obowiązkowego szkolenia dla osób pracujących z systemami krytycznymi, wymóg zatwierdzania zmian w systemach krytycznych przez komitet ds. zarządzania konfiguracją (koszt = 100 000 dolarów).		
	Ryzyko szczątkowe	Niskie		

SCENARIUSZ 6: PONOWNE WYKORZYSTANIE KOMPONENTÓW Z PODATNOŚCIAMI W SYSTEMACH

Informacje ogólne

W ramach swoich standardowych działań rozwojowych spółka ABC ponownie wykorzystuje wewnętrznie opracowane i otwartoźródłowe komponenty systemowe przy tworzeniu swoich rozwiązań komercyjnych. Niedawne głośne cyberataki wykorzystywały luki występujące w komponentach używanych w systemie, a klienci spółki ABC domagają się większej przejrzystości jako sposobu na zmniejszenie ich własnego ryzyka.

Spółka ABC postanowiła przeprowadzić analizę scenariusza zagrożeń, aby określić, jakie kroki może podjąć, aby poprawić bezpieczeństwo swoich produktów i zaoferować klientom większą pewność, że podejmuje niezbędne kroki, aby chronić ich przed tego typu atakami.

Środowisko

Spółka Firma ABC jest liderem na rynku oprogramowania do planowania i analiz finansowych *(ang. financial planning and analysis – FP&A)*. Jej klienci polegają na wydanym rozwiązaniu do przechowywania, przetwarzania i analizowania wrażliwych informacji finansowych, takich jak ewidencje księgowe.

Zdarzenie powodujące zagrożenie

Apache Struts (powszechnie stosowany komponent oprogramowania) jest używany jako komponent w ramach rozwiązania komercyjnego spółki ABC. Podatność występująca w Apache Struts została załatana w marcu 2021 roku. Motywowane korzyściami finansowymi organizacje cyberprzestępców poszukiwały możliwości wykorzystania tej podatności w rozwiązaniach komercyjnych.

Spółka ABC zapewnia częste aktualizacje usuwające podatności i błędy w swoim oprogramowaniu komercyjnym. W tym przypadku omawiany komponent nie został uwzględniony w ramach tych aktualizacji.

Przedmiotowa luka jest obecna i możliwa do wykorzystania w rozwiązaniu spółki ABC.

Analiza scenariusza zagrożeń

Gdyby napastnikom udało się odkryć lukę w produkcie spółki ABC, potencjalny przebieg zdarzeń mógłby wyglądać następująco:

Dobrze przygotowana grupa cyberprzestępców mogłaby zainstalować złośliwy kod korzystając z oprogramowania klientów spółki ABC. Korzystając z tego kodu, cyberprzestępcy będą w stanie wydobyć i sprzedać wrażliwe, nieujawnione informacje finansowe spółek publicznych, notowanych na giełdach na całym świecie. Po odkryciu ataku, reputacja spółki ABC zostałaby bezpowrotnie zniszczona w związku z negatywnymi informacjami. Klienci spółki ABC mogą podjąć przeciwko niej działania prawne w związku z niezałataniem znanych luk w ich oprogramowaniu.

Strategie ograniczania ryzyka

Spółka ABC zidentyfikowała następujące obszary do poprawy w celu wzmocnienia swoich praktyk bezpiecznego tworzenia oprogramowania i zwiększenia zaufania do swoich produktów:

- Zapewnienie, że deweloperzy będą szkoleni w zakresie bezpiecznych praktyk rozwoju oprogramowania oraz zostaną poinstruowani w zakresie korzystania z narzędzi do zwalczania podatności, tak aby tworzone oprogramowanie było bezpieczne.
- Zapewnienie, że ponownie wykorzystane komponenty systemu – niezależnie od tego, czy zostały opracowane wewnętrznie, czy też stanowią oprogramowanie otwartoźródłowe –są badane i analizowane w ramach standardowego procesu pod kątem znanych podatności (patrz SA-15).
- Inwentaryzacja komponentów systemu, aby wspomóc utrzymanie produktu w całym cyklu życia (patrz CM-8).
- Ciągłe monitorowanie składników systemu pod kątem pojawiających się podatności oraz opracowanie odpowiednich procesów umożliwiających ich szybkie usunięcie po udostępnieniu poprawki. Automatyzacja procesu tam, gdzie jest to możliwe (patrz CA-7, RA-5).

Tabela C-7 – Scenariusz 6

Scenariusz zagrożenia	**Źródło zagrożenia**	Organizacja cyberprzestępców – podatne na ataki komponenty oprogramowania.
	Podatność	Niezrozumienie i brak monitorowania stanu podatności komponentów używanych w oprogramowaniu oraz brak terminowych aktualizacji w celu załatania znanych podatności.
	Opis zdarzenia powodującego zagrożenie	Organizacja cyberprzestępców wykorzystuje znaną lukę w oprogramowaniu do zainstalowania złośliwego kodu w celu uzyskania dostępu do wrażliwych informacji finansowych zawartych w instancjach aplikacji używanych przez klientów spółki ABC.
	Istniejące działania	Spółka ABC wdrożyła kompleksowy i bezpieczny cyklu życia systemu, który koncentruje się na wykrywaniu i usuwaniu podatności w kodzie opracowanym przez jej deweloperów. Spółka ABC często wydaje poprawki usuwające podatności występujące w jej produktach.
	Rezultat zdarzenia powodującego zagrożenie	W wyniku podatności przeszło 10 głównych klientów spółki ABC pada ofiarą cyberprzestępców. Negatywne informacje dotyczące ataku powodują spadek kursu akcji spółki ABC o 5%. Konkurenci firmy ABC wykorzystują atak i promują własne praktyki bezpieczeństwa, aby się wyróżnić i zdobyć udział w rynku. Spółka ABC narażona jest na znaczne koszty prawne z powodu działań podejmowanych przez poszkodowanych klientów. Spółka ABC odnotowała odejście 5% klientów w ciągu roku po ataku.

Jednostki podmiotu, procesy, informacje, aktywa lub interesariusze, których dotyczy zdarzenie		Dział produktów zajmujący się oprogramowaniem FP&A
Ryzyko	**Wpływ**	Wysoki – 350 milionów dolarów łącznych kosztów, znaczące szkody reputacyjne, utrata udziału w rynku, spadek ceny akcji, utrata klientów
	Prawdopodobieństwo	Wysokie – prawdopodobieństwo wystąpienia wynoszące 20% rocznie
	Narażenie na ryzyko (Wpływ ryzyka x Prawdopodobieństwo)	Wysokie: Narażenie na stratę w wysokości 70 milionów dolarów
	Dopuszczalny poziom ryzyka	Umiarkowany – 20 milionów dolarów: Komitet ds. ryzyka spółki ABC stwierdził, że nie chce stracić więcej niż 20 milionów dolarów z powodu pojedynczego zdarzenia związanego z cyberbezpieczeństwem, które może mieć wpływ na produkty klientów.
Ograniczanie ryzyka	**Potencjalne strategie ograniczające ryzyko oraz środki bezpieczeństwa związane z obszarem SCRM**	Zapewnienie, że deweloperzy będą szkoleni w zakresie bezpiecznych praktyk rozwoju oprogramowania oraz zostaną poinstruowani w zakresie korzystania z narzędzi do zwalczania podatności, tak aby tworzone oprogramowanie było bezpieczne. Zapewnienie, że ponownie wykorzystane komponenty systemu – niezależnie od tego, czy zostały opracowane wewnętrznie, czy też stanowią oprogramowanie otwartoźródłowe –są badane i analizowane w ramach

		standardowego procesu pod kątem znanych podatności (patrz SA-15). Inwentaryzacja komponentów systemu, aby wspomóc utrzymanie produktu w całym cyklu życia (patrz CM-8). Ciągłe monitorowanie składników systemu pod kątem pojawiających się podatności oraz opracowanie odpowiednich procesów umożliwiających ich szybkie usunięcie po udostępnieniu poprawki. Automatyzacja procesu tam, gdzie jest to możliwe (patrz CA-7, RA-5).
	Szacunkowy koszt strategii ograniczających ryzyko	Szkolenie dla deweloperów: 500 – 800 000 dolarów. Proces inwentaryzacji komponentów systemu: 1,2 – 1,5 miliona dolarów. Ciągłe monitorowanie podatności komponentów systemu: 800 000 – 1,2 miliona dolarów.
	Zmiana wpływu	Wysoki – 350 milionów dolarów (bez zmian w oparciu o określone środki bezpieczeństwa).
	Zmiana prawdopodobieństwa	Niskie – prawdopodobieństwo wystąpienia wynoszące 5% rocznie.
	Poziom narażenia na nowe ryzyko	Umiarkowane: 17,5 miliona dolarów.

ZAŁĄCZNIK D WZORY DOKUMENTÓW ZWIĄZANYCH Z OBSZAREM C-SCRM[51]

1. Strategia oraz plan wdrożenia C-SCRM

Aby przeciwdziałać zagrożeniom cyberbezpieczeństwa w całym łańcuchu dostaw, podmioty opracowują strategię C-SCRM. Strategia C-SCRM, której towarzyszy plan wdrożenia, jest opracowywana na poziomie podmiotu (poziomie 1), choć jednostki odpowiedzialne za realizację misji oraz różne obszary działalności (poziom 2) mogą dostosowywać strategię C-SCRM do konkretnych potrzeb misji na podstawie ustaleń na poziomie podmiotu. Strategia i plan wdrożenia C-SCRM powinny opierać się na nadrzędnej strategii zarządzania ryzykiem podmiotu i być zgodne z obowiązującymi przepisami, rozporządzeniami wykonawczymi, dyrektywami i regulacjami.

Typowe elementy strategii i planu wdrożenia, zgodnie z poniższym szablonem, obejmują strategiczne podejście do zmniejszenia narażenia podmiotu na ryzyko związane z łańcuchem dostaw poprzez wymogi zarządzania ryzykiem w skali całego podmiotu, odpowiedzialność, tolerancję na ryzyko, role i obowiązki oraz kryteria eskalacji. Należy pamiętać, że strategia i plan wdrożenia mogą być opracowane jako jeden dokument lub rozbite na wiele dokumentów. Niezależnie od tego, rezultaty tych działań powinny być ze sobą ściśle powiązane.

1.1. WZÓR STRATEGII I PLANU WDROŻENIA C-SCRM

1.1.1. CEL

Należy określić wysokopoziomowy cel dokumentu strategicznego i wdrożeniowego, dostosowując go do misji, wizji i wartości podmiotu. Należy opisać, jaką pozycję zajmują strategia i plan wdrożenia w stosunku do innej dokumentacji C-SCRM utrzymywanej na różnych poziomach. Należy zapewnić jasny kierunek dla priorytetów C-SCRM podmiotu i jego ogólnego podejścia do realizacji tych priorytetów.

[51] Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

Przykładowy tekst

Celem niniejszej strategii i dokumentu wdrożeniowego jest zapewnienie planu wdrożenia skutecznych zdolności, praktyk, procesów i narzędzi C-SCRM w podmiocie w celu wsparcia jego wizji, misji i wartości.

Podejście strategiczne jest zorganizowane wokół zestawu celów, które obejmują zakres misji podmiotu i odzwierciedlają etapowe, osiągalne, strategiczne podejście do zapewnienia pomyślnego wdrożenia i skuteczności działań C-SCRM w całym podmiocie.

Niniejszy dokument strategiczno-wdrożeniowy omawia niezbędne funkcje podstawowe, role, obowiązki oraz podejście, jakie podmiot przyjmie w celu wdrożenia możliwości C-SCRM. W miarę opracowywania i uzupełniania misji i polityki biznesowej oraz planów systemowych, będą one włączane jako załączniki do niniejszego dokumentu. Wszystkie trzy poziomy dokumentacji powinny być okresowo poddawane wspólnym przeglądom w celu zapewnienia spójności i konsekwencji.

Niniejsza strategia i plan wdrożenia są celowo ukierunkowane na ustanowienie podstawowych możliwości. Te podstawowe funkcje - takie jak definiowanie polityk, obszarów odpowiedzialności oraz dedykowanych zasobów - zapewnią, że podmiot będzie mógł z czasem rozszerzać i rozwijać swoje możliwości w zakresie C-SCRM. Plan ten uznaje i podkreśla również potrzebę podnoszenia świadomości wśród pracowników oraz zapewnienia odpowiedniego szkolenia w celu zrozumienia obszaru C-SCRM i rozwoju kompetencji niezbędnych do realizacji działań w zakresie C-SCRM.

Ta wstępna strategia i plan wdrożenia uwzględniają również zależności od wysiłków, procesów i decyzji koordynacyjnych w całej branży. W miarę wyjaśniania i przekazywania rządowych i ogólnobranżowych kierunków, wytycznych dotyczących procesów i wymogów, podmiot będzie aktualizować i udoskonalać swoją strategię oraz plany i działania wdrożeniowe.

1.1.2. ZGODNOŚĆ Z PRZEPISAMI

Należy wymienić ustawy, zarządzenia, dyrektywy, rozporządzenia, polityki, standardy i wytyczne, które regulują strategię i wdrażanie C-SCRM.

1.1.3. CELE STRATEGICZNE

Cele strategiczne stanowią podstawę do określenia zabezpieczeń i wymagań C-SCRM na poziomie podmiotu. Każdy z celów wspiera osiągnięcie określonego celu podmiotu w zakresie realizacji niezawodnych działań w zakresie C-SCRM oraz rezultatów zmniejszających ryzyko. Łącznie cele zapewniają organizacji podstawowe elementy potrzebne do wprowadzenia w życie możliwości C-SCRM i skutecznego realizowania celu podmiotu.

Cele strategiczne powinny dotyczyć istotnych zdolności i czynników umożliwiających realizację działań w zakresie C-SCRM, takich jak:

- Wdrożenie hierarchii zarządzania ryzykiem i podejścia do zarządzania ryzykiem.
- Ustanowienie struktury zarządzania podmiotem, która integruje wymagania C-SCRM i włącza te wymagania do jego zasad i polityk.
- Określanie podejścia do oceny ryzyka dostawcy.
- Wdrożenie programu jakości i niezawodności, który obejmuje proces i praktyki zapewniania jakości i kontroli jakości.
- Ustanowienie wyraźnych, opartych na współpracy ról, struktur i procesów dla funkcji związanych z łańcuchem dostaw, cyberbezpieczeństwem, bezpieczeństwem produktów i bezpieczeństwem fizycznym oraz innych istotnych funkcji.
- Zapewnienie, że odpowiednie zasoby zostały wyznaczone i są wykorzystywane w związku z obszarami bezpieczeństwa informacji i C-SCRM, aby zapewnić właściwe wdrożenie polityk, wytycznych i zabezpieczeń.
- Wdrożenie skutecznego programu zarządzania incydentami w celu zapewnienia sprawnego identyfikowania incydentów bezpieczeństwa, reagowania na ich wystąpienie oraz ograniczania ich skutków.
- Uwzględnienie kluczowych dostawców w planowaniu awaryjnym, reagowaniu na incydenty oraz planowaniu odtworzenia po katastrofie i testach.

Przykładowy tekst

Cel 1: Skuteczne zarządzanie ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw

Cel ten odnosi się do podstawowego zamierzenia podmiotu, jakim jest dążenie do wdrożenia działań w zakresie C-SCRM. Ustanowienie i utrzymanie programu C-SCRM umożliwi jednostkom odpowiedzialnym za ryzyko w podmiocie określenie, ocenę i ograniczenie ryzyka związanego z łańcuchem dostaw dla aktywów podmiotu, jego funkcji i powiązanych usług. Wdrażanie początkowych działań, które będą utrzymywane i rozwijane pod kątem skupienia na określonych obszarach, a także zakresu oraz głębokości, będzie realizowane etapami i będzie obejmować w holistyczny sposób potrzeby pracowników, procesów i technologii, aby zapewnić, że podmiot jest w stanie osiągnąć pożądane cele C-SCRM w obszarach takich jak poprawa świadomości, ochrony i odporności.

Cel 2: Bycie zaufanym źródłem zaopatrzenia dla klientów

Przeciwdziałanie ryzyku związanemu z łańcuchem dostaw zróżnicowanych produktów podmiotu wymaga podejścia opartego na ustalaniu priorytetów, struktury, ulepszonych procesów i stałego zarządzania. Praktyki i środki bezpieczeństwa związane z obszarem C-SCRM muszą być dostosowane do odrębnych i zróżnicowanych zagrożeń i podatności łańcucha dostaw, które mają zastosowanie do klientów podmiotu. Cel ten może być osiągnięty poprzez:

- Wzmocnienie procesów weryfikacji, wymogów C-SCRM i nadzoru nad dostawcami zewnętrznymi oraz
- Zapewnienie, że potrzeby klientów są zaspokajane zgodnie z ich apetytem na ryzyko związane z cyberbezpieczeństwem, tolerancją i środowiskiem.

Cel 3: Pozycjonowanie podmiotu jako lidera branży w zakresie C-SCRM

Podmiot jest dobrze przygotowany do tego, by wprowadzać i rozwijać usprawnienia dotyczące sposobu zarządzania ryzykiem związanym

z cyberbezpieczeństwem w łańcuchach dostaw. W związku z tym podmiot musi wykorzystać tę pozycję do wspierania komunikacji, zachęcania i edukowania podmiotów z branży na temat wymagań i oczekiwań w zakresie rozwiązywania problemów związanych z ryzykiem w łańcuchu dostaw.

1.1.4. PLAN WDROŻENIA I ŚLEDZENIE POSTĘPÓW

Należy określić metodologie i etapy, według których będzie śledzony postęp realizacji celów strategicznych C-SCRM podmiotu. Chociaż kontekst podmiotu wpływa na ten proces w dużym stopniu, podmioty powinny określić horyzonty czasowe w celu priorytetyzacji zadań o charakterze krytycznym lub fundamentalnym. Niezależnie od wyznaczonego horyzontu czasowego, wdrożenie praktycznych, priorytetowych planów jest niezbędne do rozpoczęcia tworzenia lub wzmacniania zdolności C-SCRM.

Gdy zostaną określone poziomy bazowe planu wdrożenia, należy uwzględnić proces eskalacji oraz mechanizm informacji zwrotnej w celu wprowadzania zmian w planie wdrożenia i śledzenia postępów.

Przykładowy tekst

Realizacja celów strategicznych C-SCRM [podmiotu] oraz osiągnięcie skuteczności operacyjnej działań leżących u ich podstaw wymagają formalnego podejścia i zaangażowania w śledzenie postępów. [Podmiot] będzie śledzić i oceniać realizację swoich celów strategicznych poprzez określenie pomocniczych etapów oraz dat ich osiągnięcia w planie wdrożenia. Monitorowanie i sprawozdawczość w zakresie elementów planu wdrożenia wymagają podziału obowiązków w wielu obszarach podejścia opartego na współpracy między zespołami w całym podmiocie.

Poniższy plan wdrożenia będzie utrzymywany przez osoby odpowiedzialne za misję oraz procesy biznesowe, a także poddawany przeglądom przez zespół kierownictwa wyższego szczebla w ramach regularnych działań nadzorczych. Ryzyka i kwestie, które mają wpływ na plan wdrożenia, powinny być proaktywnie zgłaszane do zespołu kierownictwa wyższego szczebla przez osoby odpowiedzialne za misję i procesy biznesowe lub ich zespoły. Plan wdrożenia może być następnie zmieniony zgodnie za zgodą kierownictwa wyższego szczebla.

Tabela D-1: Cel 1 - Główne etapy wdrażania w celu skutecznego zarządzania ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw

Etap planu wdrożenia	Status	Osoba odpowiedzialna	Priorytet	Data realizacji
Opracowanie polityki oraz obszarów odpowiedzialności	Zaplanowane	J. Kowalski	Natychmiast	XX/XX/XX
Ustanowienie i zapewnienie nadzoru wykonawczego i kierownictwa	Wykonane	...	W następnej kolejności	...
Włączenie działań związanych z obszarem C-SCRM do ram zarządzania ryzykiem w podmiocie	Opóźnione	...	Do wykonania później	...
Utworzenie biura zarządzania programem C-SCRM	Anulowane	...	...	...
Ustalenie ról i obowiązków oraz przypisanie odpowiedzialności	...	...	...	...
Opracowanie planów w zakresie C-SCRM.	...	...	...	...
Ustanowienie jednostki odpowiedzialnej za zwiększanie świadomości wewnętrznej	...	...	...	...

Etap planu wdrożenia	Status	Osoba odpowiedzialna	Priorytet	Data realizacji
Określenie, ustalenie priorytetów i wdrożenie możliwości oceny ryzyka związanego z łańcuchem dostaw	...	...	...	...
Ustanowienie, udokumentowanie i wdrożenie środków bezpieczeństwa związanych z obszarem C-SCRM na poziomie podmiotu	...	...	...	...
Określenie wymagań dotyczących zasobów na potrzeby działań w zakresie C-SCRM i zapewnienie trwałego finansowania	...	...	...	...
Opracowanie działań związanych z monitorowaniem osiągnięć programu C-SCRM	...	...	...	...

Tabela D-2: Cel 2 - Etapy realizacji w zakresie pełnienia roli zaufanego źródła dostaw dla klientów

Etap planu wdrożenia	Status	Osoba odpowiedzialna	Priorytet	Data realizacji
Włączenie działań C-SCRM do linii biznesowych ukierunkowanych na klienta, programów oraz oferty rozwiązań	Zaplanowane	J. Kowalski	Natychmiast	XX/XX/XX
Zapewnienie, że pracownicy wsparcia klienta są świadomi wymagań dotyczących zarządzania i zagrożeń związanych z cyberbezpieczeństwem w całym łańcuchu dostaw	Wykonane	...	W następnej kolejności	...
Ustanowienie minimalnych poziomów bazowych gwarancji dotyczących cyberbezpieczeństwa w łańcuchu dostaw	Opóźnione	...	Do wykonania później	...
Ustanowienie procesów reagowania na zidentyfikowane ryzyka oraz monitorowania wpływu na łańcuch dostaw podmiotu	Anulowane	...	...	...

Tabela D-3: Cel 3 - Etapy realizacji pozycjonowania podmiotu jako lidera branży w zakresie C-SCRM

Etap planu wdrożenia	Status	Osoba odpowiedzialna	Priorytet	Data realizacji
Koordynacja i współpraca z organami bezpieczeństwa państwa i organami ścigania w celu zapewnienia szybkiego dostępu do krytycznych zagrożeń łańcucha dostaw	Zaplanowane	J. Kowalski	Natychmiast	XX/XX/XX
Ocena możliwości usprawnienia działań związanych z obszarem C-SCRM oraz wzmocnienie wymogów i nadzoru nad wspólnymi rozwiązaniami i usługami	Wykonane	...	W następnej kolejności	...
Wspieranie świadomości i kompetencji dotyczących obszaru C-SCRM poprzez szkolenia i rozwój pracowników, w tym szkolenia z bezpiecznego kodowania dla deweloperów	Opóźnione	...	Do wykonania później	...
Wydanie białych ksiąg i publicznych wytycznych związanych z obszarem C-SCRM	Anulowane	...		...

1.1.5. ROLE I OBOWIĄZKI

Należy wyznaczyć osoby odpowiedzialne za wzory strategii oraz planu wdrożenia, a także kluczowych współpracowników. Należy podać rolę i nazwisko każdej osoby lub grupy, a także w razie potrzeby informacje kontaktowe (np. przynależność, adres, adres e-mail, numer telefonu).

Przykładowy tekst

- Wyższe kierownictwo powinno:
  - ✓ Zatwierdzić cele strategiczne podmiotu w zakresie C-SCRM i plan wdrożenia.
  - ✓ Zapewnić nadzór nad wdrożeniem i skutecznością działań w zakresie C-SCRM.
  - ✓ Przekazywać wytyczne dotyczące działań w zakresie C-SCRM i decyzje dotyczące priorytetów i potrzeb kadrowych.
  - ✓ Określić apetyt podmiotu na ryzyko oraz poziom tolerancji ryzyka.
  - ✓ Reagować niezwłocznie na eskalację problemów i zagadnień związanych z wysokim poziomem ryzyka dotyczącego obszaru C-SCRM, które mogłyby wpłynąć na postawę ryzyka podmiotu.
- Osoby odpowiedzialne za misję oraz procesy biznesowe powinny:
  - ✓ Określić apetyt na ryzyko oraz poziom tolerancji ryzyka na poziomie misji, zapewniając, że są one zgodne z oczekiwaniami podmiotu.
  - ✓ Określić wymagania dotyczące zarządzania ryzykiem w łańcuchu dostaw oraz wdrożyć środki bezpieczeństwa wspierające cele podmiotu.
  - ✓ Wykonywać analizy krytyczności funkcji i zasobów związanych z misją.
  - ✓ Przeprowadzać oceny ryzyka dla zamówień związanych z misją i działalnością.

1.1.6. DEFINICJE

Należy podać kluczowe definicje terminów wykorzystanych w szablonie strategii i wdrożenia, a w razie potrzeby podać przykłady charakterystyczne dla danego podmiotu.

Przykładowy tekst

- Podmiot: Organizacja o określonej misji, celu i granicach, która wykorzystuje systemy informacyjne do realizacji rzeczonej misji i jest odpowiedzialna za

zarządzanie własnym ryzykiem i rezultatami. Podmiot może obejmować każde z wymienionych lub wyłącznie niektóre z wymienionych obszarów – zamówienia, zarządzanie programami, zarządzanie finansowe (np. budżet), kadry, bezpieczeństwo oraz systemy informacyjne, zarządzanie informacjami i misją.

- Cel: Określenie celów podmiotu oraz docelowego rezultatu działań.

1.1.7. PRZEGLĄD I UTRZYMANIE

Należy określić wymaganą częstotliwość przeglądów szablonów strategii oraz planu wdrożenia. Utrzymanie tabeli przeglądów pozwoli na wykorzystanie mechanizmu kontroli wersji. Szablony strategii i planu wdrożenia są żywymi dokumentami, które muszą być aktualizowane i przekazywane wszystkim odpowiednim osobom, w tym pracownikom, wykonawcom i dostawcom.

Przykładowy tekst

Szablony strategii i planu wdrożenia [podmiotu] muszą być weryfikowane co najmniej raz na trzy do pięciu lat ze względu na zmiany w prawie, polityce, normach, wytycznych i środkach bezpieczeństwa. Dodatkowe kryteria, które mogą spowodować wprowadzenie zmian pomiędzy przeglądami, obejmują:

- Zmianę polityk, które mają wpływ na szablon strategii i planu wdrożenia.
- Istotne wydarzenia związane ze strategią i wdrożeniem.
- Wprowadzenie nowych technologii.
- Odkrycie nowych podatności.
- Zmiany operacyjne lub środowiskowe.
- Braki w szablonach strategii i planu wdrożenia.
- Zmianę zakresu.
- Inne kryteria specyficzne dla podmiotu.

Tabela D-4: Tabela kontroli wersji

Numer wersji	Data	Opis zmiany/wersji	Rozdziały/Strony, których dotyczą zmiany	Zmiany dokonane przez nazwisko/stanowisko/podmiot

2. POLITYKA C-SCRM

Polityka C-SCRM kieruje realizacją strategii C-SCRM. Polityka C-SCRM może być opracowana na poziomie 1 bądź na poziomie 2 i jest oparta na czynnikach specyficznych dla misji i podmiotu, w tym na kontekście ryzyka, decyzjach dotyczących ryzyka oraz działaniach związanych z ryzykiem w ramach strategii C-SCRM. Polityki C-SCRM wspierają odpowiednie polityki podmiotu (np. politykę zamówień i zapatrzenia, politykę bezpieczeństwa i prywatności informacji, politykę logistyki, politykę łańcucha dostaw). Polityki C-SCRM odnoszą się do celów i zadań nakreślonych w strategii C-SCRM podmiotu, która z kolei opiera się na planie strategicznym podmiotu. Polityka C-SCRM powinna również uwzględniać misję i obszary biznesowe, a także wymagania klientów wewnętrznych i zewnętrznych. Polityki C-SCRM określają również punkty integracji C-SCRM z procesami zarządzania ryzykiem w podmiocie. Dodatkowo, polityka C-SCRM powinna określać role i obowiązki związane z obszarem C-SCRM w zakresie przeprowadzania Ocena zabezpieczeń i autoryzacji, wszelkie zależności pomiędzy tymi rolami oraz interakcje pomiędzy nimi. Polityki C-SCRM na poziomie 1 są bardziej rozległe, z kolei polityki C-SCRM na poziomie 2 są specyficzne dla misji i funkcji biznesowej. Role dotyczące obszaru C-SCRM określają odpowiedzialność za zamówienia, przeprowadzanie ocen ryzyka, gromadzenie informacji o zagrożeniach w łańcuchu dostaw, identyfikację i wdrażanie środków ograniczających ryzyko, a także monitorowanie oraz inne funkcje C-SCRM.

2.1. WZÓR POLITYKI C-SCRM

2.1.1. ZGODNOŚĆ Z PRZEPISAMI

Należy wymienić ustawy, zarządzenia, dyrektywy, rozporządzenia, polityki, standardy i wytyczne, które regulują politykę C-SCRM.

Przykładowy tekst dla poziomu 1

- Polityki
  - ✓ [Polityka zarządzania ryzykiem [podmiotu]
  - ✓ Polityka bezpieczeństwa informacji [podmiotu]
- Przepisy
- Rozporządzenia

Przykładowy tekst dla poziomu 2

- Polityki
  - ✓ Polityka C-SCRM [podmiotu]
  - ✓ Polityka bezpieczeństwa informacji [misji i procesu biznesowego]
- Rozporządzenia
- Wytyczne

2.1.2. OPIS

Należy opisać cel i zakres polityki C-SCRM, nakreślić intencje kierownictwa podmiotu w zakresie realizacji planu, egzekwowania uwzględnionych środków bezpieczeństwa i zapewnienia jego aktualności. Należy określić poziomy, do których polityka ma zastosowanie. Może zaistnieć potrzeba utworzenia polityki C-SCRM w całości lub w części na podstawie istniejących polityk lub innych wytycznych.

Na poziomie 2, polityki C-SCRM powinny zawierać wykaz wszystkich polityk i planów poziomu 1, które stanowią podstawę polityk poziomu 2, zawierać krótkie wyjaśnienie obszaru misji oraz działalności, a także skrócony opis zakresu zastosowania (np. planów, systemów, rodzajów zamówień itp.) polityk C-SCRM poziomu 2.

Przykładowy tekst dla poziomu 1

[Podmiot] dostrzega ryzyko związane z produktami, usługami oraz nabywanymi, używanymi i oferowanymi klientom rozwiązaniami.

Celem polityki programu C-SCRM [podmiotu] jest skuteczne wdrożenie i utrzymanie zdolności do zapewnienia zwiększonej pewności, że produkty, usługi i rozwiązania wykorzystywane i oferowane przez [podmiot] są godne zaufania, odpowiednio zabezpieczone i odporne oraz zdolne do działania zgodnie z wymaganymi normami jakości.

C-SCRM to systematyczny proces identyfikacji i oceny podatności, wrażliwości i zagrożeń w całym łańcuchu dostaw oraz wdrażania strategii i środków bezpieczeństwa w celu zmniejszenia ekspozycji na ryzyko i zwalczania zagrożeń. Ustanowienie i utrzymanie programu C-SCRM w całym podmiocie umożliwi jednostkom odpowiedzialnym za ryzyko określenie, ocenę i ograniczenie ryzyka związanego z łańcuchem dostaw dla aktywów podmiotu, jego funkcji i powiązanych usług.

Przykładowy tekst dla poziomu 2

Osoby odpowiedzialne za [misję i proces biznesowy] są świadome jego krytyczności dla realizacji [celów podmiotu]. Jednym z kluczowych elementów produkcji jest koordynacja i współpraca z dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych oraz innymi dostawcami usług związanych z ICT/OT. Osoby odpowiedzialne uznają, że realizacja ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw może zakłócić lub całkowicie zahamować zdolność [misji i procesu biznesowego] do wytwarzania produktów w wymaganym czasie i zgodnie z wymaganym standardem jakości.

W oparciu o cele C-SCRM określone w [polityce poziomu 1 podmiotu], celem polityki [misji i procesu biznesowego] jest wdrożenie działań dotyczących obszaru C-SCRM, które umożliwią ocenę ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw, a także jego monitorowanie i reagowanie na jego przejawy. Działania w zakresie C-SCRM, które są zgodne z polityką i wymaganiami określonymi przez program C-SCRM podmiotu, zapewnią granice, w ramach których [misja i proces biznesowy] dostosuje procesy i praktyki C-SCRM do wyjątkowych wymogów związanych z pozyskiwaniem komponentów i wytwarzaniem kluczowych produktów.

2.1.3. POLITYKA

Należy określić obowiązkowe wysokopoziomowe stwierdzenia, na których opiera się polityka, które stanowią podstawę celów i założeń planu strategicznego C-SCRM podmiotu, misji i funkcji biznesowych oraz wymagań klienta wewnętrznego i zewnętrznego.

Przykładowy tekst dla poziomu 1

Program C-SCRM [podmiotu] jest ustanowiony w celu wdrożenia i utrzymania zdolności do:

- Oceny i zapewnienia odpowiedniej reakcji na ryzyko związane z cyberbezpieczeństwem, które wynika z nabycia i użytkowania produktów objętych ochroną.
- Ustalenia priorytetów oceny ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw oraz działań w zakresie reagowania na ryzyko w oparciu o ocenę krytyczności misji, systemu, komponentu, usługi lub zasobu.
- Opracowania ogólnej strategii C-SCRM i wysokopoziomowego planu wdrożenia, polityki i procesów.
- Włączenia praktyk zarządzania ryzykiem w łańcuchu dostaw w całym cyklu życia nabywania i zarządzania aktywami artykułów objętych programem.
- Udostępniania informacji dotyczących obszaru C-SCRM zgodnie z ogólnobranżowymi kryteriami i wytycznymi.

Realizowania i nadzorowania postępów we wdrażaniu i skuteczności strategiczna C-SCRM powinien:

- Być kierowany i koordynowany przez wyznaczone kierownictwo wyższego szczebla, które funkcjonuje w roli Zarządu Programu C-SCRM podmiotu i przewodniczy biuru zarządzania programem C-SCRM;
- Wykorzystywać oraz być włączony do istniejących procesów i struktur zarządzania ryzykiem i podejmowania decyzji [podmiotu];
- Być oparty na podejściu zespołowym i mieć oparty na współpracy i interdyscyplinarny charakter;

- Uwzględniać podejście do zarządzania ryzykiem w oparciu o poziomy, zgodne z dokumentami, np. NIST Risk Management Framework i NSC 800-161.
- Obejmować skodyfikowane i prawne wymogi w zakresie C-SCRM oraz ogólnobranżowe i specyficzne dla podmiotu kierunki polityki, wytyczne i procesy.

Przykładowy tekst dla poziomu 2

Program C-SCRM [misji i procesu biznesowego] powinien:

- Działać zgodnie z wymogami i wytycznymi określonymi w programie C-SCRM [podmiotu].
- Współpracować z biurem zarządzania programem C-SCRM w celu stosowania praktyk i działań związanych z obszarem C-SCRM potrzebnych do oceny i monitorowania ryzyka związanego z cyberbezpieczeństwem wynikającego z realizacji podstawowych celów [misji i procesu biznesowego].
- Łączyć działania w zakresie C-SCRM z istniejącymi działaniami w celu wsparcia celu [podmiotu], jakim jest zarządzanie ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw.
- Przydzielić zasoby potrzebne do koordynacji działań C-SCRM w ramach [misji i procesu biznesowego].
- Określić krytycznych dostawców [misji i procesu biznesowego] oraz ocenić poziom narażenia na ryzyko, które wynika z tych relacji.
- Wdrożyć działania w zakresie reagowania na ryzyko w celu zmniejszenia narażenia na zagrożenia związane z cyberbezpieczeństwem w całym łańcuchu dostaw.
- Monitorować bieżący poziom narażenia na ryzyko związane z cyberbezpieczeństwem w profilu łańcucha dostaw oraz dostarczać okresowe sprawozdania stosownym interesariuszom odpowiedzialnym za zarządzanie ryzykiem podmiotu i obszar C-SCRM.

2.1.4. ROLE I OBOWIĄZKI

Należy wymienić osoby odpowiedzialne za politykę C-SCRM, a także jej kluczowych współtwórców. Należy podać rolę i nazwisko każdej osoby lub grupy, a także w razie potrzeby informacje kontaktowe (np. przynależność, adres, adres e-mail, numer telefonu).

Przykładowy tekst dla poziomu 1

- Zarządzający Programem C-SCRM jest odpowiedzialny za:
  - ✓ Kierowanie tworzeniem, rozwojem i nadzorem programu C-SCRM w porozumieniu z wyznaczonymi liderami C-SCRM.
  - ✓ Powołanie zespołu i pełnienie funkcji przewodniczącego biura zarządzania programem C-SCRM. Zespół ten będzie składał się z przewodniczącego i wyznaczonych liderów C-SCRM i będzie odpowiedzialny za opracowanie i koordynację strategii C-SCRM, planów wdrożeniowych i działań, które dotyczą kwestii związanych z obszarem C-SCRM; sprawozdawczość oraz nadzór nad programem; a także identyfikację i zalecenia dotyczące zasobów programu.
  - ✓ Eskalowanie bądź zgłaszanie problemów związanych z obszarem C-SCRM do kierownictwa wyższego szczebla, w zależności od potrzeb.
- Każdy kierownik ds. bezpieczeństwa związanego z obszarem C-SCRM jest odpowiedzialny za:
  - ✓ Wyznaczanie liderów C-SCRM (liderzy będą odpowiedzialni za udział w pracach biura zarządzania programem C-SCRM).
  - ✓ Włączenie odpowiednich funkcji C-SCRM do funkcji na poziomie podmiotu i stanowiska.
  - ✓ Wdrożenie i dostosowanie się do wymagań programu C-SCRM.

Przykładowy tekst dla poziomu 2

- Liderzy C-SCRM są odpowiedzialni za:
  - ✓ Reprezentowanie interesów i potrzeb członków biura zarządzania programem C-SCRM.
  - ✓ Prowadzenie bądź koordynowanie rozwoju i realizacji planów C-SCRM programu lub linii biznesowej. Obejmuje to zapewnienie, że takie plany są odpowiednio dostosowane do planu C-SCRM na poziomie podmiotu i są z nim zintegrowane.

- Pracownicy odpowiedzialni za obszar C-SCRM w obszarze misji lub procesu biznesowego są odpowiedzialni za:
  - ✓ Podstawowe wykonanie działań C-SCRM (np. oceny dostawców lub produktów).
  - ✓ Wsparcie dla specyficznych dla misji i działalności C-SCRM działań prowadzonych przez pracowników niezwiązanych z obszarem C-SCRM.

2.1.5. DEFINICJE

Należy wymienić kluczowe definicje opisane w polityce, a w razie potrzeby podać kontekst i przykłady charakterystyczne dla danego podmiotu.

Przykładowy tekst (dotyczy poziomu 1 bądź poziomu 2)

- Artykuły objęte ochroną: Technologie informacyjne, w tym wszelkiego rodzaju usługi przetwarzania w chmurze, sprzęt telekomunikacyjny lub usługi telekomunikacyjne; przetwarzanie informacji w systemie informacyjnym, podlegające wymogom programu w zakresie kontrolowanych informacji jawnych, a także wszystkie technologie IoT/OT (np. sprzęt, systemy, urządzenia, oprogramowanie lub usługi obejmujące wbudowane technologie informacyjne).
- Ocena ryzyka dotyczącego cyberbezpieczeństwa w łańcuchu dostaw: Systematyczne badanie ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw, prawdopodobieństwa jego wystąpienia oraz potencjalnych skutków.
- Osoba odpowiedzialna za ryzyko: Osoba lub jednostka posiadająca odpowiedzialność i uprawnienia do zarządzania ryzykiem.

2.1.6. PRZEGLĄD I UTRZYMANIE

Należy określić wymaganą częstotliwość przeglądów i utrzymania polityki C-SCRM. Utrzymanie tabeli przeglądów pozwoli na wykorzystanie mechanizmu kontroli wersji. Polityki C-SCRM są żywymi dokumentami, które muszą być aktualizowane i przekazywane wszystkim odpowiednim osobom (np. personelowi, wykonawcom i dostawcom).

Przykładowy tekst (dotyczy poziomu 1 i/lub poziomu 2)

Polityka C-SCRM [podmiotu] musi być poddawana przeglądowi co najmniej raz w roku ze względu na dynamiczne zmiany w przepisach, politykach, normach,

wytycznych i środkach bezpieczeństwa. Dodatkowe kryteria, które mogą spowodować wprowadzenie zmian pomiędzy przeglądami, obejmują:

- Zmianę polityk, które mają wpływ na politykę C-SCRM.
- Istotne zdarzenia C-SCRM.
- Wprowadzenie nowych technologii.
- Odkrycie nowych podatności.
- Zmiany operacyjne lub środowiskowe.
- Niedociągnięcia w polityce C-SCRM.
- Zmiany zakresu.
- Inne kryteria specyficzne dla podmiotu.

Tabela D-5: Tabela kontroli wersji

Numer wersji	Data	Opis zmiany/ wersji	Rozdziały/Strony, których dotyczą zmiany	Zmiany dokonane przez nazwisko/stanowisko/podmiot

3. PLAN C-SCRM

Plan C-SCRM jest opracowywany na poziomie 3, dotyczy konkretnego wdrożenia i określa sposób realizacji polityki, wymagania, ograniczenia i założenia. Może być samodzielny lub stanowić element planu bezpieczeństwa i prywatności systemu. W przypadku ich włączenia, elementy C-SCRM muszą być wyraźnie wyróżnione. Plan C-SCRM dotyczy zarządzania, wdrażania i monitorowania zabezpieczeń C-SCRM oraz rozwoju i utrzymania systemów w całym cyklu życia systemu w celu wspierania misji i funkcji biznesowych. Plan C-SCRM dotyczy systemów o wysokim i umiarkowanym stopniu zagrożenia określonym na podstawie dokumentu [NSC 199].

Biorąc pod uwagę, że łańcuchy dostaw mogą się znacznie różnić w zależności od podmiotu, plany C-SCRM powinny być dostosowane do poszczególnych programów, podmiotów i kontekstów operacyjnych. Dostosowane plany C-SCRM stanowią podstawę do

określenia, czy technologia, usługa, komponent systemu lub system są odpowiednie do celu oraz czy środki bezpieczeństwa muszą być odpowiednio dostosowane. Dostosowane plany C-SCRM pomagają podmiotom skoncentrować zasoby na najbardziej krytycznych funkcjach misji i działalności w oparciu o wymagania oraz ich środowisko ryzyka.

Poniższy szablon planu C-SCRM stanowi wyłącznie przykład. Podmioty mogą dowolnie kształtować oraz wdrażać różne podejścia do opracowania i prezentacji planu C-SCRM. Podmioty mogą wykorzystać zautomatyzowane narzędzia, aby zapewnić, że wszystkie istotne sekcje planu C-SCRM zostały uwzględnione. Zautomatyzowane narzędzia mogą pomóc w dokumentowaniu informacji z planu C-SCRM, takich jak inwentaryzacja komponentów, poszczególne role, informacje o wdrożeniu środków bezpieczeństwa, diagramy systemu, krytyczność komponentów łańcucha dostaw oraz współzależności.

3.1. WZÓR PLANU C-SCRM

3.1.1. NAZWA I IDENTYFIKATOR SYSTEMU

Należy określić niepowtarzalny identyfikator bądź nazwę dla systemu. Należy podać wszelkie stosowne nazwy historyczne oraz odpowiednie tytuły dokumentów poziomu 1 i poziomu 2.

Przykładowy tekst

Niniejszy plan C-SCRM zawiera przegląd wymogów bezpieczeństwa dla systemu [nazwa systemu] [niepowtarzalny identyfikator] i opisuje istniejące lub planowane do wdrożenia środki bezpieczeństwa w zakresie cyberbezpieczeństwa łańcucha dostaw w celu zapewnienia stosownych zabezpieczeń C-SCRM odpowiednich dla informacji, które mają być przesyłane, przetwarzane lub przechowywane przez system.

Środki bezpieczeństwa wdrożone w systemie [niepowtarzalny identyfikator] spełniają wymogi określone w strategii C-SCRM podmiotu oraz wytycznych dotyczących polityki.

3.1.2. OPIS SYSTEMU

Należy opisać funkcję, cel i zakres działania systemu oraz zawrzeć opis przetwarzanych informacji. Należy także przedstawić ogólny opis podejścia systemu do zarządzania ryzykiem łańcucha dostaw związanym z badaniami i rozwojem, projektowaniem, produkcją, zakupem, dostawą, integracją, eksploatacją i utrzymaniem oraz utylizacją systemów, komponentów systemu lub usług systemowych.

Należy zapewnić, że plan C-SCRM opisuje system w kontekście tolerancji podmiotu na ryzyko łańcucha dostaw, uwzględniając dopuszczalne strategie ograniczania ryzyka łańcucha dostaw lub środki bezpieczeństwa, proces stałej oceny i monitorowania ryzyka łańcucha dostaw, metody wdrażania i rozpowszechniania planu oraz opis i uzasadnienie podjętych środków ograniczających ryzyko łańcucha dostaw. Opisy muszą być zgodne z misją i funkcjami biznesowymi systemu; granicami autoryzacji systemu; ogólną architekturą systemu, w tym wszelkimi systemami wspierającymi i powiązaniami; sposobem, w jaki system wspiera misje podmiotu; oraz środowiskiem systemu ustanowionymi na poziomach 1 i 2.

Przykładowy tekst

System zarządzania dokumentami (*ang. document management system - DMS*) służy do zapewnienia dynamicznych repozytoriów informacji, hierarchii plików i funkcji współpracy w celu usprawnienia wewnętrznej komunikacji i koordynacji pracy zespołu. Dane obsługiwane w ramach systemu zawierają dane osobowe. System DMS jest rozwiązaniem komercyjnym, które zostało zakupione bezpośrednio od sprawdzonego dostawcy – [nazwa dostawcy], na terenie kraju. System został skonfigurowany do potrzeb podmiotu. Do wdrożenia i utrzymania systemu nie są wykorzystywane żadne biblioteki kodu podmiotów zewnętrznych. Jest on hostowany w warstwie zarządzania głównego dostawcy wirtualnej chmury prywatnej podmiotu.

System DMS jest systemem kategorii 1, który w przypadku przestoju musi mieć zapewniony czas odtworzenia na poziomie 1 godziny. Podmiot utrzymuje środowisko odzyskiwania po awarii – w tym celu korzysta z usług drugiego dostawcy chmury prywatnej, na które podmiot może się przełączyć, jeśli istnieje prawdopodobieństwo, że czas odtworzenia zostanie przekroczony na podstawowej platformie.

3.1.3. TYP I KATEGORYZACJA INFORMACJI O SYSTEMIE

W poniższych tabelach określono rodzaje informacji, które są przetwarzane, przechowywane lub przekazywane przez system i/lub jego transgraniczny łańcuch

dostaw. Podmioty korzystają z dokumentu [NSC 800-60], [NARA CUI] lub innych typów informacji właściwych dla danego podmiotu w celu określenia typów informacji i tymczasowych poziomów wpływu. Korzystając z wytycznych dotyczących kategoryzacji informacji i systemów zawartych w dokumencie [NSC 199], podmiot określa poziomy wpływu na bezpieczeństwo dla każdego typu informacji.

Należy określić poziom wpływu (tj. niski, umiarkowany, wysoki) dla każdego atrybutu bezpieczeństwa (tj. poufności, integralności, dostępności).

Przykładowy tekst

Tabela D-6: Typ i kategoryzacja informacji o systemie

Typ informacji	**Atrybuty bezpieczeństwa (poziomu wpływu)**		
	Poufność (niski, umiarkowany, wysoki)	**Integralność (niski, umiarkowany, wysoki)**	**Dostępność (niski, umiarkowany, wysoki)**

W oparciu o powyższą tabelę należy wskazać górną granicę wpływu na atrybuty bezpieczeństwa w skali niski, umiarkowany, wysoki. Należy także określić ogólną kategoryzację systemu.

Tabela D-7: Kategoryzacja wpływu na bezpieczeństwo

Cel bezpieczeństwa	**Poziom wpływu na bezpieczeństwo**
Poufność	□ niski □ umiarkowany □ wysoki
Integralność	□ niski □ umiarkowany □ wysoki
Dostępność	□ niski □ umiarkowany □ wysoki
Ogólna kategoria bezpieczeństwa systemu	□ niski □ umiarkowany □ wysoki

3.1.4. STATUS OPERACYJNY SYSTEMU

Przykładowy tekst

Tabela D-8: Status operacyjny systemu

Należy wskazać status operacyjny systemu. Jeśli wybrano więcej niż jeden status, należy wymienić, których części systemu dotyczą poszczególne statusy

Status systemu		
□	Operacyjny	System działa i jest wykorzystywany w produkcji.
□	W trakcie rozwoju	System jest projektowany, rozwijany lub wdrażany.
□	Poważne zmiany	System przechodzi poważne zmiany, rozwój lub transformację.
□	Usuwanie	System nie jest sprawny.

3.1.5. DIAGRAMY SYSTEMU/SIECI, INWENTARYZACJA, DZIAŁANIA W CYKLU ŻYCIA

Należy załączyć aktualny i szczegółowy schemat systemu i sieci wraz ze spisem komponentów systemu lub odniesienie do miejsca, w którym można znaleźć schematy i informacje o spisie.

Należy zapewnić kontekst w stosunku do cyklu życia systemu, aby zapewnić, że działania są mapowane i śledzone. Gwarantuje to pełne pokrycie działań C-SCRM, ponieważ operacje te mogą wymagać powtarzania i reintegracji (z wykorzystaniem technik spiralnych lub zwinnych) w całym cyklu życia. Działania w ramach planu C-SCRM są wymagane od koncepcji poprzez etapy rozwoju, produkcji, wykorzystania, wsparcia i wycofania.

Przykładowy tekst

Komponenty [systemu] mogą obejmować:

- opis komponentu,
- numer wersji,
- numer licencji,
- właściciela licencji,

- rodzaj licencji (np. dla pojedynczego użytkownika, licencja publiczna, freeware[52]),
- kod kreskowy/numer,
- nazwę hosta (tj. nazwa używana do identyfikacji komponentu w sieci),
- typ komponentu (np. serwer, router, stacja robocza, przełącznik),
- producenta,
- model,
- numer seryjny,
- numer rewizji komponentu (np. wersja oprogramowania sprzętowego),
- lokalizację fizyczną: (należy podać konkretne umiejscowienie komponentów w szafach serwerowych),
- nazwę sprzedawcy.

3.1.6. WYMIANA INFORMACJI I POŁĄCZENIA SYSTEMOWE

Należy wymienić wszelkie porozumienia dotyczące wymiany informacji (np. porozumienia typu ISA, protokoły ustaleń, protokoły uzgodnień między systemami, datę zawarcia porozumienia, status autoryzacji bezpieczeństwa innych systemów, nazwisko osoby autoryzującej, opis połączenia oraz diagramy pokazujące przepływ każdej wymiany informacji.

Przykładowy tekst

Tabela D-9: Wymiana informacji i połączenia systemowe

Data umowy	Nazwa Systemu	Podmiot	Rodzaj połączenia lub metoda wymiany informacji	Kategoryzacja według NSC 199	Status autoryzacji	Imię i nazwisko oraz tytuł osoby autoryzującej

[52] Freeware – licencja oprogramowania umożliwiająca darmowe rozprowadzanie aplikacji bez ujawnienia kodu źródłowego

3.1.7. SPECYFIKACJA ŚRODKÓW BEZPIECZEŃSTWA

Należy udokumentować środki bezpieczeństwa C-SCRM w celu zapewnienia, że plan uwzględnia wymagania dotyczące opracowania godnych zaufania, bezpiecznych, chroniących prywatność i odpornych komponentów i systemów, w tym stosowania zasad projektowania z myślą o bezpieczeństwie wdrażanych jako część procesów inżynierii bezpieczeństwa systemów opartych na cyklu życia. Należy uwzględnić odpowiednie obszary tematyczne, takie jak oceny, standardowe procedury operacyjne, obowiązki, oprogramowanie, sprzęt, produkty, usługi i zagadnienia związane z obszarem DevSecOps.

Dla każdego środka bezpieczeństwa należy przedstawić dokładny opis sposobu wdrożenia oraz stosowny poziom bazowy. Należy uwzględnić wszelkie istotne artefakty dotyczące wdrożenia środków bezpieczeństwa. Należy uwzględnić wszelkie uzasadnienia dotyczące dostosowania środków bezpieczeństwa, jeśli dotyczy. Należy odwołać się do odpowiednich polityk C-SCRM poziomu 1 bądź poziomu 2, które w stosownych przypadkach zapewniają dziedziczone środki bezpieczeństwa. Warto pamiętać, że w podmiocie może istnieć wiele polityk poziomu 1, ustanowionych przez różne jednostki organizacyjne lub osoby.

Przykładowy tekst

SR-6 OCENY I RECENZJE DOSTAWCÓW

Realizacja: W ramach kompleksowej strategii bezpieczeństwa informacji podmiot ustanowił program C-SCRM, aby wdrożyć działania związane z zarządzaniem ryzykiem dotyczącym cyberbezpieczeństwa w całym łańcuchu dostaw. Biuro zarządzania programem C-SCRM jest odpowiedzialne za przeprowadzanie ocen ryzyka cyberbezpieczeństwa partnerów biznesowych zajmujących się integracją z [systemem] zgodnie z wymogami polityki C-SCRM poziomu 2 w skali całego podmiotu. Materiały szkoleniowe i uświadamiające w zakresie C-SCRM muszą być również zapewnione wszystkim osobom przed uzyskaniem dostępu do [systemu].

Zabezpieczenia rozszerzone: Zastosowanie mają zabezpieczenia rozszerzone nr 2, 7 i 8 opisane w dokumencie [NSC 800-161].

(2) RECENZJE DOSTAWCÓW

Realizacja: Biuro zarządzania programem C-SCRM przeprowadza recenzje dostawców w formie analiz ryzyka łańcucha dostaw przed zawarciem umowy o nabycie systemów informacyjnych, komponentów lub usług dotyczących [systemu]. Dokumenty strategiczne poziomu 1 i poziomu 2 nakładają wymagania w zakresie analiz ryzyka łańcucha dostaw na partnerów biznesowych starających się o nabycie systemów, komponentów bądź usług IT. Procedura analizy ryzyka łańcucha dostaw stanowi przewodnik krok po kroku dla partnerów biznesowych, który należy stosować w ramach przygotowań do oceny dostawców przez biuro zarządzania programem C-SCRM.

(7) RECENZJA PRZED WYBOREM/AKCEPTACJĄ/AKTUALIZACJĄ

Realizacja: Polityka poziomu 2 określa, jakie działania integracyjne związane z [systemem] wymagają przeprowadzenia analizy ryzyka łańcucha dostaw. Proces i wymagania są określone w standardowej procedurze operacyjnej.

(8) WYKORZYSTANIE INFORMACJI ZE WSZYSTKICH ŹRÓDEŁ

Realizacja: Biuro zarządzania programem C-SCRM wykorzystuje wszystkie źródła informacji podczas przeprowadzania oceny ryzyka łańcucha dostaw dla [systemu].

3.1.8. IDENTYFIKACJA RÓL

Należy określić rolę, nazwiska, dział/wydział, podstawowy i alternatywny numer telefonu oraz adres e-mail kluczowych pracowników zajmujących się cyberbezpieczeństwem w łańcuchu dostaw lub wyznaczyć osoby kontaktowe (np. przedstawicieli dostawców, ekspertów zajmujących się zamówieniami, liderów inżynierii, partnerów biznesowych) podając ich rolę, imię i nazwisko, adres, podstawowy i alternatywny numer telefonu oraz adres e-mail.

Przykładowy tekst

Tabela D-10: Określenie roli

Rola	Imię i nazwisko	Dział/wydział	Główny numer telefonu	Alternatywny numer telefonu	Adres e-mail
Przedstawiciel dostawcy					
Specjalista ds. zamówień					
Lider inżynierii					
Partner biznesowy					
Usługodawca					

3.1.9. SYTUACJE AWARYJNE I KRYZYSOWE

W przypadku organizacji, które decydują się na zakup produktów w przypadku operacji awaryjnych lub kryzysowych, podmioty mogą być zmuszone do ominięcia normalnych procedur zakupu wykorzystujących typowe procesy w obszarze C-SCRM, aby zapewnić ciągłość realizacji misji. Działania związane z zawieraniem umów, które nie są weryfikowane przy użyciu zatwierdzonych procesów planu C-SCRM, wprowadzają ryzyko operacyjne dla podmiotu.

W stosownych przypadkach należy opisać skrócone procedury zamówień, których należy przestrzegać w sytuacjach awaryjnych i kryzysowych, takie jak dane kontaktowe specjalistów w zakresie C-SCRM, zamówień oraz przedstawicieli działów prawnych, którzy mogą udzielać porad poza granicami formalnego łańcucha zatwierdzania.

Przykładowy tekst

W przypadku sytuacji awaryjnej i nagłej potrzeby zakupu komponentu, biuro zarządzania programem C-SCRM zaoferuje swoją pomoc w postaci ekspertów zajmujących się zagadnieniami w zakresie C-SCRM w celu zapewnienia wsparcia w razie braku formalnego łańcucha zatwierdzenia. CIO jest uprawniony do udzielania zezwoleń na ominięcie formalnych procedur. Aktualne informacje kontaktowe dotyczące ekspertów zajmujących się obszarem C-SCRM znajdują się poniżej:

- Ekspert ds. C-SCRM:
  - ✓ Imię i nazwisko,
  - ✓ Adres e-mail,
  - ✓ Numer telefonu.
- Specjalista ds. zamówień:
  - ✓ Imię i nazwisko,
  - ✓ Adres e-mail,
  - ✓ Numer telefonu.
- Specjalista ds. prawnych:
  - ✓ Imię i nazwisko,
  - ✓ Adres e-mail,
  - ✓ Numer telefonu.

3.1.10. POWIĄZANE PRZEPISY PRAWA, REGULACJE I POLITYKI

Należy wymienić wszelkie obowiązujące przepisy, rozporządzenia, dyrektywy, polityki i regulacje, które mają zastosowanie do systemu. W przypadku poziomu 3 należy uwzględnić odpowiednie plany strategiczne i wdrożeniowe C-SCRM poziomu 1 oraz tytuły polityk C-SCRM poziomu 2.

Przykładowy tekst

Podmiot zapewnia zgodność środków bezpieczeństwa ujętych w planie C-SCRM z obowiązującymi przepisami ustawowymi, wymogami regulacyjnymi i wytycznymi zewnętrznymi,) oraz wewnętrznymi politykami i dokumentami strategicznymi dotyczącymi C-SCRM.

3.1.11. PRZEGLĄD I UTRZYMANIE

Należy dołączyć tabelę, w której określona jest data zmiany, opis zmiany oraz nazwisko osoby, która dokonała zmiany. Plany dotyczące C-SCRM poziomu 3 należy poddawać przeglądom oraz aktualizować na kolejnych etapach cyklu życia systemów, podczas przeglądów oraz w przypadku znaczących działań związanych z zawieraniem umów, a także w razie potrzeby należy weryfikować je pod kątem zgodności z planami wyższego poziomu. Należy upewnić się, że plan jest dostosowany do zmieniających się wpływów czynników zewnętrznych, takich jak zagrożenia i zmiany w podmiocie lub środowisku.

Przykładowy tekst

Tabela D-11: Przegląd i utrzymanie

Numer wersji	Data	Opis zmiany/wersji	Rozdziały/Strony, których dotyczą zmiany	Zmiany dokonane przez nazwisko/stanowisko/podmiot

3.1.12. ZATWIERDZENIE PLANU C-SCRM

Dokument należy opatrzyć podpisem (elektronicznym lub odręcznym) oraz datą przeglądu i zatwierdzenia planu bezpieczeństwa systemu.

Przykładowy tekst

Osoba zatwierdzająca:

X _____

Imię i nazwisko

Data

3.1.13. LISTA AKRONIMÓW

Należy wyszczególnić i rozwinąć wszystkie akronimy wykorzystywane w planie C-SCRM.

Przykładowy tekst

Tabela D-12: Lista akronimów

Akronim	Opis
AO	Authorizing Official – Osoba autoryzująca
C-SCRM	Zarządzanie ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw
CŻS	Cykl życia systemu

3.1.14. ZAŁĄCZNIKI

Należy uwzględnić wszelkie istotne artefakty, które mogą dotyczyć planu C-SCRM.

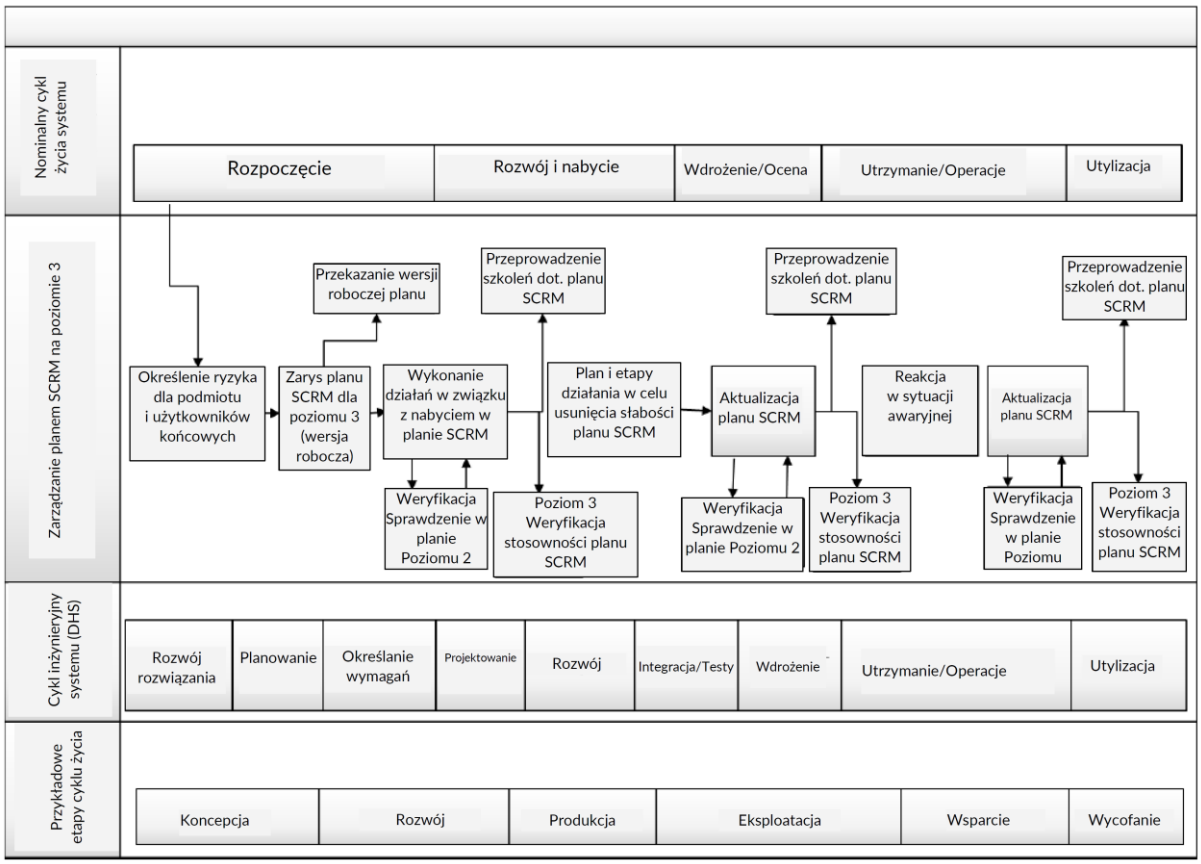
Przykładowy tekst

- Umowy z dostawcami
- Plany C-SCRM wykonawców lub dostawców

3.1.15. PLAN C-SCRM I CYKLE ŻYCIA

Plany C-SCRM powinny obejmować w sposób kompleksowy cykle życia systemów i programów, w tym badania i rozwój, projektowanie, wytwarzanie, zamówienia, dostarczanie, integrację, eksploatację oraz likwidację/wycofanie z eksploatacji. Działania związane z planem C-SCRM powinny być zintegrowane z procesami cyklu życia systemu i oprogramowania podmiotu. Podobne środki bezpieczeństwa w planie C-SCRM mogą być stosowane w więcej

niż jednym procesie cyklu życia. Poniższy rysunek wskazuje, w jaki sposób działania planu C-SCRM mogą być zintegrowane z różnymi przykładowymi cyklami życia.



Rysunek D-1: Przykładowy cykl życia planu C-SCRM

4. SZABLON OCENY RYZYKA DOTYCZĄCEGO CYBERBEZPIECZEŃSTWA W ŁAŃCUCHU DOSTAW

Ocena ryzyka dotyczącego cyberbezpieczeństwa w łańcuchu dostaw (C-SCRA)[53] umożliwia przegląd wszelkich produktów, usług lub zewnętrznych dostawców, które mogą być źródłem ryzyka związanego z cyberbezpieczeństwem dla podmiotu zamawiającego. Celem szablonu oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw jest przedstawienie zestawu pytań, które podmiot nabywający może wykorzystać w zależności od wybranych środków bezpieczeństwa. Ocena ta jest zwykle przeprowadzana przez biuro zarządzania programem C-SCRM na poziomie operacyjnym (poziom 3). Ocena uwzględnia dostępne informacje publiczne i prywatne w celu kompleksowej analizy sytuacji, w tym znane zagrożenia związane z cyberbezpieczeństwem w całym łańcuchu dostaw, prawdopodobieństwo ich wystąpienia oraz ich potencjalny wpływ na podmiot oraz jego informacje i systemy. Ze względu na mnogość analiz oraz próśb o informacje z nimi związane, podmiot powinien ocenić względny priorytet analiz i uwzględnić go jako czynnik wpływający na wymóg ich przeprowadzania.

Podobnie jak w przypadku innych opisanych szablonów, szablon oceny ryzyka łańcucha dostaw został przytoczony jedynie jako przykład. Podmioty powinny dostosować poniższe treści do swoich działań dotyczących ryzyka na poziomach 1 i 2. Przeprowadzenie oceny ryzyka dotyczącego cyberbezpieczeństwa w łańcuchu dostaw jest prawdopodobnie najbardziej widocznym i czasochłonnym elementem działań w obszarze C-SCRM, dlatego musi być zaprojektowana z myślą o efektywnej realizacji na szeroką skalę, a także musi mieć odpowiednie wsparcie, określone przepływy pracy oraz stosowną automatyzację, jeśli jest to możliwe. Organizacje powinny zapoznać się z treścią załącznika E w celu uzyskania dodatkowych wytycznych dotyczących oceny ryzyka łańcucha dostaw.

[53] Na potrzeby niniejszego dokumentu wyrażenie „ocena ryzyka dotyczącego cyberbezpieczeństwa w łańcuchu dostaw" należy uznać za równoważne z wyrażeniem „ocena ryzyka łańcucha dostaw" – takie rozwiązanie zostało zastosowane w celu ujednolicenia terminologii.

4.1. WZÓR DOKUMENTU ZWIĄZANEGO Z OBSZAREM C-SCRM

4.1.1. WŁADZA I ZGODNOŚĆ

Należy wymienić ustawy, zarządzenia, dyrektywy, rozporządzenia, polityki, standardy i wytyczne, które regulują prowadzenie ocen ryzyka łańcucha dostaw.

Przykładowy tekst

- Przepisy:
- Polityki:
  - ✓ Standardowa procedura operacyjna [podmiotu] w zakresie oceny ryzyka łańcucha dostaw
  - ✓ Czynniki oceny ryzyka łańcucha dostaw [podmiotu]
  - ✓ Kryteria oceny krytyczności [podmiotu] na potrzeby oceny ryzyka łańcucha dostaw;
- Rekomendacje:
  - ✓ NSC 800-53: PM-30, RA-3, SA-15, SR-5.
  - ✓ NSC 800-37.
  - ✓ NSC 800-161.: Załącznik C.
  - ✓ normy ISO 28001:2007.

4.1.2. OPIS

Należy opisać cel i zakres szablonu oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw oraz odnieść się do działań podmiotu w obszarze C-SCRM i zobowiązania do przeprowadzania ocen ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw w tym kontekście. Należy przedstawić powiązania szablonu z zasadami, ramami i praktykami zarządzania ryzykiem w podmiocie. Może to obejmować przegląd procesów oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw podmiotu, standardowych procedur operacyjnych oraz ocen krytyczności, które regulują użycie tego szablonu.

Należy poprzeć uzasadnienie realizacji oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw podkreślając korzyści płynące z ograniczenia spodziewanych strat wynikających z niekorzystnych zdarzeń cyberbezpieczeństwa w łańcuchu dostaw, a także roli biura zarządzania programem C-SCRM w skutecznym przeprowadzeniu tych ocen w skali.

Należy przedstawić przegląd granic autoryzacji podmiotu, systemów i usług w zakresie oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw.

Należy podać dane kontaktowe i inne zasoby, do których czytelnicy mogą uzyskać dostęp w celu dalszego zaangażowania się w proces oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw.

Przykładowy tekst

Niniejsze oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw mają na celu kompleksową ocenę ryzyka [podmiotu] ze strony podmiotów zewnętrznych, które mogą wyrządzić szkodę lub narazić je na szwank w związku z zagrożeniami związanymi z cyberbezpieczeństwem. Ryzyko związane z cyberbezpieczeństwem w łańcuchu dostaw obejmuje narażenia, zagrożenia i podatności związane z produktami i usługami przechodzącymi przez łańcuch dostaw, a także narażenia, zagrożenia i podatności dotyczące samego łańcucha dostaw i jego dostawców.

Szablon oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw stanowi źródło wytycznych dla biura zarządzania programem C-SCRM w zakresie przeglądu ryzyka cyberbezpieczeństwa w łańcuchu dostaw i zapewnienia, że oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw są odpowiednio, sprawnie i skutecznie przeprowadzane zgodnie ze zobowiązaniem i uprawnieniami podmiotu.

Osoby chcące wprowadzić produkty, usługi lub dostawców powinni zapoznać się z poniższym wzorem. Umożliwi to dostarczenie stosownych informacji do biura zarządzania programem C-SCRM w celu zapewnienia terminowego wykonania oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw i zapewni, że poszczególne etapy procesu będą dostosowane do kolejnych etapów oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw.

Proces oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw składa się z pięciu podstawowych kroków, przedstawionych w poniższym szablonie[54]:

[54] Zasady metodologii oraz wytyczne stanowiące ich podstawę znajdują się w treści Załącznika D poświęconego etapowi oceny.

1. Gromadzenie informacji i analiza zakresu.
2. Analiza zagrożeń.
3. Analiza podatności.
4. Analizy wpływu.
5. Analiza reakcji na ryzyko.

Aby dowiedzieć się więcej o procesie oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw lub złożyć prośbę o ocenę do biura zarządzania programem C-SCRM, należy skorzystać ze [strony intranetowej podmiotu] lub skontaktować się z [adres e-mail biura zarządzania programem C-SCRM].

4.1.3. GROMADZENIE INFORMACJI I ANALIZA ZAKRESU

Należy określić cele i założenia oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw oraz nakreślić zakres kluczowych informacji wymaganych do odpowiedniego zdefiniowania systemu, operacji, architektury wspierającej i granic autoryzacji. Należy przekazać osobom proszącym o ocenę kluczowe pytania mające na celu ułatwienie gromadzenia i analizy tych informacji. Biuro zarządzania programem C-SCRM będzie następnie wykorzystywać te informacje jako punkt odniesienia dla kolejnych analiz i próśb o przekazanie danych.

Przykładowy tekst

Tabela D-13: Gromadzenie informacji i analiza zakresu

Kwestionariusz oceny zarządzania ryzykiem w łańcuchu dostaw		
Rozdział 1: Przegląd wniosku	**Odpowiedź:**	**Autor odpowiedzi:**
Imię i nazwisko wnioskodawcy		Nabywca
Cel i zadania oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw		Nabywca
Opis systemu		Nabywca
Omówienie architektury		Nabywca
Określenie granicy autoryzacji		Nabywca

Kwestionariusz oceny zarządzania ryzykiem w łańcuchu dostaw		
Data oceny		Nabywca
Imię i nazwisko oceniającego		Nabywca
Rozdział 2: Przegląd ryzyka wewnętrznego produktu/usługi		
Za jaki odsetek sprzedaży produktu/usługi przez dostawcę odpowiada podmiot?		Nabywca lub Dostawca
Jak szeroko stosowany jest lub będzie produkt lub usługa w podmiocie?		Nabywca
Czy produkt/usługa są wytwarzane w lokalizacji geograficznej, która jest uważana za obszar ryzyka geopolitycznego dla podmiotu w oparciu o jego główny obszar działania?		Nabywca lub Dostawca
Czy produkt jest wytwarzany lub opracowywany w kraju określonym jako zagraniczny wróg lub kraj budzący szczególny niepokój?		Nabywca
Czy zmiana dostawcy tego produktu lub usługi na alternatywnego dostawcę stanowiłaby dla podmiotu znaczący koszt lub wysiłek?		Nabywca
Czy podmiot ma istniejące relacje z innym dostawcą produktu/usługi?		Nabywca
Jaka jest pewność podmiotu, że będzie w stanie uzyskać wysokiej jakości produkty/usługi niezależnie od poważnych zakłóceń w łańcuchu dostaw, zarówno wynikających z działalności ludzi, jak i z przyczyn naturalnych?		Nabywca
Czy podmiot utrzymuje rezerwę produktu/usługi?		Nabywca
Czy produkt lub usługa są odpowiednie do celu? (tj. czy są zdolne do realizacji celów lub poziomów usług)?		Nabywca
Czy produkt/usługa spełnia istotną funkcję z punktu widzenia bezpieczeństwa? Jeśli tak, proszę ją opisać.		Nabywca
Czy produkt/usługa posiada dostęp na poziomie root do sieci IT, systemów OT lub wrażliwych platform?		Nabywca

Kwestionariusz oceny zarządzania ryzykiem w łańcuchu dostaw		
Czy naruszenie zasad ochrony produktu/usługi może doprowadzić do awarii systemu lub poważnej degradacji jego działania?		Nabywca
Czy w przypadku naruszenia zasad ochrony prowadzącego do awarii systemu lub poważnej degradacji jego działania istnieje znany niezależny, niezawodny środek zaradczy?		Nabywca
Czy produkt lub usługa root będą lub są połączone z platformą, która jest udostępniana klientom przez podmiot?		Nabywca
Czy produkt/usługa będzie przesyłać, generować, utrzymywać lub przetwarzać dane o wysokiej wartości, takie jak dane osobowe, medyczne lub dotyczące płatności?		Nabywca
Czy produkt/usługa będą miały dostęp do systemów, które przesyłają, generują, utrzymują lub przetwarzają dane o wysokiej wartości, takie jak dane osobowe, medyczne lub dotyczące płatności?		Nabywca
Czy dostawca będzie wymagał fizycznego dostępu do obiektów podmiotu w związku z dostarczaniem produktu/usługi?		Nabywca
W oparciu o powyższe informacje, jaki jest poziom krytyczności produktu lub usługi dla podmiotu rot (tj. krytyczny, wysoki, umiarkowany, niski)?		Nabywca
Rozdział 3: Omówienie dostawcy		
Czy zidentyfikowano kluczowych dostawców?		Dostawca
Czy zweryfikowano strukturę posiadania podmiotu dostawcy, w tym jednostki zagraniczne, jak i krajowe?		Dostawca
Jeśli dostawca korzysta z dystrybutorów, czy zostali zweryfikowani pod kątem potencjalnego ryzyka?		Dostawca
Czy dostawca ma siedzibę w Polsce?		Dostawca
Czy dostawca ma powiązania personalne lub zawodowe (np. dyrektorów, kierowników wyższego szczebla, pracowników, konsultantów lub wykonawców) z jakimkolwiek		Dostawca

Kwestionariusz oceny zarządzania ryzykiem w łańcuchu dostaw		
zagranicznym rządem?		
Czy jakiekolwiek podmioty gospodarcze występujące w łańcuchu dostaw są własnością obcych państw, podlegają ich kontroli lub wpływom? Jeśli tak, to czy jest to związane z przeciwnikami lub państwem będącymi powodem do niepokoju?		Dostawca
Czy prawa i przepisy jakiegokolwiek obcego kraju, w którym dostawca posiada siedzibę, ośrodki badawczo-rozwojowe, produkcyjne, testowe, pakujące, dystrybucyjne lub usługowe, a także w których prowadzi działalność, wymagają udostępniania technologii lub danych temu krajowi?		Dostawca
Czy dostawca zadeklarował, skąd będą kupowane komponenty zamienne?		Dostawca
Czy zidentyfikowano i zweryfikowano struktury własności i lokalizacje wszystkich dostawców, podwykonawców i dostawców podrzędnych?		Dostawca
Czy dostawca wykorzystuje scenariusze zagrożeń do weryfikacji dostawców podrzędnych?		Dostawca
Czy dostawca posiada dokumenty pozwalające na powiązanie numerów części oraz ich producentów?		Dostawca
Czy dostawca może przedstawić listę podmiotów, u których zaopatruje się w sprzęt i oprogramowanie wykorzystywane w realizacji zamówienia?		Dostawca
Czy dostawca wdrożył środki zabezpieczające przed podróbkami?		Dostawca
Czy dostawca zabezpiecza kluczowe informacje o programie, które mogą być narażone poprzez interakcje z innymi dostawcami?		Dostawca
Czy dostawca przeprowadza przeglądy i inspekcje oraz wdrożył odpowiednie zabezpieczenia w celu wykrywania lub uniknięcia wykorzystania podrobionego sprzętu, zmanipulowanego sprzętu lub oprogramowania, a także podatności oraz wycieków danych?		Dostawca

Kwestionariusz oceny zarządzania ryzykiem w łańcuchu dostaw		
Czy przy zakupie oprogramowania dostawca korzysta z branżowych standardów bazowych i jakich?		Dostawca
Czy dostawca przestrzega prawa oraz regulacji?		Dostawca
Czy dostawca posiada procedury bezpiecznego utrzymania i aktualizacji po wdrożeniu?		Dostawca
Rozdział 4: Polityka i procedury		
Czy dostawca określił polityki i procedury, które pomagają zminimalizować ryzyko związane z łańcuchem dostaw, w tym związane z potrzebami pozyskiwania towarów od podmiotów zewnętrznych?		Dostawca
Czy dostawca określa krytyczność i możliwości systemu?		Dostawca
Czy wszystkie osoby związane z zamówieniem (np. dostawca, biuro zarządzania programem C-SCRM) rozumieją potencjalne zagrożenia i ryzyka w łańcuchu dostaw?		Dostawca
Jakie jest obywatelstwo wszystkich zaangażowanych osób? Jeśli jest to wymagane, czy wszyscy zaangażowani pracownicy są obywatelami Polski?		Dostawca
Czy dostawca wdrożył zabezpieczenia przed zagrożeniami wewnętrznymi?		Dostawca
Czy dostawca weryfikuje i monitoruje wszystkich pracowników mających kontakt z przedmiotowym wyrobem, systemem lub usługą, aby wiedzieć, czy stanowią zagrożenie?		Dostawca
Czy dostawca stosuje, rejestruje i śledzi działania ograniczające ryzyko w całym cyklu życia wyrobu, systemu lub usługi?		Dostawca
Czy wszyscy pracownicy dostawcy podpisali umowy o nieujawnianiu informacji?		Dostawca
Czy dostawca pozwala swojemu personelowi lub poddostawcom na dostęp zdalny do środowisk?		Dostawca

Kwestionariusz oceny zarządzania ryzykiem w łańcuchu dostaw		
Rozdział 5: Logistyka (jeśli dotyczy)		
Czy dostawca wdrożył udokumentowane procesy śledzenia i kontroli wersji?		Dostawca
Czy dostawca analizuje zdarzenia (środowiskowe lub spowodowane przez człowieka), które mogą przerwać jego łańcuch dostaw?		Dostawca
Czy gotowe części dostawcy są kontrolowane w taki sposób, by nigdy nie były pozostawiane bez nadzoru lub narażone na manipulacje?		Dostawca
Czy gotowe części dostawcy są przechowywane w zamkniętych pomieszczeniach?		Dostawca
Czy dostawca posiada proces zapewniający integralność przy zamawianiu części u swojego dostawcy?		Dostawca
Czy inwentaryzacje dostawcy są okresowo sprawdzane pod kątem narażenia na działanie czynników zewnętrznych lub manipulacji?		Dostawca
Czy dostawca posiada bezpieczne procedury niszczenia materiałów dotyczące nieużywanych i złomowanych części nabytych od swojego dostawcy?		Dostawca
Czy istnieje udokumentowany łańcuch nadzoru nad wdrażaniem produktów i systemów?		Dostawca
Rozdział 6: Projektowanie i rozwój oprogramowania (jeśli dotyczy)		
Czy dostawca zna wszystkich swoich dostawców, którzy będą pracować nad projektem produktu/systemu?		Dostawca i Producent
Czy dostawca dostosowuje swój cykl życia systemu do standardu bezpiecznego tworzenia oprogramowania (np. Microsoft Security Development Life Cycle)?		Dostawca i Producent
Czy dostawca wykonuje wszystkie prace rozwojowe w kraju?		Dostawca i Producent

Kwestionariusz oceny zarządzania ryzykiem w łańcuchu dostaw		
Czy tylko polscy obywatele mają dostęp do środowisk programistycznych?		Dostawca i Producent
Czy dostawca zapewnia swoim deweloperom szkolenia z zakresu cyberbezpieczeństwa?		Dostawca i Producent
Czy dostawca używa zaufanych narzędzi do tworzenia oprogramowania?		Dostawca i Producent
Czy dostawca stosuje zaufane środki bezpieczeństwa informacji w celu zabezpieczenia środowiska rozwojowego (np. bezpieczne konfiguracje sieci, ścisłe środki kontroli dostępu, dynamiczne/statyczne narzędzia do zarządzania podatnościami, testy penetracyjne)?		Dostawca i Producent
Czy dostawca weryfikuje oprogramowanie otwartoźródłowe przed użyciem?		Dostawca i Producent
Czy kompilatory oprogramowania dostawcy są stale monitorowane?		Dostawca i Producent
Czy dostawca posiada udokumentowane standardy testowania i konfiguracji oprogramowania?		Dostawca i Producent
Rozdział 7: Bezpieczeństwo dotyczące produktu lub usługi (jeśli dotyczy, jeden kwestionariusz na produkt/usługę)		
Nazwa produktu lub usługi		Producent
Rodzaj produktu (np. sprzęt, oprogramowanie, usługa)		Producent
Opis produktu lub usługi		Producent
Numer części (jeśli dotyczy)		Producent
Czy producent określił formalne role i zakresy odpowiedzialności za wdrożenie i nadzór nad bezpieczeństwem w całym procesie rozwoju lub produkcji oferowanych produktów?		Producent

Tłumaczenie

Kwestionariusz oceny zarządzania ryzykiem w łańcuchu dostaw		
Czy producent posiada procesy dotyczące integralności produktu, które są zgodne z normami takimi jak ISO 27036 lub SAE AS6171?		Producent
Opcjonalnie: Czy produkt jest zgodny z normą Federal Information Processing Standards (FIPS) 140-2? Jeśli tak, proszę podać poziom FIPS.		Producent
Czy producent dokumentuje i przekazuje wymagania dotyczące środków bezpieczeństwa dla sprzętu, oprogramowania lub oferowanych rozwiązań?		Producent
Czy w ciągu ostatniego roku producent został ukarany grzywną lub karą ze strony jakiejkolwiek jednostki rządowej lub organu regulacyjnego w związku z dostawą produktu lub usługi? Jeśli tak, proszę podać szczegóły.		Producent
Czy w ciągu ostatniego roku producent uczestniczył w sporach związanych z dostawą produktu lub usługi? Jeśli tak, proszę podać szczegóły.		Producent
Czy producent dostarcza wykaz materiałów dla produktów, usług lub komponentów, w tym wszystkich nośników, urządzeń logicznych, oprogramowania sprzętowego oraz oprogramowania instalowanego na urządzeniach?		Producent
Czy w przypadku komponentów sprzętowych wchodzących w skład oferty produktowej lub usługowej dostawca nabywa je wyłącznie od producentów oryginalnego sprzętu lub licencjonowanych sprzedawców?		Dostawca
Czy producent wdrożył politykę lub proces zapewniające, że żaden z dostawców lub komponentów nie znajduje się na żadnej liście podmiotów objętych sankcjami?		Producent
W jaki sposób producent zapobiega wprowadzeniu złośliwych lub podrobionych komponentów do swojej oferty produktów lub rozwiązań?		Producent

Kwestionariusz oceny zarządzania ryzykiem w łańcuchu dostaw		
Czy producent zarządza integralnością własności intelektualnej swoich produktów lub oferty usługowej?		Producent
W jaki sposób producent ocenia, priorytetyzuje i usuwa zgłoszone podatności w produktach lub usługach?		Producent
W jaki sposób producent zapewnia, że podatności w produktach lub usługach są usuwane w odpowiednim czasie, aby ograniczyć możliwość ataku?		Producent
Czy producent utrzymuje i zarządza programem zgłaszania i reagowania na incydenty bezpieczeństwa związane z produktem?		Producent
Jaki proces wykorzystuje producent w celu zapewnienia, że klienci oraz podmioty zewnętrzne (w tym organizacje sektora publicznego) otrzymują informacje o incydentach dotyczących wykorzystywanych produktów i usług?		Producent

4.1.4. ANALIZA ZAGROŻEŃ

Należy określić proces analizy zagrożeń, a także kryteria, które zostaną wykorzystane do oceny zagrożenia produktu, usługi lub dostawcy. Należy uwzględnić rubrykę z definicjami kategorii, aby zwiększyć przejrzystość wyników oceny.

Przykładowy tekst

Analiza zagrożeń oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw ocenia i charakteryzuje poziom zagrożenia dla integralności, wiarygodności i autentyczności produktu, usługi lub dostawcy. Analiza ta opiera się na zdolności i zamiarze podmiotu stwarzającego zagrożenie do naruszenia zasad ochrony lub wykorzystania produktu, usługi lub dostawcy w łańcuchu dostaw. Po zakończeniu analizy przypisywany jest jeden z następujących poziomów zagrożenia:

- **Krytyczny:** Informacje wskazują na bezpośrednie zagrożenie o wrogim charakterze (np. przeciwnik prowadzi aktywny atak na produkt, usługę lub dostawcę, dokonuje sabotażu lub wykorzystuje je do swoich celów).

- **Wysoki:** Informacje wskazują na to, że istnieje bezpośrednie zagrożenie (np. susza na danym obszarze geograficznym w połączeniu z lokalizacją danego podmiotu grozi dużym ryzykiem wystąpienia pożaru lasu).
- **Umiarkowany:** Informacje wskazują, że zagrożenie może mieć średni potencjał na wpłynięcie na podmiot lub ryzyko ataku jest średnie (np. istnieje konkretne zagrożenie, jednak nie ma możliwości lub zamiaru przeprowadzania ataku, wykorzystania produktu lub dokonania jego sabotażu).
- **Niski:** Informacje wskazują, że zagrożenie nie istnieje lub ma niski potencjał na wpłynięcie na podmiot lub ryzyko ataku jest niskie (np. zagrożenia nie mają możliwości ani zamiaru przeprowadzania ataku, wykorzystania produktu lub dokonania jego sabotażu).

Aby odpowiednio przypisać powyższe oznaczenia, biuro zarządzania programem C-SCRM i wnioskodawcy powinni wykorzystać kwestionariusz gromadzenia informacji oraz określania skali w celu koordynacji zbierania informacji związanych z produktem, usługą lub działalnością dostawcy, strukturą własności, kluczowym personelem zarządzającym, informacjami finansowymi, przedsięwzięciami biznesowymi, ograniczeniami regulacyjnymi i potencjalnymi zagrożeniami. W przypadku zaobserwowania powodów do obaw podczas wstępnego zbierania danych należy przeprowadzić dodatkowe analizy dotyczące wyżej wymienionych zagadnień.

4.1.5. ANALIZA PODATNOŚCI

Należy określić metody analizy podatności i kryteria, które zostaną wykorzystane do oceny podatności ocenianego produktu, usługi lub dostawcy. Należy uwzględnić rubrykę z definicjami kategorii, aby zwiększyć przejrzystość wyników analizy.

Przykładowy tekst

Analiza podatności oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw ocenia, a następnie charakteryzuje podatność produktu, usługi lub dostawcy w całym cyklu życia lub współpracy. Analiza obejmuje ocenę łatwości wykorzystania przez potencjalne zagrożenie o umiarkowanych możliwościach. Analiza ta opiera się na zdolności i zamiarze podmiotu stwarzającego zagrożenie do naruszenia zasad

ochrony lub wykorzystania produktu, usługi lub dostawcy w łańcuchu dostaw. Po zakończeniu analizy przypisywany jest jeden z następujących poziomów zagrożenia:

- **Krytyczny:** Produkt, usługa lub dostawca zawiera podatności lub słabości, które są całkowicie odsłonięte i łatwe do wykorzystania.
- **Wysoki:** Produkt, usługa lub dostawca zawiera podatności lub słabości, które są w dużym stopniu odsłonięte i możliwe do wykorzystania.
- **Umiarkowany:** Produkt, usługa lub dostawca zawiera podatności lub słabości, które są umiarkowanie odsłonięte i trudne do wykorzystania.
- **Niski:** Produkt, usługa lub dostawca zawiera podatności i słabości, które są odsłonięte w małym stopniu i jest mało prawdopodobne, że zostaną wykorzystane.

Aby odpowiednio przypisać powyższe oznaczenia, biuro zarządzania programem C-SCRM i wnioskodawcy powinni koordynować zbieranie informacji związanych z produktem, usługą lub dostawcą w zakresie szczegółów operacyjnych, możliwości wykorzystania, szczegółów usługi, znanych podatności i technik ograniczania wpływu.

4.1.6. ANALIZY WPŁYWU

Należy określić metody analizy wpływu i kryteria, które zostaną wykorzystane do oceny krytyczności ocenianego produktu, usługi lub dostawcy. Należy uwzględnić rubrykę z definicjami kategorii, aby zwiększyć przejrzystość wyników oceny.

Przykładowy tekst

Analizy wpływu oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw ocenia, a następnie charakteryzuje wpływ produktu, usługi lub dostawcy w całym cyklu życia lub współpracy. Analiza obejmuje całościowy przegląd funkcjonalny w celu identyfikacji krytycznych funkcji i komponentów w oparciu o ocenę potencjalnych szkód spowodowanych przez możliwość utraty, uszkodzenia lub naruszenia zasad ochrony produktu, materiału lub usługi na działalność lub realizację misji podmiotu. Po zakończeniu analizy przypisywany jest jeden z następujących poziomów wpływu:

- **Krytyczny:** Nieprawidłowe działanie produktu, usługi lub dostawcy spowoduje przerwę w działalności podmiotu lub niedopuszczalne obniżenie poziomu usług, a przywrócenie ich do akceptowalnego poziomu będzie wymagało przeznaczenia dużej ilości czasu oraz zasobów.
- **Wysoki:** Nieprawidłowe działanie produktu, usługi lub dostawcy spowoduje poważną przerwę w działalności podmiotu lub znaczące obniżenie poziomu usług, a przywrócenie ich do akceptowalnego poziomu będzie wymagało przeznaczenia znaczących ilości czasu oraz zasobów.
- **Umiarkowany:** Nieprawidłowe działanie produktu, usługi lub dostawcy spowoduje przerwę w działalności podmiotu, jednak powrót do normalności będzie prosty i nie będzie niósł za sobą żadnych poważnych konsekwencji.
- **Niski:** Nieprawidłowe działanie produktu, usługi lub dostawcy nie spowoduje poważnych problemów dla podmiotu, a powrót do normalności będzie prosty i nie będzie niósł za sobą żadnych poważnych konsekwencji.

Aby odpowiednio przypisać powyższe oznaczenie, biuro zarządzania programem C-SCRM i wnioskodawcy powinni koordynować zbieranie informacji związanych z krytycznymi funkcjami i komponentami podmiotu, identyfikacją zamierzonego środowiska użytkowników produktu lub usługi oraz informacji o dostawcy.

4.1.7. ANALIZA REAKCJI NA RYZYKO

Należy określić metody analizy ryzyka i kryteria, które zostaną wykorzystane do oceny produktu, usługi lub dostawcy. Należy uwzględnić rubrykę z definicjami kategorii, aby zwiększyć przejrzystość wyników oceny.

Przykładowy tekst

Ocena narażenia na ryzyko w ramach oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw stanowi kompleksową ocenę opartą na analizie prawdopodobieństwa i wpływu. Wynik analizy prawdopodobieństwa stanowi połączony wynik analizy zagrożeń i podatności, jak przedstawiono na poniższym rysunku.

Poziom prawdopodobieństwa					
	Podatność				
		Niski	Umiarkowany	Wysoki	Krytyczny
Zagrożenie	Krytyczny	Umiarkowanie prawdopodobne	Wysoce prawdopodobne	Bardzo prawdopodobne	Bardzo prawdopodobne
	Wysoki	Umiarkowanie prawdopodobne	Wysoce prawdopodobne	Wysoce prawdopodobne	Bardzo prawdopodobne
	Umiarkowany	Mało prawdopodobne	Umiarkowanie prawdopodobne	Wysoce prawdopodobne	Wysoce prawdopodobne
	Niski	Mało prawdopodobne	Mało prawdopodobne	Umiarkowanie prawdopodobne	Umiarkowanie prawdopodobne

Rysunek D-2: Przykład określania prawdopodobieństwa

Poziom narażenia na ryzyko ustalony w ramach oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw jest następnie ustalany w oparciu o wynik analizy prawdopodobieństwa i wpływu. Jeśli dla danego produktu lub usługi zidentyfikowano wiele słabych punktów, każdemu z nich przypisuje się poziom ryzyka oparty na prawdopodobieństwie wystąpienia i wpływie.

Ogólne narażenie na ryzyko					
	Wpływ				
		Niski	Umiarkowany	Wysoki	Krytyczny
Prawdopodobieństwo (zagrożenie i wrażliwość)	Bardzo prawdopodobne	Umiarkowany	Wysoki	Krytyczny	Krytyczny
	Wysoce prawdopodobne	Umiarkowany	Umiarkowany	Wysoki	Krytyczny
	Umiarkowanie prawdopodobne	Niski	Umiarkowany	Wysoki	Wysoki
	Mało prawdopodobne	Niski	Niski	Umiarkowany	Wysoki

Rysunek D-3: Przykład określenia narażenia na ryzyko

Wyżej wymienione analizy ryzyka i oceny stanowią mierniki, które pozwalają podmiotowi zadecydować, czy należy kontynuować zakup produktu, usługi lub zaangażowanie dostawcy. Decyzje o kontynuacji muszą być rozważone w kontekście apetytu na ryzyko i tolerancji ryzyka na wszystkich poziomach podmiotu, jak również strategii ograniczających ryzyko, które mogą zostać zastosowane w celu zarządzania ryzykiem związanym z nabyciem produktu, usługi lub zaangażowaniem dostawcy.

4.1.8. ROLE I OBOWIĄZKI

Należy wymienić osoby odpowiedzialne za politykę oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw, a także jej kluczowych współtwórców. Należy podać rolę i nazwisko każdej osoby lub grupy, a także w razie potrzeby informacje kontaktowe (np. przynależność, adres, adres e-mail, numer telefonu).

Przykładowy tekst

- Biuro zarządzania programem C-SCRM odpowiada za:
  - ✓ utrzymanie polityki, procedur i metodologii oceny zagrożenie i ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw;
  - ✓ przeprowadzenie standardowych procedur operacyjnych oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw;
  - ✓ utrzymywanie kontaktów z wnioskodawcami pragnącymi zamówić produkt, usługę lub skorzystać z usług dostawcy;
  - ✓ przedstawianie kierownictwu wyników oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw, aby pomóc w kształtowaniu postawy wobec ryzyka w podmiocie.
- Wnioskodawca odpowiada za:
  - ✓ wypełnianie formularzy wniosków oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw i podanie wszystkich wymaganych informacji;

- ✓ odniesienie się do wszystkich próśb o uzupełnienie informacji ze strony biura zarządzania programem C-SCRM w procesie oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw;
- ✓ przestrzeganie wszelkich postanowień i realizacja działań nakazanych przez biuro zarządzania programem C-SCRM po zatwierdzeniu wniosku oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw.

4.1.9. DEFINICJE

Należy wymienić kluczowe definicje opisane w polityce, a w razie potrzeby podać kontekst i przykłady charakterystyczne dla danego podmiotu.

Przykładowy tekst

- Zamówienie: Proces pozyskiwania systemu, produktu lub usługi.

4.1.10. PRZEGLĄD I UTRZYMANIE

Należy określić wymaganą częstotliwość aktualizacji szablonu oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw. Utrzymanie tabeli przeglądów pozwoli na wykorzystanie mechanizmu kontroli wersji. Szablony oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw są żywymi dokumentami, które muszą być aktualizowane i przekazywane wszystkim odpowiednim osobom (np. pracownikom, wykonawcom i dostawcom).

Przykładowy tekst

Szablon oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw musi być poddawany przeglądowi co najmniej raz w roku ze względu na dynamiczne zmiany w przepisach, politykach, normach, wytycznych i środkach bezpieczeństwa.

Dodatkowe kryteria, które mogą spowodować wprowadzenie zmian pomiędzy przeglądami, obejmują:

- Zmiany polityki, które mają wpływ na szablon oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw.
- Istotne zdarzenia C-SCRM.
- Wprowadzenie nowych technologii.

- Odkrycie nowych podatności.
- Zmiany operacyjne lub środowiskowe.
- Braki w szablonie oceny ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw.
- Zmiany zakresu.
- Inne kryteria specyficzne dla podmiotu.

Przykładowy tekst

Tabela D-14: Tabela kontroli wersji

Numer wersji	Data	Opis zmiany/wersji	Rozdziały/Strony, których dotyczą zmiany	Zmiany dokonane przez nazwisko/stanowisko/podmiot

ZAŁĄCZNIK E FASCSA[55]

WPROWADZENIE

Cel, grupy docelowe oraz kontekst

Niniejszy załącznik uzupełnia treść dokumentu NSC 800-161 i zawiera dodatkowe rekomendacje dotyczące podmiotów sektora publicznego w zakresie czynników oceny ryzyka łańcucha dostaw, dokumentacji oceny, poziomów ryzyka oraz reagowania na ryzyko.

Jak omówiono we wstępie do głównego dokumentu NSC 800-161, ustawa *The Federal Acquisition Supply Chain Security Act of 2018* (FASCSA), tytuł II ustawy *SECURE Technology Act* (P. L. 115-390)[56], została uchwalona w celu poprawy koordynacji działań władzy wykonawczej, wymiany informacji o ryzyku w łańcuchach dostaw oraz realizacji działań mających na celu przeciwdziałanie ryzyku w łańcuchach dostaw. Na mocy ustawy został powołany do życia międzyorganizacyjny organ wykonawczy – Federal Acquisition Security Council (FASC)[57] działający na szczeblu podmiotu federalnego. Organ ten jest upoważniony do realizacji szeregu działań mających na celu zmniejszenie narażenia rządu federalnego na ryzyko związane z łańcuchem dostaw oraz wpływu tego ryzyka.

Ustawa FASCSA zapewnia FASC (Federal Acquisition Security Council) i organizacjom wykonawczym uprawnienia związane z ograniczaniem ryzyka dotyczącego łańcuchów dostaw, w tym możliwość wykluczenia lub usunięcia źródeł i wybranych produktów[58].

[55] Treść załącznika E zawiera dane uzupełniające dla zainteresowanych organizacji. *Instytucje* powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje uzupełniające.

[56] Akt obowiązujący w amerykańskim systemie prawnym i nie ma odpowiednika w polskim porządku prawnym. Treść aktu może być pomocna przy tworzeniu stosownych polityk.

[57] Dodatkowe informacje na temat władz, członków, funkcji i procesów FASC można znaleźć w dokumencie Federal Acquisition Security Council Final Rule, 41 CFR Parts 201 oraz 201-1. Patrz: https://www.govinfo.gov/content/pkg/FR-2021-08-26/pdf/2021-17532.pdf.

[58] Zgodnie z definicją zawartą w ustawie FASCSA, pojęcie produktów oznacza: Technologie informacyjne, w tym wszelkiego rodzaju usługi przetwarzania w chmurze, sprzęt telekomunikacyjny lub usługi telekomunikacyjne; przetwarzanie informacji w publicznym lub prywatnym systemie informacyjnym, podlegające wymogom programu w zakresie kontrolowanych informacji jawnych, a także wszystkie technologie IoT/OT (np. sprzęt, systemy, urządzenia, oprogramowanie lub usługi obejmujące wbudowane technologie informacyjne).

Ustawa zobowiązuje również organizacje do ustalania oraz realizacji oceny ryzyka związanego z łańcuchem dostaw. Rekomendacje zawarte w niniejszym Załączniku E dotyczą tego wymogu określonego w ustawie FASCSA i odpowiadają na potrzebę zapewnienia bazowego poziomu spójności i dostosowania między obszarami oceny ryzyka oraz reagowania na ryzyko związane z cyberbezpieczeństwem w łańcuchy dostaw, a także obszarami zarządzania ryzykiem w łańcuchach dostaw na poziomie całego rządu, realizowanymi przez upoważnione organy[59].

Zakres

W ZAKRESIE

Niniejszy załącznik skupia się przede wszystkim na zapewnieniu organizacjom dodatkowych wytycznych dotyczących artykułu 1326 (a) (1) FASCSA[60], który wymaga od organizacji wykonawczych oceny ryzyka w łańcuchu dostaw wynikającego z nabycia i wykorzystania produktów oraz odpowiedniego reagowania na to ryzyko. Ustawa nakazuje organizacjom wykonywanie tej czynności i innych działań związanych z zarządzaniem ryzykiem w łańcuchu dostaw zgodnie z normami, wytycznymi i praktykami opracowanymi przez NIST.

POZA ZAKRESEM

Artykuł 4713 ustawy FASCSA[61] dotyczy uprawnień organizacji wykonawczych do przeprowadzania działań związanych z zamówieniami publicznymi objętymi przepisami. Szczegółowe wytyczne dotyczące tych działań wykraczają poza zakres niniejszego załącznika. Ustawa FASCSA wymaga, aby Federalna Rada ds. Regulacji Zamówień (FAR) określiła regulacje niezbędne do realizacji tych postanowień. NIST współpracuje i będzie nadal współpracować z FASC oraz podmiotami odpowiedzialnymi za zamówienia, aby opracować zharmonizowane wytyczne.

Niniejszy załącznik nie zawiera rekomendacji dotyczących sposobu przeprowadzania oceny – zapewniają je szkolenia oparte na rolach, edukacja oraz doświadczenie

[59] Dotyczy rynku amerykańskiego. Podano w celach informacyjnych dla zainteresowanych.

[60] Patrz: 41 USC 1326 (a) (1)

[61] 41 USC 4713

zawodowe. Zalecanym źródłem informacji jest również dokument NSC 800-30. Organizacje powinny podjąć kroki w celu zapewnienia, że pracownicy, którzy obecnie i w przyszłości będą odpowiedzialni za przeprowadzanie ocen ryzyka związanego z łańcuchem dostaw, posiadają odpowiednie umiejętności, wiedzę oraz rozległe doświadczenie wystarczające do określenia i rozróżnienia oznak ryzyka związanego z cyberbezpieczeństwem w łańcuchu dostaw oraz jego oceny. Organizacje zachęca się do inwestowania w szkolenia mające na celu rozwój i utrzymanie kompetencji w zakresie umiejętności analitycznych i wiedzy na temat zarządzania ryzykiem w łańcuchu dostaw. Szkolenie z zakresu kontrwywiadu i bezpieczeństwa jest również zdecydowanie zalecane dla pracowników biura zarządzania programem C-SCRM lub personelu, którego obowiązki dotyczą wykonywania ocen ryzyka związanego z cyberbezpieczeństwem łańcucha dostaw. Budowanie tej zdolności pomaga zapewnić wystarczające zrozumienie i świadomość zagrożeń dla łańcucha dostaw związanych z atakami, a jednocześnie umożliwia rozwój liderów w zakresie zarządzania ryzykiem, którzy będą w stanie zapewniać doradztwo oraz wsparcie decyzji i działań w zakresie reagowania na ryzyko.

Związek z dokumentem NSC 800-161

Praktyki i procesy mające na celu ocenę ryzyka, reagowanie oraz zarządzanie ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw są obszernie omówione w głównej części i załącznikach do dokumentu NSC 800-161. Niniejszy załącznik zawiera dodatkowe, rozszerzone wytyczne dostosowane do potrzeb organizacji. Niniejsze rekomendacje opisują zakres i rodzaj informacji i dokumentacji dotyczących ocen ryzyka w łańcuchu dostaw, wykorzystywanych do wspierania decyzji i działań w zakresie reagowania na ryzyko oraz udzielania porad w tym zakresie, zarówno wewnętrznie w przypadku przedstawicieli wyższego szczebla, jak i zewnętrznie, w przypadku organów takich jak FASC.

Niniejsze rozszerzone wytyczne mają również na celu zapewnienie podstawowej spójności i wystarczalności procesów i informacji dotyczących ryzyka w łańcuchach dostaw wykorzystywanych do celów związanych z oceną i dokumentacją, a także usprawnienie wymiany informacji i opracowanie zaleceń dla odpowiednich

decydentów, zarówno w danej organizacji, jak i na poziomie całego rządu. W ramach niezbędnego wsparcia dla analizy i procesu decyzyjnego na poziomie podmiotu publicznego, organizacje dysponują pełną elastycznością w zakresie oceny ryzyka i zarządzania nim w sposób zgodny z szerszymi wytycznymi zawartymi w głównej części dokumentu NSC 800-161 i jego załącznikach, a także wdrożonymi politykami, misją oraz priorytetowymi potrzebami czy istniejącymi praktykami (w zakresie, w jakim są one wystarczające).

Definicja ryzyka związanego z łańcuchem dostaw według ustawy FASCSA oraz dokumentu NSC-161

Organizacje powinny zwrócić uwagę, że definicja ryzyka łańcucha dostaw w ustawie FASCSA skupia się na ryzyku wynikającym z oceny, że podmiot stwarzający zagrożenie ma zamiar i możliwości prowadzenia złośliwych działań lub wyrządzenia szkody w inny sposób. Z kolei definicja i zakres ryzyka dotyczącego cyberbezpieczeństwa w łańcuchu dostaw opracowana przez NIST jest pod wieloma względami zgodna z definicją FASCSA, jednak charakteryzuje ją szerszy zakres – obejmuje bowiem ryzyko związane z celowymi złośliwymi działaniami, jak i innymi zagadnieniami. Zgodnie z zaleceniem zawartym w ustawie FASCSA, aby organizacje opierały się na normach i wytycznych NIST, organizacje muszą zapewnić, że ich działania w zakresie oceny ryzyka i reagowania na ryzyko dotyczą wszystkich zagrożeń związanych z cyberbezpieczeństwem w całym łańcuchu dostaw.

OCENA RYZYKA ZWIĄZANEGO Z ŁAŃCUCHEM DOSTAW

Informacje ogólne

Ustawa FASCSA wymaga, aby organizacje przeprowadzały oceny ryzyka w łańcuchach dostaw oraz ustalały priorytety tych ocen przy nabywaniu produktów, a także podczas ich użytkowania lub wykorzystywania. W większości przypadków wymusza to również konieczność oceny źródła produktu. Oceny ryzyka w łańcuchach dostaw przeprowadzane przez organizacje są w dużym stopniu uzależnione od środowiska operacyjnego i przypadku użycia związanego z produktem. Organizacje mają swobodę w stosowaniu wytycznych NIST do realizacji tych działań – nie istnieje jedno uniwersalne podejście do przeprowadzania ocen ryzyka. W celu ułatwienia

przeprowadzenia obowiązkowych ocen na poziomie całego rządu, wymaganych w celu oceny ryzyka, które może mieć wpływ na bezpieczeństwo narodowe lub misje wielu organizacji, istnieje potrzeba zapewnienia, że informacje i dokumentacja ocen ryzyka dotyczących łańcuchów dostaw organizacje zachowują poziom bazowy należytej staranności i normalizacji.

Informacje wykorzystywane do oceny będą obejmowały co najwyżej trzy kategorie danych:

1. Informacje o celu i kontekście (specyficzne dla danego przypadku użycia) wykorzystywane do zrozumienia środowiska ryzyka oraz do informowania i ustalania tolerancji ryzyka w odniesieniu do danego przypadku użycia.
2. Dane lub informacje uzyskane ze źródła.
3. Informacje pochodzące ze wszystkich źródeł, które mogą obejmować publicznie dostępne dane, źródła rządowe (w tym źródła niejawne) oraz komercyjne i płatne źródła danych.

Cel i kontekst, a także czas przeprowadzenia oceny dostawcy lub produktu w cyklu życia systemu lub zamówienia, wpływają na różnice zakresu, obszary oraz źródła, z których pozyskiwane są informacje wykorzystywane w ocenie.

Ustawa FASCSA uwzględnia, że organizacje mają ograniczone zasoby, jednak stwierdza konieczność priorytetyzacji ocen ryzyka w łańcuchach dostaw[62]. Priorytetyzacja nie ma być w tym przypadku rozumiana jako konieczność wyboru podzbioru źródeł lub artykułów, które powinny być poddane ocenie. Organizacje powinny raczej ustanowić wielopoziomowy zestaw priorytetów proporcjonalnych do krytyczności i potencjału wpływu ryzyka. Podział ten można następnie wykorzystać do wyznaczania terminów, kolejności, zakresu i częstotliwości ocen ryzyka w łańcuchu dostaw.

Poza priorytetami wynikającymi z czynników zewnętrznych, takich jak wytyczne rządowe, wymagania prawne itd., a także czynniki wpływające na priorytet ustanowione przez organizacje, dokument NSC 800-161 wskazuje, by organizacje

[62] Patrz: artykuł 1326 (a)(2) FASCSA.

priorytetowo traktowały oceny dotyczące kluczowych dostawców oraz krytycznych systemów i usług, ponieważ kompromitacja tych źródeł i produktów prawdopodobnie spowoduje większe szkody niż w przypadku rozwiązań i dostawców o niższej krytyczności. W przypadku tych ocen organizacje powinny uwzględnić wszystkie podstawowe czynniki ryzyka opisane w rozdziale „Bazowe czynniki ryzyka (typowe i minimalne)" uzupełniając i ustalając wagi czynników zgodnie z przypadkami użycia, aby odpowiednio uwzględnić wszystkie rodzaje zagrożeń i ryzyk. W przypadku dostawców i produktów innych niż krytyczne, jeśli nie istnieją inne zobowiązania oraz wymogi w tym zakresie, organizacje mają większą dowolność w wyborze bazowych czynników ryzyka opisanych w niniejszym załączniku zgodnie ze swoimi politykami wewnętrznymi i praktykami, a także ich uwzględnieniu przy ocenie ryzyka związanego z łańcuchem dostaw. Jeżeli jednak istnieje jedno lub więcej wiarygodnych ustaleń, które wskazują na to, że może istnieć lub istnieje znaczne ryzyko dla łańcucha dostaw (patrz schemat istotności ryzyka dla łańcucha dostaw), może być wymagane przeprowadzenie bardziej kompleksowej oceny, obejmującej wszystkie bazowe czynniki ryzyka lub bardziej szczegółowe badania i analizy czynników ryzyka. Więcej informacji znajduje się w wytycznych dotyczących reagowania na ryzyko opisanych w rozdziale dot. reagowania na ryzyko.

Odpowiedzialność za określenie poziomów priorytetów w zakresie ocen ryzyka dotyczących łańcucha dostaw, oceny wpływu, podejmowania decyzji dotyczących reagowania na ryzyko oraz podejmowania działań w oparciu o ustalenia zawarte w ocenach ryzyka dotyczących łańcucha dostaw są z natury rzeczy działaniami rządowymi, które nie mogą być zlecane na zewnątrz. Niektóre organizacje mogą jednak polegać na współpracy z wykwalifikowanym podmiotem zewnętrznym w celu uzyskania wsparcia w prowadzeniu analiz, dokumentowaniu ustaleń i przeglądzie istotnych informacji. Aby wspomóc swoje działania w zakresie badań i oceny, organizacje mogą również uzyskać dostęp do dostępnych komercyjnie danych lub narzędzi. W zamówieniach publicznych i umowach należy zawrzeć odpowiednie wymogi dotyczące dostępu do informacji na temat ryzyka w łańcuchach dostaw, posługiwania się nimi i ich zabezpieczania. Brak takiego działania stanowi lukę

w zabezpieczeniach i tworzy nieuzasadnione ryzyko dla łańcucha dostaw. Ponadto taka luka może podważyć celowość wysiłków organizacji w zakresie ocen ryzyka dotyczących łańcucha dostaw lub nawet ułatwić powodzenie złośliwych działań przeciwników. Ponadto personel organizacji powinien stosować się do wytycznych dyrektorów do spraw etyki oraz działów prawnych, aby zapewnić, że istnieją zabezpieczenia przed konfliktem interesów oraz niewłaściwym lub nieuprawnionym dostępem do informacji lub ich ujawnieniem, ponieważ informacje na temat ryzyka w łańcuchach dostaw mogą być informacjami wrażliwymi, chronionymi, a w niektórych przypadkach nawet niejawnymi. W przypadku tej ostatniej kategorii informacji organizacje muszą zapewnić przestrzeganie przepisów, polityk i procedur dotyczących informacji niejawnych oraz ograniczyć dostęp wyłącznie do pracowników, którzy posiadają odpowiednie poświadczenia, uprawnienia dostępu oraz wymagają tych informacji w swojej pracy.

We wszystkich przypadkach pracownicy wspierający przeprowadzanie oceny mają obowiązek zachowania obiektywności oraz kierowania się rozsądkiem, a także utrzymania należytej staranności w badaniu i analizowaniu dostawców i produktów, ponieważ informacje na temat ryzyka w łańcuchach dostaw stanowią podstawę do podejmowania późniejszych decyzji i działań w zakresie reagowania na ryzyko.

Bazowe czynniki ryzyka (typowe, minimalne)

W tej części opisano bazowe czynniki ryzyka w łańcuchu dostaw oraz rekomendacje, które organizacje powinny uwzględnić w określonej przez siebie metodologii ocen ryzyka dotyczących łańcucha dostaw (lub włączyć czynniki zawarte w tej metodologii). Czynniki te należy wykorzystywać jako wytyczne do analiz, określania oraz oceny ryzyka w procesach ocen ryzyka dotyczących łańcucha dostaw, które obejmują kluczowych dostawców lub krytyczne produkty. Wspólny poziom bazowy czynników ryzyka pomaga również zapewnić należytą staranność przeprowadzanych analiz, które stanowią podstawę decyzji i działań w zakresie reagowania na ryzyko, niezależnie od tego, czy mają one miejsce na różnych poziomach w ramach organizacji, czy na poziomie międzyorganizacyjnym.

Organizacje powinny oceniać dodatkowe czynniki poza czynnikami bazowymi, które uznają za istotne i stosowne dla danego przypadku oceny.

Cele ustanowienia tego bazowego zestawu czynników obejmują:

- ustanowienie poziomu oceny dostawców oraz produktów;
- zapewnienie, że minimalne niezbędne informacje są dostępne dla FASC, gdy są wymagane;
- promowanie spójności i porównywalności między organizacjami;
- pomoc w przeprowadzaniu bardziej zaawansowanych analiz, takich jak analiza trendów, związków przyczynowo-skutkowych lub korelacji pomiędzy zidentyfikowanymi wskaźnikami ryzyka a zrealizowanym ryzykiem;
- ustanowienie i utrzymanie bazy informacji wystarczającej do określania i zrozumienia potencjalnych opcji ograniczania ryzyka oraz ustalania priorytetów i analizy decyzji dotyczących ryzyka.

Poniższa tabela E-1 zawiera listę bazowych czynników ryzyka oraz odpowiadające im definicje lub opisy. Czynniki te są spójne i zgodne z czynnikami zawartymi w Zasadach Końcowych FASC[63]. W prawej kolumnie znajduje się lista rodzajów informacji, które mogą zostać określone i uznane za wskaźnik ryzyka. Lista ta ma służyć jako punkt odniesienia i nie obejmuje wszystkich możliwych wskaźników ryzyka. Informacje dotyczące kontekstowych czynników ryzyka powinny być znane organizacji i często są już udokumentowane (np. w planie bezpieczeństwa systemu lub planie zamówień). Ocena tych czynników specyficznych dla danego przypadku użycia i wynikających z kontekstu pomaga zrozumieć ryzyko podstawowe[64], pozwala na określenie i wybór odpowiednich środków bezpieczeństwa w zakresie cyberbezpieczeństwa i zarządzania ryzykiem w łańcuchu dostaw oraz wymogów dotyczących zamówień, a także pomaga w określeniu progu tolerancji ryzyka dla produktu związanego z danym przypadkiem użycia.

[63] CFR Part 201-1.300 Evaluation of Sources and Covered Articles

[64] Na potrzeby niniejszego dokumentu termin „ryzyko podstawowe" oznacza poziom ryzyka przy istniejącym zestawie środków bezpieczeństwa.

Kolejny zestaw czynników ryzyka związanych z podatnościami i zagrożeniami skupia się na ryzyku, które może być związane z samym produktem, powiązanym dostawcą lub łańcuchem dostaw. Organizacje przeanalizują wnioski związane z czynnikami bazowymi oraz dowolnymi innymi w celu stwierdzenia, czy istnieją oznaki zagrożenia ze strony podmiotu stwarzającego zagrożenie, prawdopodobieństwo naruszenia zasad bezpieczeństwa lub wyrządzenia szkody oraz konsekwencji wystąpienia takiego zdarzenia, a także czy ocenione ryzyko dotyczące dostawcy lub produktu mieści się w ramach dopuszczalnego poziomu tolerancji ryzyka lub go przekracza.

Tabela E-1: Bazowe czynniki ryzyka

Bazowy czynnik ryzyka	Definicja lub wytyczna	Wskaźniki ryzyka (jeśli dotyczy)
Przypadek użycia/kontekst (ryzyko podstawowe)		
Cel	Zrozumienie wymogów dotyczących produktu lub usługi oraz sposobu jego wykorzystania.	• Opcje dostępne na rynku pozwalające na zaspokojenie potrzeby. • Pilność potrzeby. • Czas trwania potrzeby.
Krytyczność	Określenie, czy produkt, usługa lub dostawca stanowią system krytyczny, krytyczny komponent systemu, krytyczną usługę lub kluczowego dostawcę. Dodatkowe wytyczne znajdują się w głównej treści dokumentu oraz w glosariuszu do dokumentu NSC 800-161 Informacje dotyczące oprogramowania krytycznego z punktu widzenia rozporządzenia wykonawczego znajdują się również w Załączniku F.	• Dostawca, produkt lub jego część składowa pełni kluczową funkcję, ma zasadniczy wpływ na taką funkcję lub naruszenie zasad bezpieczeństwa może doprowadzić do zagrożenia dla realizacji funkcji, zagrożenia życia lub bezpieczeństwa wewnętrznego, infrastruktury krytycznej lub interesu bezpieczeństwa narodowego. Może też być współzależny z innym produktem pełniącym lub mającym zasadnicze znaczenie dla takich funkcji.

Bazowy czynnik ryzyka	Definicja lub wytyczna	Wskaźniki ryzyka (jeśli dotyczy)
Informacje i dane	Należy określić i udokumentować rodzaj, ilość, cel i przepływ danych oraz informacji wykorzystywanych lub dostępnych przez produkt, usługę lub dostawcę.	• Potrzeba lub możliwość dostępu do nadzorowanych informacji jawnych lub informacji niejawnych. • Informacje będą udostępniane osobom lub podmiotom zewnętrznym innym niż główny wykonawca lub dostawca. • Naruszenie wejść lub wyjść produktu może spowodować zagrożenie życia.
Poziom zależności od dostawcy lub produktu	Należy określić oraz opisać stopień, w jakim organizacja jest zależna od produktu lub dostawcy oraz powody tej zależności.	• Częstotliwość wykorzystania produktu lub usługi w organizacji. • Jedno źródło dostaw. • Dostępność produktu lub usługi na rynku. • Dostępność lub dopuszczalne alternatywy dla produktu, usługi lub dostawcy.
Środowisko użytkownika/operacyjne, w którym produkt jest używany lub instalowany, lub w którym uruchamiana jest usługa	W przypadku produktów będących składnikiem systemów lub stanowiących ich komponent, środowisko użytkownika powinno być opisane w planie bezpieczeństwa systemu oraz planie systemu związanym z obszarem C-SCRM. W przypadku usług opartych na pracy wykonywanej przez pracowników należy określić oraz	• Plan bezpieczeństwa systemu oraz plan bezpieczeństwa związany z obszarem C-SCRM powinny określać oraz dokumentować ryzyka oraz opisywać wybrane środki bezpieczeństwa wdrożone lub wymagane do wdrożenia w celu ograniczenia tych ryzyk. • Istotne czynniki środowiskowe, które powodują obawy związane z ryzykiem, powinny być

Bazowy czynnik ryzyka	Definicja lub wytyczna	Wskaźniki ryzyka (jeśli dotyczy)
	udokumentować istotne informacje dotyczące środowiska użytkownika (tj. miejsca wykonywania pracy), które mogą wiązać się z ryzykiem dla organizacji.	udokumentowane w planach zamówień, a odpowiednie środki bezpieczeństwa uwzględnione w ofertach i umowach.
Współzależność między organizacjami	Należy określić oraz opisać współzależności między organizacjami dotyczące danych, systemów oraz funkcji i misji.	• Produkt pełni funkcję wspierającą usługi wspólne dla całego sektora publicznego. • Produkt wymienia dane z kluczowym systemem innej organizacji. • Wykonawca utrzymuje narzędzie analityczne, które przechowuje nadzorowane informacje jawne dotyczące całego sektora publicznego.
Podatności lub zagrożenia (ryzyko dziedziczne)		
Funkcjonalność, cechy i składniki produktu	Informacje informują o tym, czy produkt lub usługa są odpowiednie do celu oraz o stopniu pewności, że zostały spełnione obowiązujące wymiary C-SCRM (zob. rozdział 1.4 głównego dokumentu) oraz że istnieją nieusunięte słabości lub podatności.	• Możliwości dostawcy w zakresie wytworzenia i dostarczenia produktu lub usługi zgodnie z oczekiwaniami. • Wbudowane funkcje bezpieczeństwa lub ich brak • Podmiot zarządzający lub kontrolujący zabezpieczenia. • Opcje i ograniczenia bezpiecznej konfiguracji. • Zarządzanie i kontrola zabezpieczeń (kto, jak?). • Możliwości lub wymagania

Bazowy czynnik ryzyka	Definicja lub wytyczna	Wskaźniki ryzyka (jeśli dotyczy)
		w zakresie transmisji sieciowej/internetowej oraz metody połączeń. • Zestawienie materiałów obejmujących oprogramowanie oraz sprzęt.
		• Każda transmisja informacji lub danych (w tym, jeśli jest znana, identyfikacja źródła i lokalizacji inicjatora lub odbiorcy transmisji) realizowana przez produkt lub trafiająca do produktu niezbędna dla jego funkcjonowania.
Informacje o firmie (tj. dostawcy)	Informacje o firmie (wielkość, struktura, kluczowi liderzy i kondycja finansowa).	• Drzewo struktury podmiotu. • Okres prowadzenia działalności. • Fuzje i przejęcia (w przeszłości i obecnie). • Umowy z obcymi rządami. • Baza klientów i trendy. • Związki lub wcześniejsze doświadczenia liderów (działalność zarządu lub dyrektorów w zagranicznych rządach lub wojsku). • Stabilność zatrudnienia, wysoka rotacja lub zwolnienia na poziomie kierownictwa wyższego szczebla. • Liczba pracowników w danej lokalizacji i w całym podmiocie.

Bazowy czynnik ryzyka	Definicja lub wytyczna	Wskaźniki ryzyka (jeśli dotyczy)
		• Inwestorzy/inwestycje. • Sprzedaż patentów podmiotom zagranicznym. • Wskaźniki i trendy finansowe • Sprawozdania finansowe/audyt.
Jakość/Dotychczasowe wyniki	Informacje na temat możliwości dostawcy w zakresie wytwarzania i dostarczania produktu zgodnie z oczekiwaniami Powinno to obejmować określenie praktyk zapewnienia jakości związanych z zapobieganiem błędom lub wadom w wytwarzanych/ opracowywanych produktach oraz unikaniem problemów podczas dostarczania rozwiązań lub usług klientom.	• Informacje o wynikach w przeszłości. • Istotne oceny lub skargi klientów. • Wycofania produktów z rynku. • Wskaźniki jakości. • Informacje o programie jakości oraz certyfikacja.
Pracownicy	Informacje o pracownikach powiązanych lub zatrudnionych przez dostawcę lub podmiot w łańcuchu dostaw produktu lub usługi.	• Program dostawcy dotyczący weryfikacji pracowników, w tym istnienie programu dotyczącego zagrożeń wewnętrznych oraz informacja na temat przeprowadzania kontroli i weryfikacji wcześniejszego zatrudnienia pracowników. • Historia zatrudnienia przez wywiad, wojsko, organy ścigania lub inne służby bezpieczeństwa obcego państwa.

Bazowy czynnik ryzyka	Definicja lub wytyczna	Wskaźniki ryzyka (jeśli dotyczy)
		• Rotacja pracowników. • Poziom zatrudnienia i kompetencje. • Dowody wątpliwej lojalności oraz nieetycznych lub nielegalnych zachowań i działań.
Fizyczne	Informacje związane z fizycznymi aspektami środowiska, struktur, obiektów lub materiałów dotyczące zabezpieczeń oraz konsekwencji ich uszkodzenia, niedostępności lub naruszenia zasad ochrony.	• Informacje na temat skuteczności fizycznych środków bezpieczeństwa, w tym procedur i praktyk, które pomagają we wspieraniu bezpieczeństwa fizycznego. • Bliskość infrastruktury krytycznej lub wrażliwych zasobów lub funkcji misji. • Klęski żywiołowe lub zagrożenia sejsmiczne i klimatyczne.
Geopolityczne	Informacje związane z lokalizacją geograficzną lub regionem istotnym dla dostawcy lub łańcucha dostaw związanego z dostawcą, produktem bądź usługą.	• Polityczne przełomy lub korupcja w danej lokalizacji. • Zakłócenia w handlu. • Wymogi prawne. • Niestabilność kraju lub regionu.
Własność zagraniczna, kontrola lub wpływy	Posiadanie, kontrola lub wpływ na dostawcę lub produkty rzez podmioty zagraniczne (np. rząd zagraniczny lub strony będące własnością lub kontrolowane przez rząd zagraniczny, a także inne	• Kraj określony jako zagraniczny przeciwnik lub kraj będący zagrożeniem. • Dostawca lub jego poddostawcy komponentów posiadają siedzibę główną, obiekty badawcze, rozwojowe, produkcyjne, testowe, pakujące,

Bazowy czynnik ryzyka	Definicja lub wytyczna	Wskaźniki ryzyka (jeśli dotyczy)
	powiązania między źródłem a podmiotem zagranicznym).	dystrybucyjne lub usługowe albo prowadzą działalność w obcym kraju, w tym w kraju budzącym szczególne obawy lub uznanym za przeciwnika.
	Rząd zagraniczny posiada bezpośrednią lub pośrednią możliwość kierowania lub decydowania o sprawach, które mają wpływ na działalność przedsiębiorstwa.	• Określone powiązania zawodowe oraz personalne dostawcy – w tym dyrektorów, kierowników wyższego szczebla, pracowników, konsultantów lub wykonawców) z jakimkolwiek zagranicznym rządem. • Wpływ przepisów jakiegokolwiek obcego kraju, w którym dostawca posiada siedzibę, ośrodki badawczo-rozwojowe, produkcyjne, testowe, pakujące, dystrybucyjne lub usługowe, a także w których prowadzi działalność. • Charakter lub stopień własności, kontroli lub wpływu obcych państw na dostawcę. • Własność, kontrola lub wpływ obcych państw na wszelkie podmioty gospodarcze uczestniczące w łańcuchu dostaw, w tym na spółki zależne i podwykonawców; w tym wpływ lub własność przeciwników państwa lub kraju budzącego obawy. • Wszelkie przesłanki wskazujące, że dostawca może

Bazowy czynnik ryzyka	Definicja lub wytyczna	Wskaźniki ryzyka (jeśli dotyczy)
		zostać częściowo lub w całości przejęty przez podmiot zagraniczny lub przeciwnika zagranicznego. • Dostawca z siedzibą w kraju (bez niezależnej oceny sądowej), w którym prawo nakazuje współpracę ze służbami bezpieczeństwa tego kraju, w tym udostępnianie danych osobowych i innych informacji szczególnie chronionych. • Przesłanki świadczące o możliwości kontrolowania lub wpływania przez obcy interes na działalność lub zarządzanie dostawcy lub podmiotu w łańcuchu dostaw. • Kluczowi dyrektorzy w łańcuchu dostaw mają powiązania z zagranicznymi urzędnikami państwowymi lub podmiotami, w tym członkowie zarządu, dyrektorzy, generalni partnerzy i kierownicy wyższego szczebla. • Obcokrajowcy lub kluczowy personel zarządzający z obcego kraju zaangażowany w projektowanie, rozwój, produkcję lub dystrybucję produktu. • Znane powiązania dostawcy z wywiadem, organami ścigania lub innymi służbami

Bazowy czynnik ryzyka	Definicja lub wytyczna	Wskaźniki ryzyka (jeśli dotyczy)
		bezpieczeństwa obcego państwa lub przeciwnika. • Dostawca ma siedzibę lub znajduje się pod wpływem/kontrolą kraju, o którym wiadomo, że dopuszcza się kradzieży własności intelektualnej.
Zgodność/Kwestie prawne	Informacje na temat niezgodności z przepisami, sporów sądowych, czynów karalnych lub innych istotnych wymogów prawnych.	• Dokumentacja zgodności z odpowiednimi przepisami prawa, regulacjami, kontraktami lub umowami obowiązującymi w kraju. • Przestrzeganie sankcji. • Przestrzeganie praw handlowych. • Wyroki/grzywny.
Oszustwa, korupcja, sankcje i dostosowanie do interesów państwa	Informacje na temat przeszłej lub obecnej działalności korupcyjnej oraz podlegania zawieszeniu, wykluczeniu lub sankcjom (patrz tabela E-2 i omówienie tabeli).	• Spory sądowe w sprawach cywilnych lub karnych. • Przeszłe lub aktualne dowody oszustwa. • Historia kradzieży własności intelektualnej. • Transakcje dostawcy dotyczące sprzedaży towarów, sprzętu lub technologii wojskowych państwom wspierającym działalność terrorystyczną lub rozprzestrzeniającym technologię rakietową bądź broń chemiczną lub biologiczną oraz transakcje określone jako „stanowiące regionalne

Bazowy czynnik ryzyka	Definicja lub wytyczna	Wskaźniki ryzyka (jeśli dotyczy)
		zagrożenie wojskowe" dla interesów państwa. • Historia nieautoryzowanych transferów technologii.
Cyberbezpieczeństwo	Informacje o praktykach w zakresie cyberbezpieczeństwa, podatnościach lub incydentach dotyczących dostawcy, produktu, usługi bądź łańcucha dostaw.	• Dowody na istnienie skutecznych polityk i praktyk w zakresie cyberbezpieczeństwa • Historia włamań do sieci komputerowej dostawcy. • Historia kradzieży własności intelektualnej dostawcy. • Informacje o przejęciu lub nabyciu technologii lub własności intelektualnej przez obce wywiady.
		• Istnienie podatności w zakresie cyberbezpieczeństwa. • Wskaźniki złośliwej działalności, w tym naruszenie, wykorzystanie lub sabotaż związane z dostawcą lub produktem. • Nieautoryzowane przekazanie informacji lub danych przez produktu do obcego kraju.
*Produkty podrabiane i niezgodne z umową (należy uwzględnić na poziomie bazowym, jeśli dotyczy dostawcy lub ocenianego produktu; a także w razie	Informacje o podróbkach, podejrzeniach o wytwarzaniu podróbek, działalności w szarej strefie lub produktach niezgodnych z wymaganiami.	• Historia dostawcy w zakresie podróbek lub produktów niezgodnych z wymaganiami. • Praktyki i środki bezpieczeństwa dostawców w zakresie przeciwdziałania podróbkom.

Bazowy czynnik ryzyka	Definicja lub wytyczna	Wskaźniki ryzyka (jeśli dotyczy)
wątpliwości)		• Zamówienia komponentów z szarej strefy.
Relacje w łańcuchu dostaw, widoczność i środki bezpieczeństwa	Informacje o łańcuchu dostaw związanym z dostawcą lub produktem.	• Dowody na wdrożenie skutecznych praktyk w zakresie C-SCRM i zarządzania relacjami z dostawcami. • Komponenty lub materiały (istotne dla produktu) pochodzą z jednego źródła w łańcuchu dostaw • Poleganie na jednym szlaku handlowym. • Pochodzenie produktu.

Informacje o tych bazowych czynnikach ryzyka powinny być w większości dostępne z ogólnodostępnych źródeł, choć ich rodzaje, jakość i zakresy mogą być zróżnicowane. W niektórych przypadkach może nie być możliwe ustalenie jakichkolwiek informacji bądź zebrane dane mogą okazać się nieznaczące, co należy udokumentować. Analizy powinny być ukierunkowane na uzyskanie wiarygodnych informacji o największym znaczeniu dla celu i kontekstu, w którym przeprowadzana jest ocena (patrz omówienie jakości informacji w rozdziale „Dokumentacja oceny i zarządzanie dokumentacją"). Ze względu na te zmienne, próba standaryzacji poziomu czynnika ryzyka nie jest możliwa ani pożądana.

Ustalenia związane z tymi czynnikami mogą stanowić zróżnicowane połączenie wielu informacji o obiektywnych faktach, zagrożeniach, podatnościach lub narażeniach, które oceniane oddzielnie lub łącznie mogą wskazywać na możliwość wystąpienia lub istnienie ryzyka. Ustalenia mogą mieć również charakter pozytywny, neutralny lub negatywny. Pozytywne ustalenia wskazują, że dostawca lub produkt charakteryzuje się wiarygodnością. Ustalenia negatywne wskazują, że istnieje lub może istnieć ryzyko, które budzi obawy i w odniesieniu do którego należy ustalić, czy ryzyko mieści się w granicach tolerancji, czy wymaga ograniczenia, lub czy może wymusić potrzebę wymiany informacji z FASC.

Uwaga! Istnienie jednego lub większej liczby wskaźników ryzyka związanych z powyższymi czynnikami nie musi wskazywać, że dostawca, produkt lub usługa stwarzają realne lub niedopuszczalne ryzyko, ani też nie wskazuje na jego dotkliwość. Należy przeanalizować, jaka kombinacja czynników i ustaleń może powodować ryzyko lub ograniczać obawy związane z ryzykiem. Niepewność co do określenia ryzyka może spowodować potrzebę przeprowadzenia dodatkowych badań i analiz due diligence, eskalację wewnętrzną lub zewnętrzną, lub zwrócenie się o poradę czy ograniczanie ryzyka jest możliwe.

Niezależnie od oceny lub w ramach jej przeprowadzania, organizacje powinny zbadać, czy istnieją jakiekolwiek przepisy lub ograniczenia, które zabraniają korzystania z usług określonych dostawców oraz nabywania lub wykorzystywania określonych komponentów, usług lub materiałów. Poniższa lista, choć nie obejmuje wszystkich obowiązujących przepisów i ograniczeń, koncentruje się na własności i kontroli przez podmioty zagraniczne, innych rodzajach wpływów zagranicznych, przeciwnikach i inwestycjach zagranicznych, które mogą stanowić zagrożenie dla krajowego łańcucha dostaw.

Korzystanie z usług takich dostawców lub nabywanie produktów, usług lub materiałów od osób lub podmiotów znajdujących się na którejkolwiek z poniższych list stanowi naruszenie prawa, chyba że zostały udzielone wyjątki lub zezwolenia, dlatego takie podmioty powinny być wykluczone z procesu zamówień publicznych. Jeżeli dany produkt został zakupiony przed wejściem w życie poniższych zakazów, organizacje powinny przeprowadzić ocenę w celu ustalenia, czy powinny nadal korzystać z zakazanych produktów lub usług, a jeśli tak, to czy można ograniczyć wszelkie zagrożenia związane z ich stosowaniem.

1. **Lista wyszczególnionych obywateli (*ang. Specially Designated Nationals - SDN*) i lista osób objętych blokadą**: Biuro Zabezpieczeń Aktywów (OFAC) Departamentu Skarbu na mocy EO 13694 i zmienionego EO 13757, przewidziało umieszczenie na liście wyszczególnionych obywateli i osób zablokowanych (SDN) stron, które uznano za odpowiedzialne za złośliwe działania w zakresie cyberbezpieczeństwa, biorące udział w tych działaniach lub zaangażowane w nie bezpośrednio lub pośrednio. Każdy podmiot, w którym jedna lub więcej takich osób bezpośrednio lub pośrednio posiada 50% lub więcej udziałów, jest uznawany za zablokowany z mocy prawa. Podmioty nie mogą dokonywać żadnych transakcji, bezpośrednio lub pośrednio, z takimi osobami lub podmiotami.
2. **Lista sankcji sektorowych (*ang. Sectoral Sanctions Identifications - SSI*)**: Sankcje sektorowe nałożone na określone osoby działające w sektorach gospodarki rosyjskiej wskazanych przez Sekretarza Skarbu zostały nałożone na mocy EO 13662 poprzez dyrektywy wydane przez OFAC zgodnie z nadanymi mu uprawnieniami. Lista SSI określa osoby działające w sektorach gospodarki rosyjskiej, z którymi osobom ze Stanów Zjednoczonych zabrania się dokonywania transakcji, zapewniania finansowania lub obrotu długiem o terminie zapadalności dłuższym niż 90 dni.
3. **Lista osób uchylających się od sankcji zagranicznych (*ang. Foreign Sanctions Evaders - FSE*)**: OFAC publikuje listę zagranicznych osób i podmiotów, co do których stwierdzono, że naruszyły, usiłowały naruszyć lub spowodowały naruszenie sankcji USA wobec Syrii lub Iranu na podstawie EO 13608. Wymienia również osoby, które realizowały transakcje na rzecz lub w imieniu osób objętych sankcjami Stanów Zjednoczonych. Zbiorowo takie osoby i organizacje są nazywane podmiotami uchylającymi się od sankcji. Obywatele oraz podmioty w Stanach Zjednoczonych nie mogą dokonywać żadnych transakcji z takimi podmiotami.

4. **Wykluczenia w systemie przyznawania zamówień (*ang. System for Award Management - SAM*)**: System SAM zawiera elektroniczny spis firm wykluczonych z programów zamówień federalnych i publicznych realizowanych przez rząd Stanów Zjednoczonych (o ile nie zaznaczono inaczej), otrzymywania kontraktów federalnych, a także z niektórych rodzajów federalnej pomocy finansowej, niefinansowej i świadczeń. System SAM obejmuje dane z centralnego rejestru wykonawców, rejestrów federalnych, informacji dostępnych w Internecie, wniosków certyfikacyjnych oraz systemu listy stron wykluczonych. Zawiera także dane z listy wykluczeń Biura Inspektora Generalnego (GSA) (CFR Title 2, Part 180).
5. **Lista CAPTA (*ang. Correspondent Account Payable-Through Account Sanctions*) – zagraniczne organizacje finansowe podlegające sankcjom w zakresie rachunków bankowych**: Lista CAPTA zastąpiła listę zagranicznych organizacji finansowych podlegających przepisom Part 561. Zawiera nazwy zagranicznych organizacji finansowych objętych sankcjami, zakazami lub warunkami, które uniemożliwiają podmiotom w Stanach Zjednoczonych prowadzenia z nimi interesów.
6. **Osoby zablokowane**: Zgodnie z przepisami 31 CFR 560 i 31 CFR 560.304 mienie i osoby znajdujące się na tej liście muszą zostać zablokowane, jeśli znajdują się w posiadaniu lub pod kontrolą obywatela Stanów Zjednoczonych.
7. **Lista stron niezweryfikowanych BIS**: Strony wymienione na liście stron niezweryfikowanych (ang. Unverified List) nie są uprawnione do otrzymywania produktów podlegających rozporządzeniu Export Administration Regulations (EAR) w drodze wyjątku od licencji.
8. **Artykuł 889 ustawy National Defense Authorization Act z 2019 roku**: O ile nie zostanie udzielony wyjątek, artykuł 889 ustawy NDAA zakazuje rządowi federalnemu, wykonawcom rządowym oraz beneficjentom dotacji i pożyczek zamawiania lub korzystania z niektórych objętych przepisami urządzeń lub usług telekomunikacyjnych związanych ze spółkami Huawei, ZTE, Hytera,

	Hikvision, Dahua i ich spółkami zależnymi w roli istotnego lub kluczowego komponentu jakiegokolwiek systemu lub jako technologii kluczowej w ramach jakiegokolwiek systemu.
9.	Wszelkie inne przepisy federalne lub prawa ograniczające nabywanie towarów, usług lub materiałów od dostawcy.

Schemat istotności ryzyka

Wymagane są wspólne ramy stanowiące punkt odniesienia dla organizacji przy określaniu odpowiedniej reakcji na ryzyko w związku z wynikami ocen ryzyka dotyczących łańcucha dostaw. Schemat ten wskazuje, czy zidentyfikowane ryzyko związane z danym dostawcą lub produktem może być zarządzane w ramach procesów C-SCRM ustanowionych przez organizację, czy też wymaga wewnętrznej lub zewnętrznej eskalacji w celu podjęcia decyzji lub działania w tym zakresie.

Przyjęcie i dostosowanie istniejącego ogólnourzędowego schematu jest wskazane, ponieważ zapewnia pewien stopień zbieżności i spójności z innymi powiązanymi procesami i wytycznymi, które są już w użyciu. Wprowadzony i opisany poniżej schemat istotności ryzyka łańcucha dostaw (*ang. Supply Chain Risk Severity Schema - SCRSS*) charakteryzuje się założeniami oraz strukturą zbliżoną do schematu istotności incydentu związanego z cyberbezpieczeństwem (*ang. Cyber Incident Severity Schema - CISS*), który został opracowany we współpracy z organizacjami realizującymi misję w zakresie cyberbezpieczeństwa lub operacji związanych z cyberbezpieczeństwem.

Schemat SCRSS jest oparty na schemacie CISS, lecz został dostosowany do ryzyka związanego z łańcuchem dostaw oraz cyberincydentów w celu zapewnienia jednolitej perspektywy dotyczącej:

- istotności ocenianego ryzyka związanego z łańcuchem dostaw związanego z danym dostawcą lub produktem;
- konieczności reakcji na ryzyko;
- poziomu niezbędnego do koordynowania lub podejmowania decyzji w zakresie reakcji na ryzyko;

- informacji, dokumentacji i procesów wymaganych do wspierania wysiłków związanych z reagowaniem na ryzyko.

Tabela E-2: Schemat istotności ryzyka

Poziom	Rodzaj	Opis
5	Istotne zagrożenie dla bezpieczeństwa narodowego	Ryzyko związane z wrogimi działaniami mające bezpośredni wpływ na interesy bezpieczeństwa narodowego.
4	Istotne ryzyko dla bezpieczeństwa narodowego	Ryzyko związane z wrogimi działaniami mające potencjalny wpływ na interesy bezpieczeństwa narodowego.
3	Znaczące ryzyko	Ryzyko związane z wrogimi działaniami, które może mieć potencjalny wpływ na wiele organizacji.
2	Znaczące ryzyko dla organizacji	Wysoki poziom ryzyka związany z kluczowym dostawcą, systemem, komponentem lub aktywem o dużej wartości dla organizacji.
1	Niskie lub umiarkowane ryzyko dla organizacji	Ocenione ryzyko, które nie spełnia wymagań dla żadnego z pozostałych czterech poziomów ryzyka.

Schemat istotności ryzyka przedstawiony w tabeli E-2 nie ma na celu zastąpienia istniejących, ustalonych przez organizację metodologii, które opisują i przypisują różne poziomy ryzyka. Należy go raczej używać jako punktu odniesienia w celu połączenia wyników oceny ryzyka przeprowadzonych przez organizację do poziomu na schemacie, który najlepiej opisuje rezultaty. Takie działanie pozwala na ocenę i opis poziomów ryzyka w sposób odpowiedni dla ich celu i kontekstu, a jednocześnie tworzy znormalizowany leksykon pozwalający na jednoznaczne opisywanie istotności ryzyka dostaw w całym podmiocie. Schemat pomaga również w przekazywaniu oczekiwań dotyczących koordynacji reakcji na ryzyko, wymiany informacji oraz obowiązków decyzyjnych związanych z każdym poziomem.

REKOMENDACJE DOTYCZĄCE REAKCJI NA RYZYKO

W zależności od poziomu ocenionego ryzyka łańcucha dostaw, organizacje mogą wymagać eskalacji i informacji z ocen ryzyka dotyczących łańcucha dostaw innym osobom w ramach swojej organizacji w celu przeprowadzenia dalszych badań, analiz lub podjęcia decyzji dotyczących reagowania na ryzyko lub zaangażowania podmiotów zewnętrznych.

Udostępnianie informacji

Ryzyko związane z łańcuchem dostaw ocenione na poziomie 3 i wyższym jest określane jako znaczące ryzyko zgodnie z zasadami FASC i wymaga obowiązkowej wymiany informacji z FASC za pośrednictwem Agencji Wymiany Informacji[65] (ISA) w celu przeglądu, a także dokonania dodatkowych analiz oraz realizacji działań. Organizacje mogą podjąć decyzję o wymianie informacji dotyczących zidentyfikowanych zagrożeń poziomu 2 lub poziomu 1 z łańcuchem dostaw FASC, zgodnie z procesami i wymogami FASC dotyczącymi wymiany informacji.

Informacje na temat ryzyka w łańcuchach dostaw, które zostały zdobyte lub określone w ramach procesów innych niż procesy oceny ryzyka, mogą również prowadzić do konieczności udostępnienia ich FASC lub innej organizacji rządowej. Przykłady takich informacji obejmują między innymi informacje o zdarzeniu w łańcuchu dostaw, incydencie w łańcuchu dostaw, informacje uzyskane od organizacji dochodzeniowej (np. Biura Inspektora Generalnego) lub anonimowe informacje otrzymane za pośrednictwem infolinii organizacji.

Wszelka wymiana informacji między organizacją a FASC, niezależnie od tego, czy jest obowiązkowa czy dobrowolna, powinna odbywać się zgodnie z wymogami i procesami wymiany informacji ustanowionymi przez FASC, a także zgodnie z ustawą i rozporządzeniami. Ponadto organizacje powinny wyznaczyć osobę odpowiedzialną, która będzie pełnić rolę łącznika w zakresie wymiany informacji z FASC. Organizacje

[65] Departament Bezpieczeństwa Wewnętrznego (DHS), w szczególności jego Agencja ds. Cyberbezpieczeństwa i Infrastruktury, został wyznaczony do pełnienia roli ISA na potrzeby FASC. Agencja ISA pełni funkcje administracyjne związane z wymianą informacji w imieniu FASC, zgodnie z przepisami 41 U.S.C. 1323 (a) (3)kk.

powinny ustanowić procesy wymiany (wysyłania i otrzymywania) informacji pomiędzy organizacją a FASC oraz ustanowić proporcjonalne wymagania i procesy dostosowane do ich organizacji w zakresie wymiany informacji na temat ryzyka w łańcuchach dostaw w ramach własnej organizacji.

Uwaga: FASC może wydać zaktualizowane lub dodatkowe wytyczne dotyczące okoliczności i kryteriów obowiązkowej i dobrowolnej wymiany informacji. Organizacje powinny zapoznać się z najbardziej aktualnymi wytycznymi FASC i postępować zgodnie z ich treścią.

Eskalacja reakcji na ryzyko i rozwiązywanie problemów

Instytucjom przypomina się o znaczeniu włączenia procesów zarządzania ryzykiem w łańcuchach dostaw do działań związanych z zarządzaniem ryzykiem w podmiocie, co zostało obszernie omówione w głównej części dokumentu oraz załącznikach do dokumentu NINSC800-161. W przypadku ryzyka, które zostało określone jako istotne z punktu widzenia SCRSS, konieczne jest przekazanie informacji o ocenie ryzyka do odpowiednich przedstawicieli wyższego szczebla w organizacji, w tym do działu prawnego. Organizacje powinny również zapewnić, że odpowiednie osoby posiadają stosowne poświadczenia bezpieczeństwa umożliwiające im dostęp do informacji niejawnych, aby wspomagać koordynację, decyzję lub działania w zakresie reagowania na ryzyko.

Ponieważ ryzyko uznane za znaczące jest z założenia związane z wrogimi działaniami, odpowiednie działania mogą obejmować współpracę z organami ścigania i kontrwywiadem, działania prawne oraz inne czynności. Udostępnianie informacji o znaczącym ryzyku FASC normalizuje i usprawnia proces, który powinny stosować organizacje w ramach oceny ryzyka.

DOKUMENTACJA OCENY I ZARZĄDZANIE REJESTRAMI

Wytyczne dotyczące dokumentacji

Instytucje muszą zapewnić, że opracowana dokumentacja oceny spełnia minimalne wymagania dokumentacyjne opisane w tym rozdziale, gdy informacje na temat dostawców lub produktów są przekazywane FASC lub eskalowane w ramach reakcji na ryzyko w związku z uprawnieniami organizacji określonych w artykule

4713. Normy bazowe w zakresie dokumentacji pomagają zapewnić opracowanie kompleksowej dokumentacji wspierającej procesy decyzyjne i działania w zakresie reagowania na ryzyko. Pomaga również promować spójność zakresu oraz organizacji treści w celu umożliwienia porównywalności, ponownego wykorzystania i wymiany informacji.

Wymagania dotyczące dokumentacji wykraczają poza gromadzenie informacji o ocenie czynników ryzyka i obejmują ogólne informacje na temat osób przeprowadzających oceny oraz czasu jej przeprowadzenia, informacje o dostawcy oraz produkcie, źródła danych wykorzystanych do uzyskania informacji, poziomy zaufania wobec poszczególnych ustaleń i zbiorczej analizy ustaleń oraz założenia i ograniczenia.

Organizacje powinny również wdrożyć i stosować określoną metodologię oceny i określania ryzyka. Metodologia ta powinna być udokumentowana lub omówiona w dokumentacji oceny dotyczącej danego dostawcy lub produktu. Wszelkie odstępstwa od metodologii wdrożonej przez organizacje powinny być opisane w rozdziale informacji ogólnych dokumentacji oceny.

Po zbadaniu i zebraniu informacji należy je uporządkować, aby uzyskać istotne ustalenia, które są zgodne z różnymi kategoriami czynników ryzyka. Informacje źródłowe (w tym metadane kontekstowe), zwłaszcza istotne ustalenia dotyczące ryzyka, powinny być udokumentowane w formie zachowującej integralność informacji i traktowane jako treść uzupełniająca, która może być wymagana do wsparcia i obrony decyzji lub działania związanego z reakcją na ryzyko. W związku z tym w ramach oceny należy uwzględnić źródła, a także informacje na temat jakości i zaufania do pozyskanych informacji oraz odpowiednio je udokumentować. Informacje wysokiej jakości powinny być aktualne, istotne, bezstronne, wystarczająco kompletne, dostępne w kontekście oraz uzyskane z wiarygodnych źródeł.

Wymogi dotyczące dokumentacji należy włączyć do istniejących polityk, procesów i procedur oceny ryzyka w łańcuchu dostaw. Wymagania te powinny być

opracowane w porozumieniu z kierownikiem organizacyjnym organizacji, w tym działem prawnym oraz pracownikami odpowiedzialnymi za zarządzanie dokumentacją, zarządzanie nadzorowanymi informacjami jawnymi i niejawnymi oraz prywatnością.

Choć format nie jest określony, minimalny zakres treści i dokumentacji oceny powinien obejmować treści opisane w tabeli E-3.

Tabela E-3: Dokumentacja oceny – minimalny zakres treści i dokumentacji

Informacje ogólne	Uwagi dodatkowe
Instytucja odpowiedzialna za ocenę	Organizacje powinny być w stanie określić punkty kontaktowe i zachować informacje o wszelkich pracownikach, którzy uczestniczyli w procesie oceny, a także określić narzędzia i źródła danych (w tym źródła komercyjne) wykorzystane na potrzeby oceny.
Data oceny lub przedział czasowy, w którym przeprowadzono ocenę	Organizacje powinny udokumentować, które z ich ustaleń mają charakter tymczasowy i mogą ulec zmianie w czasie.
Profil dostawcy: Identyfikator i informacje opisowe dotyczące ocenianego dostawcy	Należy udokumentować (w miarę możliwości) nazwę dostawcy, nazwę DBA[66], miejsce rejestracji działalności, adres fizyczny oraz lokalizację siedziby; numer DUNS[67](*ang. Data Universal Numbering System*) i kod CAGE[68]; numer telefonu; kraj rejestracji spółki; adres URL strony internetowej, strukturę spółki oraz informację na temat jej organizacji (jeśli jest znana); wielkość firmy; czas działalności; segment rynku.

[66] DBA - skrót od Doing Business As - to oficjalna fikcyjna nazwa, przybrana nazwa lub nazwa handlowa.

[67] Zastrzeżony system opracowany i zarządzany przez firmę Dun & Bradstreet (D&B), który przypisuje pojedynczym podmiotom gospodarczym unikalny numeryczny identyfikator, zwany „numerem DUNS".

[68] Kod CAGE jest skrótem od Commercial and Government Entity Code. Jest to system stworzony przez rząd Stanów Zjednoczonych w celu promowania łatwości znajdowania firm i korporacji, które pracują dla rządu USA, w szczególności Departamentu Obrony (DOD), Narodowej Agencji Aeronautyki i Administracji Kosmicznej (NASA) oraz Organizacji Traktatu Północnoatlantyckiego (NATO). Każda firma i korporacja muszą mieć wyznaczony kod CAGE, zanim będzie mogła prowadzić interesy z rządem i NATO.

Informacje ogólne	Uwagi dodatkowe
Identyfikator i informacje opisowe dotyczące ocenianego produktu	Należy udokumentować nazwę produktu, unikatowy identyfikator (np. numer modelu, numer wersji, numer seryjny), NAICS[69] i PSC[70] oraz krótki opis.
Podsumowanie celu i kontekstu oceny	Należy określić etap cyklu życia w momencie przeprowadzania oceny (np. badanie rynku, działanie związane z zamówieniem, użytkowanie operacyjne).
Metodologia oceny	Należy opisać metodologię oraz wszelkie odstępstwa od niej.
Badania, ustalenia i wyniki oceny ryzyka dostawcy lub produktu	Należy udokumentować wyniki ustaleń, identyfikacji i oceny ryzyka. W minimalnym zakresie należy przedstawić podsumowanie kluczowych ustaleń, analizę tych ustaleń oraz uzasadnienie określenia poziomu ryzyka. Podsumowanie to powinno dotyczyć potencjalnych lub istniejących zagrożeń (niezależnie od ich rodzaju) lub podatności dostawcy, produktu oraz łańcucha dostaw. Należy uwzględnić informacje na temat istotnych warunków i ograniczeń.
Ocena wpływu	W odniesieniu do celu i kontekstu oceny, należy opisać oceniony potencjał wpływu z uwagi na rodzaj, zakres i powagę określonego ryzyka.
Ograniczanie niedopuszczalnych zagrożeń	Należy uwzględnić omówienie zdolności, możliwości i gotowości dostawcy do ograniczenia ryzyka do zadowalającego poziomu, a także możliwości organizacji w tym obszarze. Należy określić możliwe opcje ograniczania ryzyka, jeśli są znane, w celu redukcji zagrożeń.

[69] Północnoamerykański System Klasyfikacji Przemysłu (ang. North American Industry Classification System - NAICS) jest standardem stosowanym przez federalne urzędy statystyczne do klasyfikowania przedsiębiorstw w celu gromadzenia, analizowania i publikowania danych statystycznych związanych z gospodarką biznesową USA.

[70] Paysafecard (PSC) – elektroniczna metoda płatności przeznaczona głównie do użytku w sklepach internetowych i bazująca na systemie pre-paid.

Informacje ogólne	Uwagi dodatkowe
Ocena poziomu dotkliwości ryzyka zgodnie ze schematem SCRSS	Należy uwzględnić poziom SCRSS oraz wyjaśnienie, dlaczego dany poziom został przypisany. Należy wziąć pod uwagę wpływ na misję lub aktywa narodowe, bezpieczeństwo narodowe i wewnętrzne oraz kluczowe funkcje związane z dostawcą lub produktem.
Reakcja na ryzyko	Należy opisać decyzje lub działania podjęte w reakcji na ryzyko (np. unikanie, ograniczanie, przekazanie do FASC w celu koordynacji i analizy).
Wszelkie inne informacje wymagane przez FASC lub dołączone według uznania organizacji	Należy opisać lub dołączyć informacje, które mogą być uwzględnione w ocenie ryzyka łańcucha dostaw, w tym informacje o wpływie na działalność organizacji oraz inne informacje wymagane przez FASC.
Przegląd informacji	Należy zapewnić zaufanie do źródeł oraz dostępnych informacji wykorzystywanych do oceny ryzyka związanego z postępowaniem, uwzględnić alternatywne rozwiązania oraz wdrożyć działania ograniczające ryzyko. Należy potwierdzić, że dokumentacja oceny została poddana przeglądowi i zatwierdzona przez odpowiednie osoby, w tym kierownictwo wyższego szczebla i dział prawny, jeśli ryzyko zostało uznane za znaczące. Przegląd dokumentacji ma również na celu zapewnienie, że dokumentacja oceny i informacje uzupełniające są odpowiednio zabezpieczone i oznaczone, a dostęp do nich jest ograniczony.

Rejestr oceny

Organizacje powinny przestrzegać wymogów dotyczących zarządzania rejestrami w odniesieniu do ocen ryzyka dotyczących łańcucha dostaw oraz informacji dodatkowych. W tym celu powinny wdrożyć polityki i procedury odnoszące się do wymogów i ograniczeń w zakresie ochrony, oznaczania, obsługi, przechowywania i rozpowszechniania rejestrów oceny i związanych z nimi treści.

Jeśli usługi w zakresie oceny (np. wsparcie analityczne) lub informacje dostarczane na zasadach komercyjnych są uzyskiwane w celu wsparcia opracowania rejestrów oceny, umowa (np. porozumienie międzyorganizacyjne) powinna określać odpowiednie wymogi i ograniczenia dotyczące zakresu, celu wykorzystania danych oraz ograniczeń, dostępu, usuwania i praw do przechowywania.

ZAŁĄCZNIK F ODPOWIEDŹ NA WEZWANIE DO PUBLIKACJI WYTYCZNYCH DOTYCZĄCYCH ZWIĘKSZANIA BEZPIECZEŃSTWA ŁAŃCUCHA DOSTAW OPROGRAMOWANIA, ZAWARTE W ZARZĄDZENIU WYKONAWCZYM NR 14028[71]

Organizacje, które chcą wdrożyć działania dotyczące zarządzania ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw zgodnie z zarządzeniem wykonawczym (EO) 14028, *Improving the Nation*'s Cybersecurity, powinny skorzystać ze specjalnego portalu internetowego NIST poświęconego EO 14028 pod adresem https://www.nist.gov/itl/executive- order-improving-nations-cybersecurity.

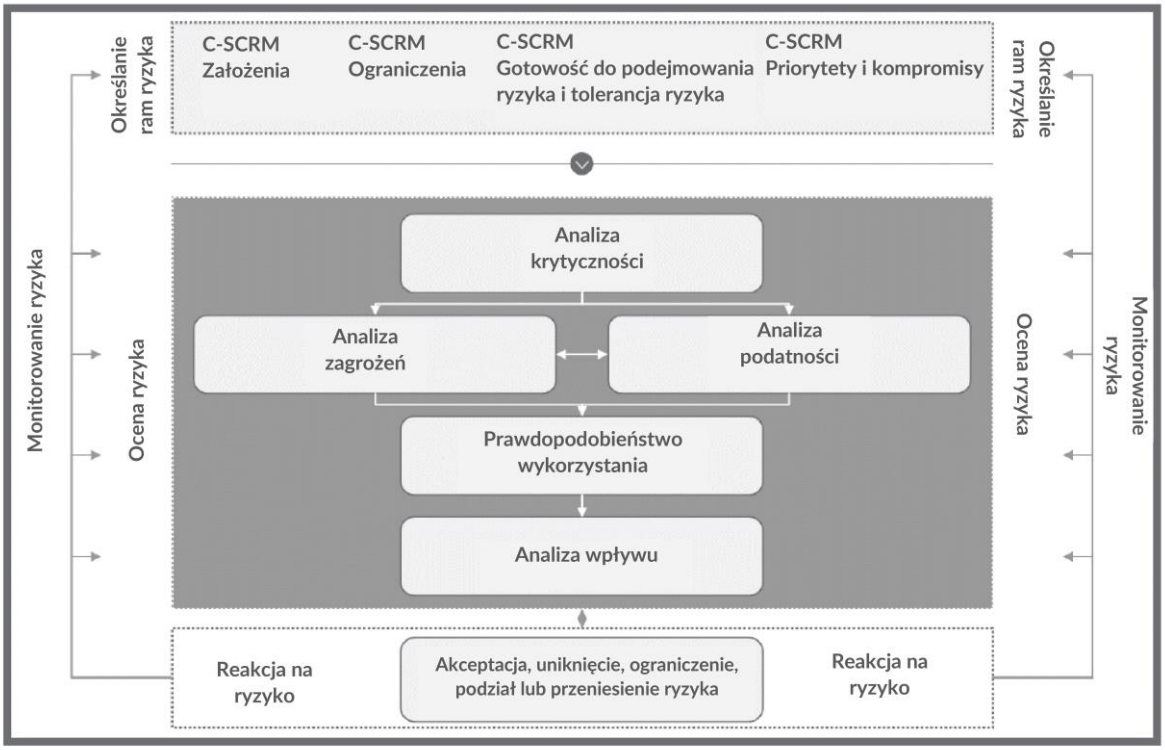
Wytyczne te zostały opublikowane w Internecie w celu:

- umieszczenia ich wraz z powiązanymi wytycznymi dotyczącymi EO publikowanymi przez NIST;
- umożliwienia aktualizacji w celu dostosowania do nowych wytycznych bez bezpośredniego wpływu na dokument NIST SP 800-161, Rev. 1; oraz
- zapewnienia możliwości identyfikowalności oraz powiązania z innymi zasobami internetowymi NIST w miarę ich wprowadzania do sieci, aby zachęcić do korzystania z nich zainteresowane strony.

[71] Treść załącznika F zawiera dane uzupełniające dla zainteresowanych organizacji.

ZAŁĄCZNIK G DZIAŁANIA ZWIĄZANE Z C-SCRM W PROCESIE ZARZĄDZANIA RYZYKIEM[72]

Zarządzanie ryzykiem to kompleksowy proces, który wymaga od podmiotów: 1) określenia ram ryzyka (tj. określenia kontekstu dla decyzji opartych na ryzyku);2) przeprowadzenia ocen ryzyka 3) reakcji na ryzyko po jego określeniu oraz 4) bieżącego monitorowania ryzyka przy użyciu skutecznej komunikacji w podmiocie oraz pętli informacji zwrotnej w celu ciągłego doskonalenia działań związanych z ryzykiem. Rysunek G-1 przedstawia wzajemne powiązania między etapami procesu zarządzania ryzykiem, w tym kolejność, w jakiej można przeprowadzić poszczególne analizy oraz interakcje wymagane do zapewnienia, że analiza obejmuje różne dane wejściowe na poziomie podmiotu, misji i operacji.



Rysunek G-1: Zarządzanie ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw (C-SCRM)

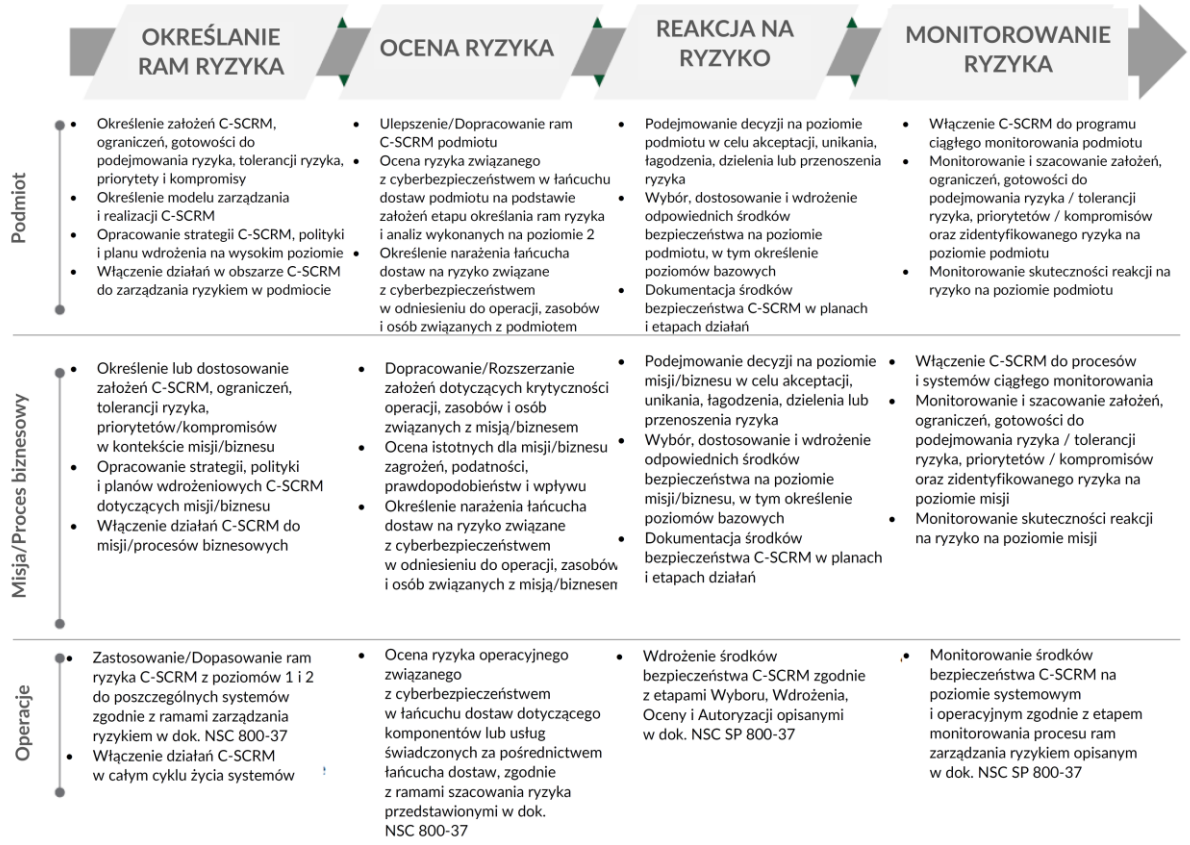
Poszczególne kroki procesu zarządzania ryzykiem (określanie ram, ocena, reagowanie i monitorowanie) mają charakter iteracyjny i nie są z natury sekwencyjne. Do

[72] Organizacje powinny zapoznać się z treścią załącznika F, aby wdrożyć niniejsze rekomendacje.

wykonywania czynności w tym samym czasie mogą być zobowiązane różne osoby, w zależności od konkretnej potrzeby lub sytuacji. Podmioty dysponują znaczną elastycznością w zakresie sposobu przeprowadzania etapów zarządzania ryzykiem (np. sekwencji, stopnia rygoru, formalności i dokładności stosowania) oraz sposobu dokumentacji i udostępniania wyników każdego etapu zarówno wewnątrz, jak i na zewnątrz. Wyniki z danego etapu procesu zarządzania ryzykiem będą miały bezpośredni wpływ na jeden lub więcej innych etapów zarządzania ryzykiem w procesie.

Rysunek G-2 podsumowuje działania C-SCRM w całym procesie zarządzania ryzykiem w miarę ich realizacji w ramach trzech poziomów ram ryzyka. Strzałki pomiędzy poszczególnymi etapami procesu zarządzania ryzykiem obrazują jednoczesny przepływ informacji i wytycznych pomiędzy tymi etapami.

Łącznie strzałki wskazują na to, że wszystkie dane wejściowe, czynności oraz rezultaty są w ciągłej interakcji i wpływają na siebie nawzajem. Więcej szczegółów znajduje się w kolejnych podrozdziałach.



Rysunek G-2: Działania związane z C-SCRM w procesie zarządzania ryzykiem

Rysunek G-2 przedstawia wzajemne powiązania między etapami procesu zarządzania ryzykiem, w tym kolejność, w jakiej można przeprowadzić poszczególne analizy oraz interakcje wymagane do zapewnienia, że analiza obejmuje różne dane wejściowe na poziomie podmiotu, misji i procesów biznesowych, a także operacji.

Pozostała część niniejszej sekcji zawiera szczegółowy opis działań C-SCRM w ramach czterech etapów procesu zarządzania ryzykiem. Struktura poszczególnych podrozdziałów poświęconych kolejnym etapom odnosi się do struktury rozdziałów 3.1 - 3.4 dokumentu [NSC 800-39]. W przypadku każdego etapu procesu zarządzanie ryzykiem struktura obejmuje dane wejściowe i warunki wstępne, działania oraz rezultaty i warunki. Działania dzielą się na zadania, zgodnie z dokumentem [NSC 800-39]. Dokument [NSC800-161] określa kroki oraz zadania procesu zarządzania ryzykiem, jednak nie powiela treści zawartych w dokumencie [NSC 800-39] – zamiast tego opisuje rekomendacje dotyczące obszaru C-SCRM oraz wszystkie powiązane

z nimi informacje, zadania i rezultaty. Dokument określa jedno zadanie, które uzupełnia listę zadań podanych w dokumencie [NSC 800-39] w ramach etapu oceny ryzyka: Zadanie 2-0, *Analiza krytyczności*.

ODBIORCY DOCELOWI

Docelowymi odbiorcami treści niniejszego załącznika są osoby odpowiedzialne za obszar C-SCRM, w szczególności za realizację procesu zarządzania ryzykiem w łańcuchu dostaw na każdym poziomie. Przykłady obejmują pracowników odpowiedzialnych za procesy i funkcje odpowiedzialnych za określanie ram i metodologii wykorzystywanych przez resztę podmiotu (np. procesów biura zarządzania programem C-SCRM, zarządzania ryzykiem w podmiocie itd.) Inni pracownicy lub inne podmioty mogą korzystać z tych wskazówek w razie potrzeby.

ZARZĄDZANIE RYZYKIEM W SKALI CAŁEGO PODMIOTU ORAZ RAMY ZARZĄDZANIA RYZYKIEM

Zarządzanie ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw wymaga zgodnych i celowych działań podmiotów na wszystkich poziomach: podmiotu, misji i procesów biznesowych oraz operacyjnym. Niniejszy dokument opisuje dwa różne, lecz wzajemnie uzupełniające się podejścia do zarządzania ryzykiem, które są iteracyjnie łączone w celu umożliwienia skutecznego zarządzania ryzykiem na trzech poziomach.

Pierwsze podejście jest określane skrótowo mianem FARM (ang. *Frame*, *Assess*, *Respond*, *and Monitor*) i składa się z czterech etapów: Określania ram ryzyka (F), Oceny ryzyka (A), Reakcji na ryzyko (R) oraz Monitorowania ryzyka (M). Proces FARM jest wykorzystywany przede wszystkim na poziomach 1 i 2 w celu ustalenia kontekstu ryzyka podmiotu oraz narażenia na ryzyko. Kontekst ryzyka ustalony na poziomach 1 i 2 wpływa na działania realizowane w ramach drugiego podejścia opisanego w dokumencie [NSC 800-37], czyli ram zarządzania ryzykiem. Ramy zarządzania ryzykiem są stosowane głównie na poziomie 3[73] - poziomie operacyjnym. W skład ram zarządzania ryzykiem wchodzi siedem etapów

[73] Proces ram zarządzania ryzykiem ma zastosowanie na poziomach 1 i 2, takie jak identyfikacja zabezpieczeń wspólnych.

procesu: Przygotowanie, Kategoryzacja, Wybór, Wdrożenie, Ocena, Autoryzacja i Monitorowanie. W ramach procesu ram zarządzania ryzykiem, dane z procesu FARM na poziomach 1 i 2 są wykorzystywane w ramach etapu przygotowania, a następnie stosowane, dostosowywane i aktualizowane na każdym kolejnym etapie procesu. Założenia dokonane na poziomach 1 i 2 są następnie iteracyjnie dostosowywane i dopasowywane do konkretnego poziomu operacyjnego lub kontekstu działań związanych z zamówieniami i zaopatrzeniem. Na przykład podmiot może podjąć decyzję o strategicznych priorytetach i zagrożeniach na poziomie 1 wpływając na określenie krytyczności misji i procesów biznesowych na poziomie 2, które z kolei wpływają na kategoryzację systemu, wybór zabezpieczeń i wdrożenie zabezpieczeń w ramach procesu ram zarządzania ryzykiem na poziomie 3 (operacyjnym). Przepływ informacji pomiędzy poziomami jest dwukierunkowy, przy czym dane wyjściowe procesu ram zarządzania ryzykiem na poziomie 3 służą do okresowego aktualizowania i udoskonalania założeń przyjętych na poziomach 1 i 2.

OKREŚLANIE RAM RYZYKA

Dane wejściowe i warunki wstępne

Określanie ram ryzyka jest krokiem, który ustanawia kontekst dla działań dotyczących obszaru C-SCRM na wszystkich trzech poziomach. Na tym etapie określa się zakres i strukturę łańcucha dostaw podmiotu, ogólną strategię zarządzania ryzykiem, konkretne strategie i plany podmiotu oraz misji i procesów biznesowych, a także poszczególne systemy informacyjne. Dane i informacje zebrane podczas procesu określania ram ryzyka stanowią dane wejściowe do planowania i dostosowywania działań C-SCRM w innych etapach procesu zarządzania ryzykiem na wszystkich trzech poziomach. Etap określania ram ryzyka jest także etapem, w którym w ramach strategii zarządzania ryzykiem na poziomie podmiotu, misji i procesów biznesowych ustanawia się wytyczne w postaci ram i metodologii.

Te ramy i metodologie zapewniają granice, normy oraz kierunki działań związanych z zarządzaniem ryzykiem w łańcuchu dostaw, które są realizowane w ramach późniejszych etapów.

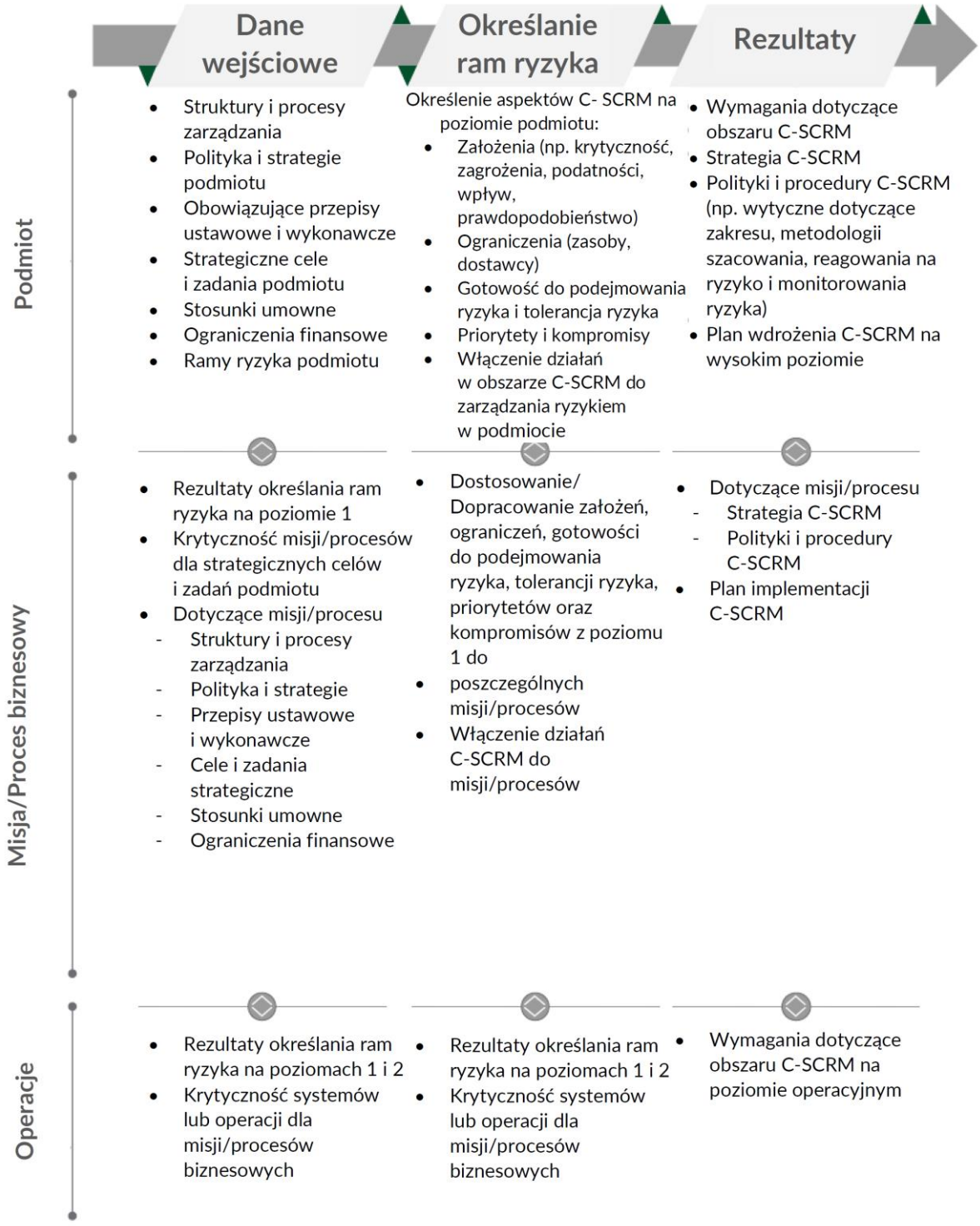
Dokument [NSC 800-39] definiuje określanie ram ryzyka jako „zbiór założeń, ograniczeń, tolerancji na ryzyko oraz priorytetów/wyborów, które kształtują podejście podmiotu do zarządzania ryzykiem". Działania związane z opracowywaniem ram ryzyka w skali całego podmiotu i C-SCRM powinny wpływać na siebie nawzajem. Założenia, które podmiot przyjmuje w odniesieniu do ryzyka, powinny wpływać na określanie ram ryzyka w ramach działań związanych z obszarem C-SCRM. W miarę jak założenia podmiotu dotyczące cyberryzyka w całym łańcuchu dostaw zmieniają się w wyniku realizacji działań C-SCRM, założenia te powinny wypływać na sposób określania ram ryzyka na poziomie podmiotu (np. poziom narażenia na ryzyko w związku ze współpracą z poszczególnymi dostawcami). Dane wejściowe do procesu określania ram ryzyka związanego z obszarem C-SCRM obejmują m.in.:

- polityki, strategie i ramy zarządzania podmiotu;
- obowiązujące przepisy ustawowe i wykonawcze;
- kluczowych dostawców organizacji oraz wykonawców,
- procesy podmiotu (dotyczących bezpieczeństwa, jakości, itp.);
- zagrożenia dla podmiotu, podatności, ryzyko i tolerancję na ryzyko;
- architekturę korporacyjną;
- cele i zadania na poziomie misji;
- poziom krytyczności misji/procesów;
- polityki bezpieczeństwa na poziomie misji;
- wymagania funkcjonalne;
- krytyczność dostarczonych komponentów systemu/produktu;
- wymagania bezpieczeństwa.

Opracowywanie ram ryzyka związanego z obszarem C-SCRM jest procesem iteracyjnym, który wykorzystuje jako dane wejściowe również dane z innych etapów procesów zarządzania ryzykiem. Rysunek D-3 przedstawia etap określania ram ryzyka oraz jego dane wejściowe i rezultaty na trzech poziomach. Na poziomie podmiotu

działania skupia się na określeniu warunków (tj. założeń, ograniczeń, apetytu na ryzyko, tolerancji ryzyka oraz priorytetów i kompromisów), które mają szerokie zastosowanie w całym podmiocie. Celem tego procesu jest kontekstualizacja ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw w odniesieniu do podmiotu oraz jego strategicznych celów i zadań. Na poziomie 2 działania koncentrują się na dostosowaniu ram ryzyka do poszczególnych misji i procesów biznesowych (np. założenia dotyczące roli usługodawcy w realizacji misji lub celów biznesowych).

Z kolei na poziomie 3, warunki określone na poziomach 1 i 2 wpływają na kolejne kroki procesu ram zarządzania ryzykiem. Począwszy od etapu przygotowania, warunki przedstawione na poziomie 1 i 2 są wykorzystywane do ustanowienia kontekstu i priorytetów zarządzania ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw w odniesieniu do poszczególnych systemów informacyjnych, komponentów systemów i dostawców usług systemowych. Z każdym kolejnym etapem procesu ram zarządzania ryzykiem (od kategoryzacji do monitorowania) założenia te są aktualizowane i dostosowywane tak, aby odnosiły się do konkretnych zagadnień na poziomie operacyjnym. Przepływ informacji musi odbywać się dwukierunkowo pomiędzy poziomami, ponieważ ustalenia i wnioski z działań na niższych poziomach mogą wpływać na warunki na wyższych poziomach.



Rysunek G-3: Działania dotyczące obszaru C-SCRM na etapie określania ram ryzyka

Rysunek G-3 do G-6 przedstawiają dane wejściowe, działania oraz rezultaty etapu określania ram ryzyka na trzech poziomach ramowego systemu zarządzania ryzykiem. Duże strzałki po lewej i prawej stronie działań przedstawiają dane wejściowe

Tłumaczenie

i rezultaty wpływające na inne etapy procesu zarządzania ryzykiem. Dane wejściowe dla tego etapu obejmują rezultaty innych etapów oraz proces zarządzania ryzykiem w podmiocie, które wpływają na procesy C-SCRM. Strzałki w górę i w dół pomiędzy poziomami obrazują przepływ informacji i wytycznych z poziomów wyższych do niższych oraz przepływ informacji zwrotnych z niższych poziomów. Łącznie strzałki wskazują na to, że wszystkie dane wejściowe, czynności oraz rezultaty są w ciągłej interakcji i wpływają na siebie nawzajem.

Ponieważ etap określania ram ryzyka jest wykorzystywany do określenia warunków, podmioty mogą uznać, że działania w ramach tego etapu są realizowane stosunkowo rzadziej niż pozostałe etapy procesu FARM. Podmioty mogą ponownie przeprowadzić działania w ramach tego etapu z określoną częstotliwością (np. raz w roku lub raz na dwa lata), w oparciu o zdefiniowane czynniki (np. zmiany biznesowe bądź nowe informacje z innych poziomów).

Działania

ZAŁOŻENIA DOTYCZĄCE RYZYKA

ZADANIE 1-1: Określenie założeń, które wpływają na sposób oceny, reagowania i monitorowania ryzyka w podmiocie.

Wytyczne uzupełniające

W ramach określania założeń dotyczących ryzyka w ramach procesu zarządzania ryzykiem (opisanego w dokumencie [NSC 800-39]) podmioty powinny wykonać następujące czynności:

- Opracować polityki C-SCRM podmiotu.
- Określić, które misje i procesy biznesowe oraz związane z nimi składniki są kluczowe dla podmiotu w celu określenia *krytyczności*.
- Określić, które misje i procesy biznesowe oraz systemy informacyjne składają się na łańcuch dostaw, uwzględniając odpowiednie usługi i produkty komercyjne.
- Ustalić priorytety w zakresie stosowania metod redukcji ryzyka w odniesieniu do tych elementów krytycznych, z uwzględnieniem czynników takich jak kwestie

bezpieczeństwa narodowego i wewnętrznego, poziomy wpływu na podstawie dokumentu NSC 199, zakres stosowania lub współzależności z innymi krytycznymi procesami i zasobami.

- Określić, scharakteryzować oraz podać reprezentatywne przykłady *źródeł zagrożeń*, *podatności*, *konsekwencji/wpływu* i *prawdopodobieństwa* zdarzeń związanych z łańcuchem dostaw.
- Określić misje C-SCRM, wymagania biznesowe i operacyjne.
- Dokonać wyboru odpowiednich metodologii oceny, w zależności od ładu korporacyjnego, kultury oraz różnorodności misji i procesów biznesowych.
- Ustanowić metody włączania wyników działań w zakresie C-SCRM do ogólnego procesu zarządzania ryzykiem w organizacji.
- Dokonywać okresowych przeglądów łańcucha dostaw w celu zapewnienia, że określone informacje pozostają aktualne w miarę zachodzących z czasem zmian.

Te założenia C-SCRM powinny być dostosowane w miarę możliwości do szerszych założeń dotyczących ryzyka, określonych w ramach programu zarządzania ryzykiem podmiotu. Kluczowym obowiązkiem dotyczącym obszaru C-SCRM (realizowanym na przykład przez biuro zarządzania programem C-SCRM) jest określenie, które z tych założeń mają zastosowanie do kontekstu C-SCRM na każdym kolejnym poziomie ram zarządzania ryzykiem. Jeżeli i kiedy zostaną zidentyfikowane nowe założenia dotyczące ryzyka (w ramach zadania 1-1), powinny one zostać dostarczone jako aktualizacje wszelkich odpowiadających im założeń dotyczących ryzyka podmiotu (ustalone w ramach zadania 1-1 procesu zarządzania ryzykiem podmiotu).

Krytyczność

Procesy krytyczne to takie, których zakłócenie, naruszenie lub wyłączenie spowodują przerwanie realizacji lub niepowodzenie misji. Procesy o znaczeniu krytycznym są zależne od systemów wspierających, które z kolei zależą od krytycznych komponentów tych systemów (np. sprzętu, oprogramowania i oprogramowania układowego). Procesy o znaczeniu krytycznym zależą również od informacji i procesów (realizowanych przez rozwiązania oraz pracowników, w tym w niektórych przypadkach wykonawców usług wsparcia). Za krytyczne należy również uznać te komponenty i procesy, które stanowią podstawę i umożliwiają realizację procesów o znaczeniu krytycznym lub stanowią zabezpieczenia wspólne (takie jak kontrola dostępu, zarządzanie tożsamością i kryptografia) oraz bezpośredni dostęp (np. zasilanie). Analiza krytyczności jest podstawową metodą, dzięki której procesy o znaczeniu krytycznym, powiązane systemy/komponenty oraz infrastruktura wspomagająca i usługi wspierające są określane wraz z odpowiednimi priorytetami. Analiza krytyczności obejmuje również analizę kluczowych dostawców, których może nie obejmować wewnętrzna analiza krytyczności (np. w zakresie współzależności w łańcuchu dostaw obejmujących dostawców podrzędnych).

Podmioty mogą dokonywać analiz krytyczności w ramach działań związanych z zarządzaniem ryzykiem podmiotu w oparciu o proces przedstawiony w dokumencie [NISTIR 8179][74]. Tam, gdzie to możliwe, działania związane z C-SCRM powinny wykorzystywać te założenia i dostosować je w celu uwzględnienia stosownego kontekstu. Dostosowanie krytyczności w ramach procesów związanych z C-SCRM obejmują wstępną analizę krytyczności poszczególnych projektów, produktów i procesów w łańcuchu dostaw w odniesieniu do procesów krytycznych na każdym poziomie. Na przykład na poziomie 1 podmiot może określić krytyczność holistycznych relacji z dostawcami dla ogólnych celów strategicznych podmiotu. Następnie na poziomie 2 podmiot może ocenić krytyczność poszczególnych dostawców, produktów i usług dla konkretnych misji i procesów biznesowych oraz

[74] Patrz NISTIR 8179, *Criticality Analysis Process Model: Prioritizing Systems and Components*.

celów strategicznych/operacyjnych. Na poziomie 3 podmiot może ocenić krytyczność dostarczonego produktu lub usługi dla określonych celów stanu operacyjnego systemów informacyjnych.

Podmioty mogą rozpocząć proces od identyfikacji kluczowych produktów lub usług dostarczanych przez dostawców, który przyczynia się do funkcjonowania i wpływa na odporność procesów i systemów podmiotu. Niektóre z tych elementów mogą być ustalone lub określone jako część planów zapewniania kontynuacji operacji po awarii. Określenie krytyczności może być oparte na roli każdego dostawcy, produktu lub usługi w realizacji wymaganego celu strategicznego lub operacyjnego procesu lub systemu. Wymagania, architektura i projekt wpływają na analizę i pomagają w określeniu minimalnego zestawu produktów i usług dostarczanych przez dostawcę, wymaganych dla prowadzenia działalności na poziomie podmiotu, misji i procesu biznesowego oraz operacyjnym. Analiza łączy odgórne i oddolne podejścia analityczne. Podejście odgórne w tym modelu umożliwia podmiotowi identyfikację krytycznych procesów, a następnie stopniowe zawężenie analizy do krytycznych systemów, które wspierają te procesy oraz krytycznych komponentów, które wspierają krytyczne funkcje tych systemów. Podejście oddolne pozwala na stopniowe prześledzenie wpływu, jaki nieprawidłowe działanie, kompromitacja lub niedostępność krytycznego komponentu miałaby na system, a w konsekwencji na powiązaną misję i proces biznesowy.

Podmioty, które przeprowadzają tę analizę, powinny uwzględnić zależności od systemu organizacyjnego i cyberbezpieczeństwa w łańcuchu dostaw, w tym kluczowych poddostawców. Na przykład podmiot może być narażony na ryzyko związane z cyberbezpieczeństwem, które wynika ze współpracy dostawcy z wybranym poddostawcą.

Określanie krytyczności jest procesem iteracyjnym, wykonywanym na wszystkich poziomach podczas określania ram ryzyka i jego oceny. Oczekuje się, że w procesie określania ram ryzyka podmiot określi krytyczność na wysokim poziomie z wykorzystaniem dostępnych informacji, a dodatkowe informacje zostaną uwzględnione na etapie oceny. Określenie krytyczności może obejmować następujące elementy:

- Zdefiniowanie procedur analizy krytyczności w celu zapewnienia, że istnieje zestaw udokumentowanych procedur wpływających na analizę krytyczności podmiotu na wszystkich poziomach.
- Przeprowadzenie analizy krytyczności na poziomie podmiotu i misji w celu określenia i ustalenia priorytetów w zakresie celów, zadań i wymagań podmiotu i misji.
- Przeprowadzenie analizy krytyczności na poziomie operacyjnym (tj. systemów i podsystemów) w celu zidentyfikowania i ustalenia priorytetów dotyczących kluczowych przepływów pracy, funkcjonalności systemu i możliwości.
- Przeprowadzenie analizy krytyczności na poziomie komponentów systemu i podsystemu w celu zidentyfikowania i ustalenia priorytetów dotyczących kluczowych elementów systemu i podsystemu (np. produktów komercyjnych).
- Przeprowadzenie szczegółowego przeglądu (np. analizy oddolnej) wpływów i interakcji między podmiotem, misją, systemem/podsystemami oraz komponentami w celu zapewnienia interakcji i współpracy między procesami.

Biorąc pod uwagę potencjalny wpływ, jaki zdarzenie w łańcuchu dostaw może mieć na działalność organizacji, jej aktywa oraz na partnerów biznesowych lub klientów, ważne jest, aby organizacje upewniły się, że oprócz krytyczności, kwestie istotności zostały włączone do ich strategii zarządzania ryzykiem w łańcuchu dostaw, praktyk oceny ryzyka oraz ogólnego zarządzania ryzykiem w łańcuchu dostaw. W odróżnieniu od krytyczności, w przypadku istotności bierze się pod uwagę, czy dana informacja zostałaby uznana przez rozsądnego inwestora podejmującego decyzję inwestycyjną za istotnie zmieniającą całokształt informacji dostępnych dla akcjonariusza[75].
Przewodniki SEC[76] stanowią:

> „... istotność ryzyka i incydentów związanych z cyberbezpieczeństwem zależy również od zakresu szkód, jakie takie incydenty mogą spowodować. Obejmuje on między innymi uszczerbek na reputacji organizacji, wpływ na wyniki

[75] Szczegółowa definicja znajduje się w glosariuszu.

[76] SEC – skrót od „security" (bezpieczeństwo).

finansowe oraz relacje z klientami i sprzedawcami, a także ryzyko sporów sądowych lub dochodzeń, działań regulacyjnych podejmowanych przez organy rządowe oraz organy innych państw".

Krytyczność może być określona dla istniejących systemów lub dla przyszłych inwestycji, działań rozwojowych lub integracyjnych w oparciu o architekturę i projekt systemu. Jest to działanie iteracyjne, które należy wykonać, gdy na etapie monitorowania ryzyka zostanie zauważona zmiana uzasadniają takie działanie.

Źródła zagrożeń

W przypadku obszaru C-SCRM źródła zagrożeń obejmują 1) zagrożenia ze strony przeciwników, takie jak cyberataki lub ataki fizyczne na łańcuch dostaw lub komponenty systemu informacyjnego przechodzące przez łańcuch dostaw; 2) przypadkowe błędy ludzkie; 3) awarie strukturalne, w tym awarie sprzętu, zabezpieczenia środowiskowe oraz wyczerpanie zasobów; oraz 4) zagrożenia środowiskowe, takie jak problemy geopolityczne, pandemie, kryzysy gospodarcze, a także katastrofy naturalne lub spowodowane przez człowieka. W odniesieniu do zagrożeń agresywnych, dokument [NSC 800-39] stwierdza, że podmioty powinny przedstawić zwięzłą charakterystykę rodzajów taktyk, technik i procedur stosowanych przez przeciwników, które mają być objęte zabezpieczeniami i środkami zaradczymi realizowanymi na poziomie 1 (podmiotu), poziomie 2 (misji i procesów biznesowych) oraz na poziomie 3 (systemu informacyjnego/usług), wyraźnie określając rodzaje źródeł zagrożeń, które mają być uwzględnione, oraz źródła zagrożeń, które nie są uwzględnione przez zabezpieczenia i środki przeciwdziałania.

Informacje o zagrożeniach mogą obejmować między innymi historyczne dane o zagrożeniach, faktyczne dane o zagrożeniach lub dane o zagrożeniach dotyczące podmiotów gospodarczych (np. dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych i innych usługodawców związanych z ICT/OT) lub dane o zagrożeniach dotyczące technologii. Informacje o zagrożeniach mogą pochodzić z wielu źródeł, w tym ze źródeł wywiadowczych) oraz z otwartych źródeł, takich jak publikacje informacyjne i handlowe, partnerzy, dostawcy i klienci.

W stosownych przypadkach podmioty mogą polegać na Agencji Wymiany Informacji (*ang. Information Sharing Agency - ISA*) Federalnej Rady Bezpieczeństwa Zamówień (*ang. Federal Acquisition Security Council - FASC*) w zakresie informacji o zagrożeniach dla łańcucha dostaw w dodatku do wyżej wymienionych źródeł. Ponieważ informacje o zagrożeniach mogą obejmować informacje niejawne, kluczowe znaczenie ma posiadanie przez organizacje możliwości przetwarzania informacji niejawnych. Informacje o zagrożeniach uzyskane w ramach tego etapu procesu powinny zostać wykorzystane do udokumentowania założeń podmiotu dotyczących warunków zagrożenia w oparciu o cechy wewnętrzne i zewnętrzne. Podczas etapu oceny, do oceny ryzyka wprowadza się aktualne informacje o zagrożeniach, aby uwzględnić krótkoterminowe zmiany warunków zagrożenia (np. ze względu na okoliczności geopolityczne), które mogą wpłynąć na decyzje podejmowane w sprawie zamówienia produktu lub usługi.

Informacje o łańcuchu dostaw (takie jak mapy łańcucha dostaw) zapewniają kontekst dla identyfikacji możliwych lokalizacji lub punktów dostępu źródeł zagrożeń wpływających na łańcuch dostaw. Zagrożenia związane z cyberbezpieczeństwem łańcucha dostaw są podobne do zagrożeń bezpieczeństwa informacji, takich jak katastrofy, atakujący czy szpiedzy przemysłowi. W tabeli G-1 wymieniono przykłady czynników zagrażających cyberbezpieczeństwu łańcucha dostaw. Załącznik G obejmuje plany reakcji na ryzyko z przykładami źródeł i czynników zagrożeń dla łańcucha dostaw wymienionych w Tabeli G-1.

Tabela G-1: Przykłady źródeł i czynników zagrożeń dla cyberbezpieczeństwa w łańcuchu dostaw

Źródła zagrożeń	Zagrożenie	Przykłady
Złośliwe: Producenci podróbek	Podróbki wprowadzone do łańcucha dostaw (patrz Załącznik B, Scenariusz 1)	Grupy przestępcze starają się pozyskiwać i sprzedawać podrobione komponenty w celu uzyskania korzyści pieniężnych. Zorganizowane grupy przestępcze poszukują zutylizowanych produktów, skupują nadwyżki

Źródła zagrożeń	Zagrożenie	Przykłady
		magazynowe i zdobywają dokumenty projektowe w celu uzyskania podzespołów przeznaczonych do sprzedaży nabywcom w szarej strefie[77].
Złośliwe: Złośliwi pracownicy	Utrata własności intelektualnej	Niezadowoleni pracownicy sprzedają lub przekazują własność intelektualną konkurentom lub zagranicznym agencjom wywiadowczym z różnych powodów, w tym ze względu na korzyści finansowe. Własność intelektualna obejmuje kod oprogramowania, projekty lub dokumentację.
Złośliwe: Wywiad zagraniczny	Dodanie złośliwego kodu (patrz Załącznik B, Scenariusz 4)	Obce wywiady chcą naruszyć łańcuch dostaw oraz dodać niechciane funkcjonalności (poprzez dodanie nowej lub modyfikację istniejącej funkcjonalności) do systemu w celu zebrania informacji lub naruszenia[78] systemu, a także wpłynięcia na misje realizowane przez system.
Złośliwe: Terroryści	Nieautoryzowany dostęp	Terroryści usiłują wniknąć do łańcucha dostaw lub zakłócić jego działanie poprzez dodawanie niepożądanych funkcjonalności w celu uzyskania informacji lub fizycznego wyłączenia i zniszczenia systemów w ramach łańcucha dostaw.

[77] Patrz dokument: [Defense Industrial Base Assessment: Counterfeit Electronics].

[78] Przykłady takich działań obejmują przejęcie kontroli nad podmiotem łańcucha dostaw lub przeprowadzenie ataku DoS w celu uniemożliwienia dostępu.

Źródła zagrożeń	Zagrożenie	Przykłady
Złośliwe: Szpiegostwo przemysłowe / Cyberprzestępcy	Szpiegostwo przemysłowe lub utrata własności intelektualnej (patrz Załącznik B, Scenariusz 2)	Szpiedzy przemysłowi lub cyberprzestępcy poszukują sposobów penetracji łańcucha dostaw w celu gromadzenia informacji lub zakłócenia działania systemu (np. poprzez wykorzystanie wykonawcy usług HVAC-*Heating, Ventilation, and Air Conditioning*) w celu kradzieży danych kart kredytowych).
Złośliwe: Zorganizowane grupy cyberprzestępcze	Naruszenie krytycznych procesów produkcyjnych przez oprogramowanie ransomware	Cyberprzestępcy przeprowadzają atak wykorzystujący oprogramowanie ransomware w celu uzyskania okupu oraz osiągnięcia korzyści finansowych. Źródła zagrożeń zdają sobie sprawę, że podmioty, zwłaszcza producenci, nie mogą pozwolić sobie na zatrzymanie produkcji.
Systemowe: Prawne/Regulacyjne	Komplikacje prawne lub regulacyjne wpływają na dostępność kluczowych produktów lub usług dostarczanych przez dostawców	Słabe przepisy antykorupcyjne, brak nadzoru regulacyjnego lub niedostateczne zabezpieczenie własności intelektualnej, zagrożenia wynikające z przepisów, polityk i praktyk w poszczególnych krajach, które osłabiają konkurencję i wolny rynek, w tym wymóg przekazywania technologii i własności intelektualnej dostawcom w obcym kraju[79].

[79] Information and Communications Technology Supply Chain Risk Management Task Force: Threat Evaluation Working Group (v3), August 2021, https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v3.pdf. Na potrzeby sprawozdania wykorzystano wersję dokumentu NIST SP 800-161 z 2015 roku.

Źródła zagrożeń	Zagrożenie	Przykłady
Systemowe: Ryzyko gospodarcze	Upadek kluczowego dostawcy prowadzi do przerwania łańcucha dostaw	Ryzyko gospodarcze wynika z zagrożeń dla płynności finansowej dostawców oraz potencjalnego wpływu na łańcuch dostaw z powodu upadku kluczowego dostawcy. Inne zagrożenia dla łańcucha dostaw, które skutkują ryzykiem gospodarczym, obejmują podatność na zmienność kosztów, zależność od dostaw z jednego źródła, koszty zmiany dostawców oraz ograniczenia wynikające z wielkości organizacji[80].
Systemowe: Przerwy w dostawach	Niedobory metali ziem rzadkich prowadzą do zakłóceń dostaw kluczowych półprzewodników	Różnorodne problemy strukturalne mogą powodować zakłócenia dostaw produktów i ich komponentów, zwłaszcza w przypadkach, gdy źródło dostaw znajduje się w jednej lokalizacji geograficznej.
Środowiskowe: Katastrofy naturalne	Klęska geopolityczna lub żywiołowa prowadzi do przerwania łańcucha dostaw	Dostępność kluczowych elementów w łańcuchu dostaw może zostać zaburzona w wyniku problemów geopolitycznych lub klęsk żywiołowych. Dzieje się tak zwłaszcza w przypadku, gdy dostawcy korzystają z usług jednego podmiotu.

[80] Information and Communications Technology Supply Chain Risk Management Task Force: Threat Evaluation Working Group (v3), August 2021, https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v3.pdf. Na potrzeby sprawozdania wykorzystano wersję dokumentu NIST SP 800-161 z 2015 roku.

Źródła zagrożeń	Zagrożenie	Przykłady
Strukturalne: Awaria sprzętu	Nieodpowiednie planowanie prowadzi do awarii platformy chmurowej	Usługa sprzedawcy lub dostawcy bez stosownych zabezpieczeń przepustowości może być narażona na awarię w przypadku nieoczekiwanych skoków zapotrzebowania na zasoby.
Przypadkowe: Niedbałość pracowników	Błąd konfiguracji prowadzi do narażenia danych	Pracownicy i wykonawcy mający dostęp do systemów informacyjnych mogą popełniać błędy, które mogą skutkować ujawnieniem danych wrażliwych. Ma to szczególne znaczenie w przypadkach, w których braki w szkoleniu lub luki w procesach zwiększają możliwości popełnienia błędów.

Podmioty mogą określać oraz rozwijać zagrożenia dotyczące obszaru C-SCRM na wszystkich trzech poziomach. W tabeli G-2 przedstawiono przykłady zagrożeń oraz różne metody charakteryzowania zagrożeń cyberbezpieczeństwa w łańcuchach dostaw na różnych poziomach.

Tabela G-2: Zagrożenia cyberbezpieczeństwa w łańcuchu dostaw

Poziom	Analiza zagrożeń	Metody
Poziom 1	• Działalność i misja podmiotu • Strategiczne relacje z dostawcami • Uwarunkowania geograficzne związane z wielkością łańcucha dostaw podmiotu	• Ustanowienie punktów wyjścia do identyfikacji zagrożeń związanych z cyberbezpieczeństwem w całym łańcuchu dostaw. • Ustanowienie procedur przeciwdziałania zagrożeniom dla całego podmiotu, takim jak wprowadzanie podróbek do krytycznych systemów i komponentów.

Poziom	Analiza zagrożeń	Metody
Poziom 2	• Misja i procesy biznesowe • Lokalizacja geograficzna • Rodzaje dostawców (np. komercyjni, dostawcy zewnętrznych usług, produkty na zamówienie) • Technologie stosowane w całym podmiocie	• Określenie dodatkowych źródeł informacji o zagrożeniach dotyczących misji podmiotu i procesów biznesowych. • Określenie potencjalnych źródeł zagrożeń na podstawie lokalizacji i dostawców w oparciu o dostępne informacje na temat cyberbezpieczeństwa w łańcuchu dostaw organizacji (np. z mapy łańcucha dostaw). • Określenie zakresu zidentyfikowanych źródeł zagrożeń dla konkretnych misji i procesów biznesowych z wykorzystaniem informacji o łańcuchu dostaw organizacji. • Ustanowienie procedur przygotowawczych w zakresie przeciwdziałania zagrożeniom oraz klęskom żywiołowym.
Poziom 3	• Cykl życia systemu	• Oparcie poziomu szczegółowości na zagrożeniach występujących w cyklu życia systemu. • Identyfikowanie i ustalanie źródeł zagrożeń w oparciu o potencjał wystąpienia zagrożeń w poszczególnych procesach cyklu życia systemu.

Podatności

Podatność to słabość systemu informacyjnego, procedur bezpieczeństwa systemu, zabezpieczeń wewnętrznych lub wdrożenia, która może zostać wykorzystana lub uruchomiona przez źródło zagrożenia [NSC 800-53]. W kontekście C-SCRM jest to każda słabość w łańcuchu dostaw, świadczonych usługach, projektowaniu systemu/komponentu, rozwoju, wytwarzaniu, produkcji, wysyłce i odbiorze, dostawie,

eksploatacji i utylizacji komponentu, która może być wykorzystana przez źródło zagrożenia. Definicja ta odnosi się do usług, systemów i komponentów opracowywanych i integrowanych w ramach cyklu życia systemu, a także do łańcucha dostaw, w tym do wszelkich środków i technik bezpieczeństwa, takich jak systemy zarządzania tożsamością lub kontroli dostępu.

Założenia dotyczące podatności dokonane w kroku określania ram ryzyka procesu FARM obejmują założenia podmiotu dotyczące podatności, które mogą zostać wykorzystane lub wywołane przez źródło zagrożenia. Na następnych etapach zostaną dopracowane i zaktualizowane, aby odzwierciedlić zmiany w czasie podczas etapu oceny. Podmioty mogą przyjmować założenia dotyczące podatności na zagrożenia związane z cyberbezpieczeństwem łańcucha dostaw. Dotyczą one:

- Podmiotów w samym łańcuchu dostaw (np. relacji z poszczególnymi dostawcami).
- Kluczowych usług świadczonych za pośrednictwem łańcucha dostaw, które wspierają krytyczną misję podmiotu i procesy biznesowe.
- Produktów, systemów i komponentów dostarczanych w ramach łańcucha dostaw i wykorzystywanych w ramach cyklu życia systemu.
- Środowisk rozwojowych i operacyjnych, które mają bezpośredni wpływ na cykl życia systemu.
- Środowisk logicznych i dostarczania, które transportują systemy oraz komponenty (logicznie lub fizycznie).

Podatności przejawiają się w różny sposób na każdym z trzech poziomów – podmiotu, misji oraz systemu informacyjnego. Na poziomie 1 podatności dotyczą całego podmiotu ze względu na struktury zarządcze i operacyjne (np. polityki, zarządzanie, procesy), warunki w łańcuchu dostaw (np. wykorzystanie produktów lub usług od jednego dostawcy) oraz cechy procesów podmiotu (np. korzystanie ze wspólnego systemu w krytycznych procesach). Na poziomie 2 podatności są specyficzne dla misji i procesu biznesowego i wynikają z jego struktur i warunków operacyjnych, takich jak zależność od określonego systemu, wkładu dostarczanego przez dostawcę lub usługi w celu osiągnięcia określonych celów operacyjnych misji i procesu biznesowego. Podatności poziomu 2 mogą się znacznie

różnić w zależności od misji i procesów biznesowych. W ramach poziomu 3 podatności przejawiają się jako braki lub słabości w dostarczanym produkcie, cyklu życia systemu, procedurach bezpieczeństwa systemu, kontrolach wewnętrznych, implementacjach systemu, danych wejściowych do systemu lub usługach dostarczanych poprzez łańcuch dostaw (takich jak komponenty systemu lub usługi).

Podmioty powinny określić metody określania podatności na cyberzagrożenia łańcucha dostaw, które są spójne z charakterystyką źródeł zagrożeń i zdarzeń oraz z ogólnym podejściem stosowanym przez podmiot do charakteryzowania podatności.

Podatności mogą dotyczyć pojedynczego źródła zagrożeń lub mieć szerokie zastosowanie w odniesieniu do wszystkich źródeł zagrożeń. Na przykład pojedynczy punkt awarii w sieci może dotyczyć zakłóceń spowodowanych przez zagrożenia środowiskowe (np. katastrofy) lub zagrożenia ze strony przeciwników (np. terrorystów). W Załączniku B przedstawiono przykłady zagrożeń cyberbezpieczeństwa łańcucha dostaw na podstawie dokumentu [NSC 800-30].

Wszystkie trzy poziomy powinny przyczynić się do określenia podejścia podmiotu do charakteryzowania podatności, zwiększając liczbę szczegółów zidentyfikowanych i udokumentowanych na niższych poziomach. Tabela G-3 obejmuje przykłady obszarów oraz różnych metod charakteryzowania podatności łańcucha dostaw na cyberzagrożenia na różnych poziomach.

Tabela G-3: Obszary podatności łańcucha dostaw na cyberzagrożenia

Poziom	Podatność	Metody
Poziom 1	• Misja i działalność podmiotu • Całość relacji z dostawcami (np. integratorzy systemów, rozwiązania komercyjne, usługi zewnętrzne)	• Badanie informacji dotyczących cyberbezpieczeństwa w łańcuchu dostaw, w tym map łańcucha dostaw w celu określenia szczególnie podatnych na zagrożenia podmiotów, lokalizacji lub składników. • Przeanalizowanie misji podmiotu pod kątem podatności na potencjalne zagrożenia dla łańcucha dostaw.

Poziom	Podatność	Metody
	• Uwarunkowania geograficzne związane z wielkością łańcucha dostaw podmiotu • Architektura korporacyjna i bezpieczeństwa • Krytyczność	• Zbadanie relacji i współzależności pomiędzy dostawcami i podmiotami zewnętrznymi pod kątem podatności na potencjalne luki w zabezpieczeniach łańcucha dostaw. • Przegląd architektury podmiotu i krytyczności, aby określić słabości, które wymagają dokładniejszych analiz na temat cyberbezpieczeństwa w łańcuchu dostaw.
Poziom 2	• Misja i procesy biznesowe • Lokalizacja geograficzna • Zależności od dostawców na poziomie misji i procesu (np. usługi zlecone) • Zastosowane technologie	• Dopracowanie analizy z poziomu 1 z myślą o określonych misjach i procesach biznesowych oraz informacjach o zagrożeniach i łańcuchu dostaw. • W razie potrzeby należy wykorzystać krajową bazę danych dotyczących podatności (NVD), Common Vulnerabilities and Exposures (CVE) i Common Vulnerability Scoring System (CVSS) lub inne metodologie w celu scharakteryzowania, skategoryzowania i oceny podatności[81]. • Należy uwzględnić wykorzystanie wytycznych dotyczących punktacji w celu nadania priorytetu podatnościom.
Poziom 3	• Poszczególne technologie, rozwiązania i usługi • Informacje na temat cyklu życia systemu łańcucha dostaw, obejmujące komponenty systemu lub usługi	• Dopracowanie analizy w oparciu o dane wejściowe dotyczące misji poziomu 2 i procesów biznesowych. • Wykorzystanie CVE, aby scharakteryzować i skategoryzować podatności, jeśli są dostępne. • Określenie słabych punktów.

[81] Patrz https://nvd.nist.gov/.

Wpływ i szkody

Pojęcie wpływu ryzyka odnosi się do wpływu utraty poufności, integralności lub dostępności informacji lub systemu na działania organizacyjne, aktywa organizacyjne, osoby fizyczne, inne organizacje lub naród – w tym interesy bezpieczeństwa narodowego. [NSC 800-53]. Wpływ szacowany w ramach etapu określania ram ryzyka stanowi długoterminowe założenia podmiotu dotyczące skutków, jakie różne zdarzenia związane z cyberbezpieczeństwem mogą mieć na jego podstawowe procesy. Założenia te są aktualizowane i dopracowywane w ramach etapu oceny, aby zapewnić, że istotne w danym momencie informacje (np. warunki rynkowe), które mogą zmienić zakres, czas trwania lub wielkość wpływu, zostaną odpowiednio uwzględnione w analizie.

Gdy jest to możliwe, podmioty powinny wykorzystywać przyjęte przez siebie założenia dotyczące konsekwencji i wpływu opracowane w ramach działań związanych z zarządzaniem ryzykiem w podmiocie. Przykładowo, jednym z takich działań jest przeprowadzenie analizy wpływu na działalność w celu określenia lub weryfikacji krytycznych procesów w ramach obowiązków podmiotu związanych z ciągłością i gotowością na wypadek awarii. Założenia te mogą jednak wymagać opracowania, jeśli jeszcze nie istnieją. Podmioty mogą utrzymywać dokumentację wpływu lub szkód, które zawierają stałe założenia dotyczące wpływu lub szkody różnych rodzajów zdarzeń związanych z cyberbezpieczeństwem (np. ujawnienie, zakłócenie, zniszczenie, modyfikacja) dotyczących zasobów podmiotu. Dokumentacja ta może podzielić wpływ i szkody na poszczególne rodzaje wpływu (np. operacyjne, środowiskowe, dotyczące bezpieczeństwa indywidualnego, reputacji, grzywien i kar, przywracania/wymiany rozwiązań, bezpośrednich szkód finansowych w sektorze infrastruktury krytycznej).

W przypadku C-SCRM podmioty powinny dopracować i zaktualizować swoje założenia dotyczące konsekwencji i wpływu, aby odzwierciedlić rolę, jaką dostępność, poufność i integralność produktów lub usług dostarczanych przez dostawców ma dla operacji podmiotu, jego aktywów i osób fizycznych. Na przykład, w zależności od jego krytyczności, utrata kluczowych materiałów lub usług dostarczanych przez dostawcę

może zmniejszyć zdolność operacyjną podmiotu lub całkowicie uniemożliwić jego działalność. W niniejszej publikacji wpływ lub szkoda są związane z podstawowymi celami podmiotu i wynikają z produktów lub usług przechodzących przez łańcuch dostaw lub samego łańcucha dostaw.

Konsekwencje i wpływ działań w zakresie C-SCRM będą charakteryzowały się różnymi przejawami na każdym z trzech poziomów hierarchii zarządzania ryzykiem. Określenie wpływu wymaga połączenia podejść odgórnego i oddolnego.
Tabela G-4 zawiera przykłady charakteryzowania konsekwencji i wpływu na różnych poziomach podmiotu.

Tabela G-4: Konsekwencje i wpływ cyberbezpieczeństwa w łańcuchu dostaw

Poziom	Wpływ	Metody
Poziom 1	• Ogólne założenia dotyczące wpływu na poziomie podmiotu • Krytyczność dostawcy (np. całościowe relacje z dostawcami)	• Zbadanie związków z poszczególnymi podmiotami w łańcuchu dostaw. • Dopracowanie analizy opracowanej na poziomie 2 w celu określenia łącznego wpływu na podstawową działalność podmiotu na poziomie 1 wynikającego ze zdarzeń związanych z cyberbezpieczeństwem w łańcuchu dostaw i realizowanym za jego pośrednictwem.
Poziom 2	• Znaczenie procesu w podstawowej działalności podmiotu • Krytyczność dostawcy dla misji/procesu	• Dla każdego rodzaju zdarzenia związanego z cyberbezpieczeństwem: • Dopracowanie analizy opracowanej na poziomie 3 w celu określenia łącznego wpływu na misję i proces biznesowy wynikającego ze zdarzeń związanych z cyberbezpieczeństwem w łańcuchu dostaw i realizowanych za jego pośrednictwem.

Poziom	Wpływ	Metody
		• Zbadanie sieci dostawców w celu zidentyfikowania skutków na poziomie biznesu/misji wynikających ze zdarzeń, które mają wpływ na poszczególne podmioty będące dostawcami.
Poziom 3	• Krytyczność procesów poziomu 2 • Krytyczność systemu • Krytyczność dostawcy dla funkcjonowania systemu (komponenty systemu i usługi)	• Określenie krytyczności systemu dla procesów bazowych poziomu 1 i 2. • Zbadanie krytyczności dostarczonych komponentów systemu lub usług dla działania systemu. • Zbadanie sieci dostawców w celu zidentyfikowania poszczególnych podmiotów, które mogą wpłynąć na dostępność krytycznych komponentów systemu lub usług.

Podmioty powinny sięgnąć do kilku źródeł informacji, które pomogą w określeniu kontekstu konsekwencji i wpływu. Preferowane są dane historyczne zbierane w ramach przeglądu danych organizacji, podobnych podmiotów, organizacji dostawców lub stosownych badań branżowych. W przypadku braków w danych historycznych należy rozważyć zwrócenie się o pomoc ekspertów oraz wykorzystanie wiedzy pracowników w całym podmiocie. Przeprowadzając rozmowy z ekspertami (np. osobami odpowiedzialnymi za technologię lub misję i procesy biznesowe) podmiot może dostosować założenia dotyczące wpływu, aby uwzględnić wyjątkowe warunki i zależności podmiotu. Dokument [NISTIR 8286] oferuje bardziej dogłębne omówienie sposobów stosowania różnych metod ilościowych i jakościowych do analizy ryzyka.

Poniżej przedstawiono przykłady konsekwencji i wpływu łańcucha dostaw związanych z cyberbezpieczeństwem:

- Trzęsienie ziemi w Malezji zmniejsza produkcję pamięci RAM trafiającej na rynek do 60% poprzedniej wartości, powodując problemy dotyczące utrzymania sprzętu i realizacji nowych projektów.

- Przypadkowe nabycie podrobionej części skutkuje przedwczesną awarią komponentu, co wpływa na realizację misji podmiotu.
- Przerwa u kluczowego dostawcy usług w chmurze skutkuje stratami z tytułu przestojów operacyjnych w wysokości 1,5 – 15 milionów dolarów.

Prawdopodobieństwo

W analizie ryzyka bezpieczeństwa informacji prawdopodobieństwo jest czynnikiem ważonym opartym na subiektywnej analizie prawdopodobieństwa, że dane zagrożenie będzie w stanie wykorzystać daną podatność [CNSSI 4009]. Ogólne założenia dotyczące prawdopodobieństwa powinny być oparte na procesie zarządzania ryzykiem w podmiocie i dopracowane w celu uwzględnienia implikacji dotyczących obszaru C-SCRM. Może się jednak okazać, że konieczne będzie opracowanie ogólnych założeń, jeśli jeszcze nie istnieją. Analiza prawdopodobieństwa w kroku określenia ram ryzyka pozwala na ustalenie założeń dotyczących względnego prawdopodobieństwa wystąpienia różnych niekorzystnych zdarzeń związanych z cyberbezpieczeństwem. Prawdopodobieństwo może ulegać zmianom w perspektywie krótkoterminowej w oparciu o warunki wewnętrzne i zewnętrzne, dlatego musi być aktualizowane i dopracowywane w ramach etapu oceny.

W przypadkach ataków określenie prawdopodobieństwa może być dokonane z wykorzystaniem danych wywiadowczych, danych historycznych oraz intuicji ekspertów w zakresie 1) zamiarów przeciwnika, 2) możliwości atakującego oraz 3) celu atakującego. W innych przypadkach (np. strukturalnych lub środowiskowych) oceny prawdopodobieństwa będą oparte na intuicji ekspertów i danych historycznych. Jeśli dane historyczne są dostępne, mogą pomóc w dalszym zmniejszeniu niepewności dotyczących prawdopodobieństwa wystąpienia zdarzeń związanych z cyberbezpieczeństwem w całym łańcuchu dostaw. Organizacje mogą znaleźć dane historyczne, sięgając do źródeł wewnętrznych, takich jak katalogi incydentów, a także źródeł zewnętrznych, w tym ISAC, w celu określenia przybliżonego prawdopodobieństwa wystąpienia różnych zdarzeń. Analiza prawdopodobieństwa może wykorzystywać wiele protokołów i metodologii użytych w poprzednim kroku. Podobnie jak w przypadku konsekwencji i wpływu, oceny prawdopodobieństwa mogą opierać się na metodach jakościowych lub ilościowych i korzystać z podobnych

technik. Aby zapewnić decydentom odpowiedni kontekst prawdopodobieństwa, podmiot powinien oszacować prawdopodobieństwo zdarzeń związanych z cyberbezpieczeństwem, które mogą mieć wpływ na łańcuch dostaw (np. prawdopodobieństwo w ciągu danego roku).

Analiza prawdopodobieństwa będzie przebiegać w różne sposoby na każdym z trzech poziomów. Tabela G-5 przedstawia niektóre aspekty oceny i metody odpowiednie dla każdego poziomu.

Tabela G-5: Obszary oceny prawdopodobieństwa zdarzeń związanych z cyberbezpieczeństwem w łańcuchu dostaw

Poziom	Prawdopodobieństwo	Metody
Poziom 1	• Ogólne założenia dotyczące zagrożeń i prawdopodobieństwa w kontekście podmiotu	• Analiza implikacji dotyczących krytycznej infrastruktury narodowej, które mogą zwiększyć narażenie podmiotu na atak.
	• Ustalenia dotyczące prawdopodobieństwa opracowane na poziomach 2 i 3. • Modele kontaktów z dostawcami, które wpływają na możliwość kontaktu ze źródłami zagrożeń	• Dopracowanie analiz z poziomów 2 i 3 w celu określenia łącznego narażenia na kontakt ze źródłami zagrożeń.
Poziom 2	• Założenia dotyczące zagrożeń i prawdopodobieństwa w kontekście misji/procesu • Model kontaktów z dostawcami na poziomie misji/procesu (np. krytyczność aktywów) • Ustalenia poziomu 3 dotyczące systemów	• Ocena warunków dotyczących misji i procesów biznesowych, które stwarzają możliwości kontaktu źródeł zagrożeń z procesami lub aktywami poprzez łańcuch dostaw. • Ocena warunków zagrożeń dotyczących łańcucha dostaw związanych z kluczowymi systemami związanymi z misją i procesami biznesowymi.

Poziom	Prawdopodobieństwo	Metody
Poziom 3	• Założenia dotyczące zagrożeń i prawdopodobieństw w kontekście systemów podmiotu • Atrakcyjność systemu i dostawcy dla napastników • Lokalizacja i warunki eksploatacji • Polityki, procesy i środki bezpieczeństwa dostawców i systemów • Rodzaj i stopień kontaktu dostawcy z systemem	• Analiza charakteru danych i materiałów przechodzących przez łańcuch dostaw i cykl życia systemu, które zmieniają prawdopodobieństwo kontaktu ze źródłem zagrożeń. • Ocena ról systemów w procesach poziomów 1 i 2, które zmieniają atrakcyjność dla napastników. • Analiza łańcucha dostaw pod kątem czynników, które mogą zwiększać prawdopodobieństwo ataku na system.

Podmioty powinny określić, jakie metody będą stosować w celu określenia prawdopodobieństwa naruszenia cyberbezpieczeństwa łańcucha dostaw, zgodnie z ogólnym podejściem stosowanym w procesie zarządzania ryzykiem. Podmioty powinny opracować odpowiednie procedury w celu dokładnego udokumentowania wszelkich założeń analizy ryzyka, które prowadzą do określenia narażenia na ryzyko, zwłaszcza w przypadku wysokiego lub krytycznego ryzyka. Wgląd w założenia może mieć kluczowe znaczenie dla umożliwienia decydentom podjęcia działań.

OGRANICZENIA PROCESU ZARZĄDZANIA RYZYKIEM

ZADANIE 1-2: Określenie ograniczeń[82] dotyczących prowadzenia oceny ryzyka, reagowania na ryzyko oraz monitorowania ryzyka w podmiocie.

Wytyczne uzupełniające

Należy określić następujące rodzaje ograniczeń, aby zapewnić, że proces zarządzania ryzykiem związanym z cyberbezpieczeństwem łańcucha dostaw jest połączony z procesem zarządzania ryzykiem podmiotu:

[82] Opis ograniczeń w kontekście zarządzania ryzykiem znajduje się w dokumencie [NSC 800-39] – Rozdział 3.1, Zadanie 1-2.

1. Ograniczenia ze strony podmiotu.
2. Ograniczenia dotyczące łańcucha dostaw.

Ograniczenia ze strony podmiotu stanowią podstawę polityki dotyczącej cyberbezpieczeństwa w łańcuchu dostaw na poziomie 1, wymogów dotyczących misji na poziomie 2 oraz wymogów dotyczących konkretnego systemu na poziomie 3. W Tabeli G-6 podano konkretne ograniczenia ze strony podmiotu i dotyczące cyberbezpieczeństwa w łańcuchu dostaw. Ograniczenia dotyczące łańcucha dostaw, takie jak polityka C-SCRM i wymagania C-SCRM, mogą wymagać opracowania, jeśli jeszcze nie istnieją.

Tabela G-6: Ograniczenia dotyczące łańcucha dostaw

Poziom	Ograniczenia ze strony podmiotu	Ograniczenia dotyczące łańcucha dostaw
Poziom 1	• Polityki, strategie i ramy zarządzania podmiotu • Obowiązujące przepisy ustawowe i wykonawcze • Misja i procesy biznesowe • Procesy podmiotu (dotyczących bezpieczeństwa, jakości, itp.) • Ograniczone zasoby	• Polityka podmiotu w zakresie C-SCRM oparta na istniejących politykach, strategiach i zarządzaniu podmiotu; obowiązujących przepisach i regulacjach; misji i procesach biznesowych; oraz procesach podmiotu • Przepisy i polityka w zakresie zamówień. • Dostępne, obowiązkowe lub ograniczone źródła dostaw lub produktów
Poziom 2	• Misja i procesy biznesowe • Krytyczność procesów • Architektura korporacyjna • Polityki bezpieczeństwa na poziomie misji	• Wymagania misji i procesów biznesowych w zakresie C-SCRM, które zostały włączone do misji i procesów biznesowych oraz architektury korporacyjnej • Umowy z dostawcami, gwarancje na produkty i umowy dotyczące odpowiedzialności

Poziom	Ograniczenia ze strony podmiotu	Ograniczenia dotyczące łańcucha dostaw
Poziom 3	• Wymagania funkcjonalne • Wymagania bezpieczeństwa	• Możliwości dotyczące obszaru C-SCRM na poziomie produktów i operacji • Dostarczane przez dostawcę gwarancje na elementy systemu i umowy serwisowe

Jedną z podstawowych metod wyrażania ograniczeń są zapisy polityki oraz dyrektywy. Polityka C-SCRM podmiotu jest kluczowym narzędziem służącym do zarządzania działaniami dotyczącymi obszaru C-SCRM. Powinna wynikać z obowiązujących przepisów prawa i regulacji i wspierać działania podmiotu, w tym zamówienia i zaopatrzenie, bezpieczeństwo informacji, zapewnianie jakości oraz łańcuch dostaw i logistykę. Polityka C-SCRM powinna odnosić się do celów, zadań i wymagań określonych w ogólnym planie strategicznym podmiotu, strategiach dotyczące misji i procesów biznesowych, a także przez klientów wewnętrznych lub zewnętrznych. Polityka C-SCRM powinna również określać punkty integracji działań związanych z obszarem C-SCRM z procesem zarządzania ryzykiem i cyklem życia systemu podmiotu.

Polityka C-SCRM powinna określać role i obowiązki zespołu C-SCRM oraz wszelkie zależności i interakcje pomiędzy tymi rolami. Role związane z C-SCRM będą obejmować obowiązki związane z gromadzeniem informacji o zagrożeniach dotyczących łańcucha dostaw, przeprowadzaniem ocen ryzyka, określaniem i wdrażaniem środków zaradczych oraz przeprowadzaniem procesów monitorowania. Określenie i potwierdzenie ról pomogą określić trudność wdrożenia planu C-SCRM. Przykładowe role związane z C-SCRM to:

- Biuro zarządzania programem C-SCRM, które opracowuje nadrzędne wytyczne dotyczące zarządzania ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw, które wpływają na decyzje dotyczące wyboru produktów w procesie projektowania systemu.
- Specjalista ds. zaopatrzenia i inżynier ds. konserwacji odpowiedzialni za identyfikację i wymianę wadliwego sprzętu.

- Specjaliści ds. odbioru, którzy weryfikują, czy składnik systemu może być włączony przez podmiot nabywający.
- Integrator systemu odpowiedzialny za utrzymanie i aktualizacje systemu, którego pracownicy pracują w siedzibie podmiotu i korzystają ze środowisk deweloperskich integratora systemu oraz infrastruktury operacyjnej jednostki nabywającej.
- Inżynier bezpieczeństwa systemu odpowiedzialny za zapewnienie, że kwestie bezpieczeństwa systemu informacyjnego są właściwie określane i uwzględniane w całym cyklu życia systemu.
- Użytkownik końcowy systemów, komponentów i usług.

Wymagania dotyczące obszaru C-SCRM powinny opierać się na politykach C-SCRM, misjach i procesach biznesowych, ocenach krytyczności na poziomie 2, a także wymaganiach w zakresie funkcjonalności i bezpieczeństwa na poziomie 3.

APETYT NA RYZYKO I TOLERANCJA RYZYKA

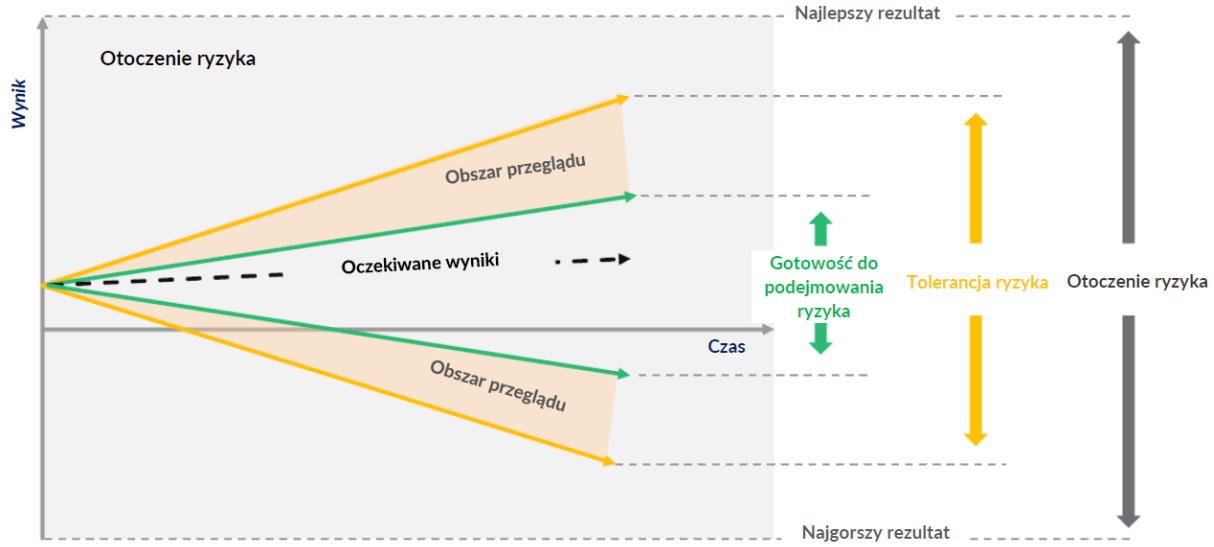
ZADANIE 1-3: Określenie poziomów apetytu na ryzyko i tolerancji ryzyka w podmiocie.

Wytyczne uzupełniające

Apetyt na ryzyko określa rodzaje i zakres ryzyka, który podmiot jest skłonny zaakceptować w dążeniu do osiągnięcia swojej wartości [NISTIR 8286]. Tolerancja ryzyka to z kolei gotowość podmiotu lub interesariuszy do ponoszenia ryzyka szczątkowego z myślą o realizacji celów, z uwzględnieniem, że na parametr ten mogą wpływać wymogi wymagania prawne lub rozporządzenia [NISTIR 8286]. Definicja tego terminu została zaadaptowana z dokumentu Committee of Sponsoring Organizations of the Treadway Commission (COSO), który stwierdza, że tolerancja ryzyka to akceptowalny poziom zmienności w kontekście realizacji określonego celu. Często tolerancję ryzyka najlepiej mierzyć w tych samych jednostkach, które służą do pomiaru związanego z nim celu. [COSO 2011] Podczas ustanawiania ram zarządzania ryzykiem zaleca się, aby podmioty tworzyły podsumowania gotowości na ryzyko i tolerancji ryzyka określające progi ryzyka. Następnie działania dotyczące obszaru

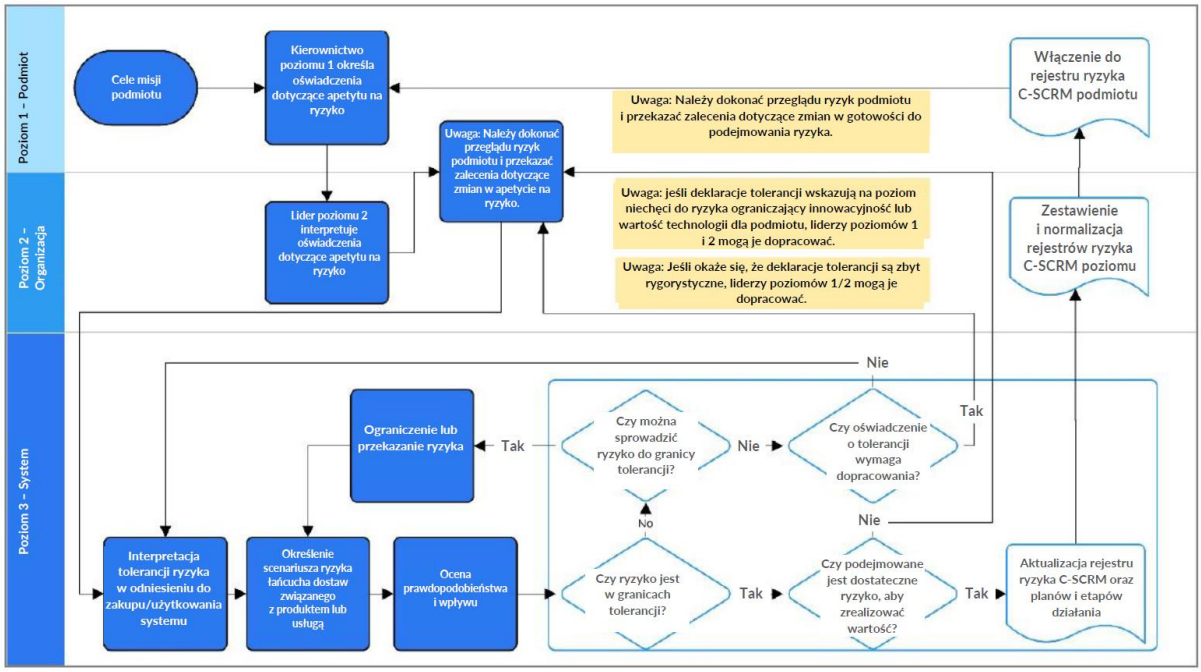
C-SCRM powinny być dostosowane do tych parametrów wynikających z procesu zarządzania ryzykiem w podmiocie. Raz ustalone parametry powinny być monitorowane i zmieniane w czasie. W kontekście C-SCRM parametry te powinny zostać ujęte w odpowiednich ramach, by wpływały na działania w tym obszarze. Osoby odpowiedzialne za C-SCRM w całym podmiocie powinny współpracować z liderami podmiotu i wspierać ich w opracowywaniu podsumowań obejmujących te dwa parametry w kontekście C-SCRM. Należy to zrobić zgodnie z kryteriami przewidzianymi w strategii ryzyka podmiotu (np. na podstawie kategorii ryzyka stosowanych przez podmiot).

Parametry te w znaczący sposób wpływają na decyzje dotyczące obszaru C-SCRM na wszystkich trzech poziomach. Niektóre podmioty mogą określać gotowość na ryzyko oraz tolerancję ryzyka w ramach szerszych działań związanych z zarządzaniem ryzykiem. W podmiotach, które nie określiły poziomu gotowości na ryzyko, interesariusze poziomu 1 powinni współpracować z kierownictwem podmiotu w celu zdefiniowania i wyrażenia tego parametru w kontekście działań w ramach programu C-SCRM. Podmioty obejmujące wiele organizacji mogą zdecydować się na dostosowanie tych parametrów do poszczególnych organizacji, misji i procesów biznesowych. Na poziomie 1 parametr ten może być ustalony w taki sposób, aby umożliwić podmiotowi realizację celów związanych z wartością (np. większa gotowość na ryzyko w związku z możliwością obniżenia kosztów prowadzenia działalności o 5%). Na poziomach 2 i 3 na deklarowaną gotowość na ryzyko wpływa tolerancja ryzyka. Na przykład organizacja charakteryzująca się niską gotowością na ryzyko związane z cyberbezpieczeństwem w łańcuchu dostaw może ustalić parametr tolerancji ryzyka wymagający dodatkowych zabezpieczeń ze strony decydentów poziomu 2 i 3 w dążeniu do osiągnięcia wartości strategicznej (np. oświadczenie o tolerancji ryzyka opracowane na podstawie ścisłych celów produkcyjnych w organizacji realizującej misję związaną z bezpieczeństwem narodowym).



Rysunek G-4: Gotowość do podejmowania ryzyka i tolerancja ryzyka

Parametry te stanowią łącznie oczekiwania i akceptowalne granice ryzyka w kontekście celów strategicznych organizacji. Rysunek G-4 ilustruje, jak gotowość do podejmowania ryzyka i tolerancja ryzyka mogą być wykorzystane przez decydentów organizacji jako wytyczne. Tolerancja ryzyka może obejmować granice wykraczające poza gotowość na jego podejmowanie, co pozwala zapewnić pewien stopień elastyczności z myślą o osiąganiu celów strategicznych organizacji. Decydenci powinni jednak dążyć do utrzymania się w granicach gotowości na podejmowanie ryzyka w normalnych warunkach i przekraczać te granice tylko wtedy, gdy jest to absolutnie niezbędne. Okresy wyników w *strefie przeglądu*, które leżą poza granicami gotowości na podejmowanie ryzyka, powinny spowodować przegląd decyzji operacyjnych oraz określenie nowych parametrów dotyczących ryzyka. Przegląd ten ma kluczowe znaczenie dla zapewnienia, że gotowość organizacji do podejmowania ryzyka pozostaje na odpowiednim poziomie i uwzględnia wewnętrzne i zewnętrzne warunki działania organizacji. Organizacja działająca np. podczas globalnej pandemii może uznać za konieczne zwiększenie poziomu ekspozycji na ryzyko związane z cyberbezpieczeństwem z myślą o poszukiwaniu alternatywnych dostawców w celu rozwiązania problemów braków towarów. Rysunek G-5 przedstawia ilustrację procesu przeglądu gotowości do podejmowania ryzyka i tolerancji ryzyka.



Rysunek G-5: Proces przeglądu apetytu na ryzyko i tolerancji ryzyka

W niektórych przypadkach liderzy organizacji mogą uznać za konieczną zmianę wytycznych, aby uniknąć nadmiernego unikania ryzyka lub nadmiernego poszukiwania ryzyka przez decydentów.

Tabela G-7 przedstawia dodatkowe przykłady współgrania obu parametrów w kontekście określania ram ryzyka w podmiocie.

Tabela G-7: Apetyt na ryzyko i tolerancja ryzyka w łańcuchu dostaw

Ograniczenia podmiotu	Ograniczenia dotyczące łańcucha dostaw
Niska gotowość do podejmowania ryzyka w odniesieniu do celów rynkowych i wymóg działania w reżimie czasowym 24/7.	**Niska tolerancja** (tj. prawdopodobieństwo nie większe niż 5%) przestojów u usługodawcy, które powodują przerwy w działaniu systemu przekraczające zapisy umów gwarancji świadczenia usług o więcej niż 10%
Niska gotowość do podejmowania ryzyka w odniesieniu do celów produkcyjnych, które wymagają > 99% terminowego dostarczania produktów klientom realizującym misje dotyczące bezpieczeństwa narodowego	**Tolerancja bliska zeru** (prawdopodobieństwo nie większe niż 5%) dla wystąpienia zakłóceń w łańcuchu dostaw, które powodują spadek poziomu produkcji poniżej 99% progu docelowego dla produktów wojskowych.

Ograniczenia podmiotu	Ograniczenia dotyczące łańcucha dostaw
Niska gotowość do podejmowania ryzyka związanego z celami bezpieczeństwa narodowego, które wymagają 99% skuteczności procesów bezpieczeństwa.	**Niska tolerancja** (tj. nie więcej niż 1%) dotycząca naruszeń zasad dostępu wykonawcy oraz przekroczeń dozwolonego czasu dostępu do systemów przetwarzających informacje niejawne o 10%
Umiarkowany apetyt na a ryzyko związane z celami operacyjnymi w obszarach innych niż kluczowe, które wymagają dostępności na poziomie 99,5%	**Umiarkowana tolerancja** (tj. prawdopodobieństwo nie większe niż 15%) dla awarii komponentów systemu powodujących przerwy w pracy systemu o znaczeniu niekrytycznym, które przekraczają cele dotyczące czasu przywracania sprawności o więcej niż 10%.

Aby zapewnić kierownictwu odpowiednie informacje przy podejmowaniu decyzji związanych z ryzykiem, podmioty powinny ustanowić wskaźniki, takie jak kluczowe wskaźniki efektywności (*ang. key performance indicators - KPI*), kluczowe wskaźniki ryzyka (*ang. key risk indicators – KRI*) służące do pomiaru rezultatów w odniesieniu do deklarowanej gotowości do podejmowania ryzyka i tolerancji ryzyka. Określenie odpowiednich źródeł danych powinno odgrywać kluczową rolę w zdefiniowanych przez podmiot procesach ustalania tych parametrów oraz ich dopracowywania. Parametry te powinny być traktowane przez podmiot jako dynamiczne. Wymaga to okresowych aktualizacji i zmian w oparciu o wewnętrzne (np. nowe przywództwo, strategia) i zewnętrzne (np. rynek, środowisko) czynniki wpływające na podmiot.

Podmioty powinny brać pod uwagę zagrożenia, podatności, ograniczenia i krytyczność cyberbezpieczeństwa łańcucha dostaw przy ustalaniu, operacjonalizacji i utrzymywaniu ogólnego poziomu gotowości do podejmowania ryzyka i tolerancji ryzyka[83].

[83] Struktury zarządzania podmiotów są bardzo zróżnicowane (patrz: [NSC 800-100, Rozdział 2.2.2]). Niezależnie od struktury zarządzania, indywidualne decyzje podmiotów dotyczące ryzyka powinny mieć zastosowanie do podmiotów i wszelkich organizacji podległych.

PRIORYTETY I KOMPROMISY

ZADANIE 1-4: Określenie priorytetów i kompromisów uwzględnianych przez podmiot w procesie zarządzania ryzykiem.

Wytyczne uzupełniające

Priorytety i kompromisy są ściśle związane z parametrami apetytu na ryzyko oraz tolerancji ryzyka, które informują o zakresie ryzyka, które jest dopuszczalne i tolerowane przez jednostkę przy realizacji jej celów. Priorytety przyjmują formę długoterminowych celów strategicznych lub krótkoterminowych założeń strategicznych, które wpływają na kalkulacje ryzyka. Priorytety i kompromisy stanowią kluczowy kontekst strategiczny działań w zakresie C-SCRM takich jak ocena alternatyw i podejmowanie decyzji dotyczących reagowania na ryzyko. W ramach określania priorytetów i kompromisów podmioty powinny rozważyć apetyt na ryzyko, tolerancję ryzyka, zagrożenia związane z cyberbezpieczeństwem w łańcuchu dostaw, podatności, ograniczenia i poziom krytyczności.

Rozważania dotyczące priorytetów i kompromisów będą różne na każdym z trzech poziomów. Na poziomie 1 priorytety i kompromisy mogą faworyzować istniejące relacje z dostawcami w poszczególnych regionach kosztem niższych kosztów nowych dostawców ze względu na chęć utrzymania zaufania i stabilności. Na poziomie 2 priorytety i kompromisy mogą sprzyjać scentralizowanym modelom zarządzania C-SCRM, które obejmują zespoły produktowe na rzecz większej standaryzacji praktyk bezpieczeństwa. Na poziomie 3 priorytety i kompromisy mogą faworyzować komponenty systemów wytwarzane w niektórych regionach geograficznych w celu uniknięcia zagrożeń środowiskowych lub geopolitycznych dla łańcucha dostaw.

Rezultaty i warunki końcowe

Dokument [NSC 800-39] określa strategię zarządzania ryzykiem jako rezultat procesu określania ram ryzyka, zakładający sposób oceny ryzyka, monitorowania go w czasie oraz reagowania na jego przejawy. Strategia ta powinna obejmować wszelkie określone aspekty C-SCRM i powinna skutkować ustanowieniem procesów dotyczących obszaru C-SCRM w całym podmiocie. Procesy te powinny być udokumentowane na jeden z trzech sposobów:

1. Włączone do istniejącej dokumentacji podmiotu.
2. Opisane w oddzielnym zestawie dokumentów, które dotyczą C-SCRM.
3. Wykorzystując połączenie oddzielnych i połączonych dokumentów w zależności od potrzeb i działań podmiotu.

Niezależnie od sposobu dokumentowania rezultatów, wynikiem etapu określania ram ryzyka powinny być następujące dokumenty:

- polityka C-SCRM;
- analiza krytyczności, w tym priorytetowe misje i procesy biznesowe oraz wpływ określany według dokumentu [FIPNSCS 199];
- metodyka i wytyczne oceny ryzyka dotyczącego cyberbezpieczeństwa w łańcuchu dostaw;
- wytyczne dotyczące reakcji na ryzyko związane z cyberbezpieczeństwem w łańcuchu dostaw;
- wytyczne dotyczące monitorowania ryzyka związanego z cyberbezpieczeństwem w łańcuchu dostaw;
- wymogi C-SCRM dotyczące misji oraz działalności;
- opracowane misje i procesy biznesowe oraz architektura korporacyjna z uwzględnieniem aspektów związanych z obszarem C-SCRM;
- wymagania dotyczące obszaru C-SCRM na poziomie operacyjnym;
- wytyczne/wymagania dotyczące bezpieczeństwa zamówień i zaopatrzenia.

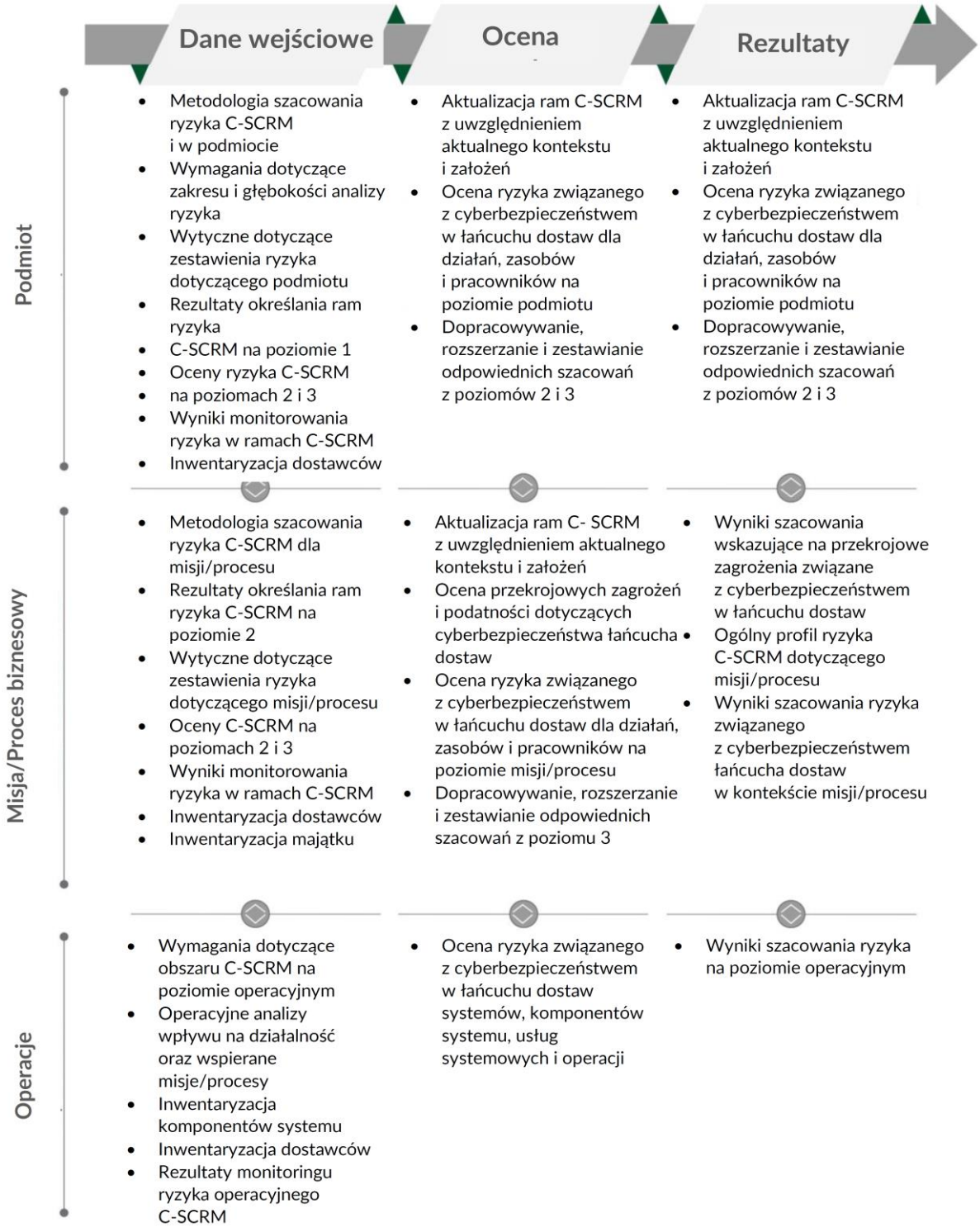
Rezultaty etapu określania ram ryzyka umożliwiają spełnienie warunków wstępnych do skutecznego zarządzania ryzykiem związanym z cyberbezpieczeństwem w całym łańcuchu dostaw i służą jako dane wejściowe do etapów oceny ryzyka, reagowania na ryzyko i monitorowania ryzyka.

OCENA RYZYKA

Dane wejściowe i warunki wstępne

Etap oceny ryzyka to etap, w którym założenia, ustalone metodologie i zebrane dane są wykorzystywane do przeprowadzenia oceny ryzyka. Liczne dane wejściowe (w tym analizy krytyczności czy parametry dotyczące gotowości do podejmowania ryzyka i tolerancji ryzyka, informacje na temat zagrożeń, analizy podatności, wiedza interesariuszy, polityki, ograniczenia i wymagania) są łączone i analizowane w celu oszacowania prawdopodobieństwa i wpływu naruszenia cyberbezpieczeństwa łańcucha dostaw. Działania w ramach etapu oceny są wykorzystywane do aktualizacji długoterminowych założeń podmiotu dotyczących ram ryzyka w celu uwzględnienia zmian w perspektywie krótkoterminowej.

Ocena ryzyka związanego z cyberbezpieczeństwem w łańcuchu dostaw powinna być połączona z ogólnym procesem oceny ryzyka w podmiocie. Wyniki oceny ryzyka związanego z obszarem C-SCRM powinny być wykorzystywane w celu informowania o potencjalnych lub rzeczywistych zagrożeniach dla cyberbezpieczeństwa w całym łańcuchu dostaw, istotnych dla każdego poziomu zarządzania ryzykiem. Rysunek G-6 przedstawia etap oceny ryzyka oraz jego dane wejściowe i rezultaty na trzech poziomach.



Rysunek G-6: Działania dotyczące obszaru C-SCRM na etapie oceny ryzyka[84]

[84] Bardziej szczegółowe informacje na temat procesu zarządzania ryzykiem można znaleźć w Załączniku C.

Analizy krytyczności, podatności i zagrożeń są niezbędne w procesie oceny ryzyka związanego z łańcuchem dostaw. Działania rozpoczynają się od aktualizacji analizy krytyczności w celu zapewnienia, że przeprowadzana ocena jest ograniczona do minimalnego zakresu obejmującego odpowiednie krytyczne procesy i działania, a także zrozumienia znaczenia i wpływu elementów łańcucha dostaw na poszczególne procesy i działania. Jak przedstawia rys. G-5, analizy podatności i zagrożeń mogą być wykonywane w dowolnej kolejności, ale powinny być wykonywane w sposób iteracyjny, aby zapewnić określenie wszystkich podatności i zagrożeń oraz ustalić, które podatności mogą być wykorzystane przez określone zagrożenia, a także powiązać podatności i zagrożenia z misjami i procesami biznesowymi lub elementami łańcucha dostaw. Po przeprowadzeniu oceny rzeczywistych zagrożeń oraz potencjalnych lub rzeczywistych podatności, informacje te zostaną wykorzystane do oceny prawdopodobieństwa ich wykorzystania – to kluczowy krok prowadzący do ustalenia ich wpływu. W tym miejscu następuje połączenie analiz krytyczności, podatności i zagrożeń, który pomaga w dalszym wyjaśnianiu i określeniu kontekstu wpływu w celu podejmowania świadomych i uzasadnionych decyzji dotyczących ryzyka.

Działania

ANALIZA KRYTYCZNOŚCI

ZADANIE 2-0: Uaktualnienie analizy krytyczności misji i procesów biznesowych, systemów i elementów systemu w celu zawężenia zakresu działań C-SCRM do najważniejszych dla realizacji misji oraz zmniejszenia zapotrzebowania na zasoby.

Wytyczne uzupełniające

Analiza krytyczności powinna obejmować łańcuch dostaw podmiotu oraz stosownych dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT, a także odpowiednie usługi i produkty pozasystemowe. Analiza krytyczności ocenia bezpośredni wpływ podmiotów na priorytety misji. Łańcuch dostaw obejmuje cykl życia systemów, usług i komponentów – określa, czy zagadnienia dotyczące

bezpieczeństwa stanowią element systemów lub komponentów, czy też są dodawane po ich stworzeniu.

Podmioty powinny aktualizować i dostosowywać analizy krytyczności opracowane w ramach ustalania ram ryzyka, w tym w ramach systemu określonego w dokumencie [NSC 199]. W przypadku systemów o niewielkim wpływie należy oceniać współzależności z systemami o umiarkowanym lub dużym wpływie, które mogą wpływać na ten parametr. Jeśli systemy są szeroko wykorzystywane w całym podmiocie, należy określić całościowy wpływ awarii komponentów lub naruszenia zasad ochrony systemu o niewielkim wpływie.

Oprócz aktualizacji i dostosowania analiz krytyczności, wykonanie analizy krytyczności na etapie oceny ryzyka może obejmować:

- Dopracowanie analizy i oceny zależności w celu zrozumienia, które komponenty mogą wymagać dodatkowych zabezpieczeń ze względu na architekturę systemu lub sieci.
- Uzyskanie i przegląd istniejących informacji, które podmiot posiada na temat krytycznych systemów/komponentów, takich jak miejsca, w których są one produkowane lub opracowywane, fizyczne i logiczne drogi dostaw, przepływy informacji i transakcje finansowe związane z tymi komponentami oraz wszelkie inne dostępne informacje, które mogą zapewnić wgląd w łańcuch dostaw tych komponentów[85].
- Aktualizacja informacji o łańcuchu dostaw, danych historycznych i cyklu życia systemu w celu identyfikacji zmian w kluczowych trasach i warunkach łańcucha dostaw.

Wynikiem uaktualnionej analizy krytyczności jest zawężona, uszeregowana pod względem ważności lista krytycznych procesów, systemów i komponentów podmiotu, a także dokładniejsze informacje dotyczące zależności w ramach łańcucha dostaw.

[85] Informacje te mogą być ustalone na podstawie mapy łańcucha dostaw podmiotu lub poszczególnych projektów i systemów informacyjnych. Mapy łańcuchów dostaw są opisami lub obrazami łańcuchów dostaw, które obejmują fizyczny i logiczny przepływ towarów, informacji, procesów i środków finansowych w obie strony. Mogą one obejmować podmioty łańcucha dostaw, lokalizacje, trasy dostaw lub transakcje.

Podmioty mogą wykorzystać proces oceny krytyczności z zadania 1-1 do aktualizacji swojej analizy krytyczności.

Ze względu na to, że na etapie oceny ryzyka dostępnych jest więcej informacji, podmioty mogą zawęzić zakres i zwiększyć dokładność analizy. Określając procesy krytyczne i związane z nimi systemy/komponenty oraz przypisując im poziomy krytyczności, należy wziąć pod uwagę następujące kwestie:

- Analiza funkcjonalna jest skuteczną metodą określania procesów i związanych z nimi komponentów krytycznych oraz wspierających zabezpieczeń.
- Plany odzyskiwania danych po awarii i zapewniania ciągłości działania często określają krytyczne systemy i komponenty systemu, co może być pomocne w ustaleniu poziomów krytyczności.
- Analiza zależności służy określeniu procesów, od których zależą inne procesy krytyczne (np. zabezpieczenia, w tym podpisy cyfrowe stosowane do wdrażania poprawek do oprogramowania).
- Określenie wszystkich punktów dostępu pomaga wskazać i ograniczyć miejsca bezpośredniego dostępu do krytycznych funkcji i komponentów.
- Analiza łańcucha wartości umożliwia ustalenie materiałów, podmiotów, rezultatów oraz klientów korzystających z usług i produktów.
- Złośliwe zmiany lub inne rodzaje naruszenia zasad bezpieczeństwa łańcucha dostaw mogą mieć miejsce w całym cyklu życia systemu.

Uzyskana w ten sposób lista procesów krytycznych i zależności w łańcuchu dostaw jest wykorzystywana w celu realizacji analizy podatności i zagrożeń, a także wstępnego określenia ryzyka związanego z obszarem C-SCRM, jak przedstawia rys. D-4. Następnie można wybrać i wdrożyć środki zapobiegawcze i ograniczające ryzyko w łańcuchu dostaw, aby zmniejszyć ryzyko do akceptowalnego poziomu.

Analiza krytyczności powinna być wykonywana iteracyjnie na dowolnym etapie cyklu życia systemu oraz równolegle na poszczególnych poziomach. W pierwszej iteracji zostaną wskazane krytyczne procesy i systemy lub komponenty, które mają

bezpośredni wpływ na realizację misji i procesów biznesowych. Kolejne iteracje będą uwzględniały informacje z analizy krytyczności, analizy zagrożeń, analizy podatności oraz strategii ograniczania ryzyka opracowanych na każdym z pozostałych poziomów. Każda iteracja będzie precyzować wyniki analizy krytyczności i skutkować dodaniem nowych zabezpieczeń. Do ustalenia oraz utrzymania wyników analizy krytyczności będzie prawdopodobnie potrzebnych kilka iteracji. Podmioty powinny dokumentować wyniki analizy krytyczności oraz dokonywać przeglądu i aktualizacji tej oceny co najmniej raz w roku.

OKREŚLENIE ZAGROŻEŃ I PODATNOŚCI

ZADANIE 2-1: Określenie zagrożeń i podatności w systemach informacyjnych oraz środowiskach, w których działają systemy.

Wytyczne uzupełniające

Oprócz określenia zagrożeń i podatności, opisanych w dokumentach [NSC 800-39] i [NSC 800-30], podmioty powinny przeprowadzić analizę zagrożeń związanych z cyberbezpieczeństwem w łańcuchu dostaw oraz analizę podatności.

Analiza zagrożeń

W przypadku C-SCRM analiza zagrożeń dostarcza precyzyjnych opisów zdarzeń powodujących zagrożenie (patrz Załącznik C) oraz potencjalnych napastników (np. państwa narodowe) oraz wektorów zagrożeń (np. dostawców zewnętrznych), przez co wpływa na zarządzanie, zamówienia, prace inżynieryjne oraz działalność podmiotu[86]Do oceny potencjalnych zagrożeń można wykorzystać różne informacje, w tym ogólnodostępne źródła, wywiad i kontrwywiad. Podmioty powinny uwzględniać, aktualizować i precyzować dane na temat źródeł zagrożeń i założenia zdefiniowane podczas pierwszego kroku procesu. Wyniki analizy zagrożeń wpływają na decyzje o zamówieniach, zmianach oraz wyborze odpowiednich środków zaradczych, które zostaną zastosowane w etapie reakcji na ryzyko. Analiza zagrożeń

[86] Informacje te mogą być ustalone na podstawie mapy łańcucha dostaw podmiotu lub poszczególnych projektów i systemów informacyjnych. Mapy łańcuchów dostaw są opisami lub obrazami łańcuchów dostaw, które obejmują fizyczny i logiczny przepływ towarów, informacji, procesów i środków finansowych w obie strony. Mogą one obejmować podmioty łańcucha dostaw, lokalizacje, trasy dostaw lub transakcje.

dotyczących łańcucha dostaw powinna opierać się na rezultatach analizy krytyczności.

Podmioty powinny wykorzystywać informacje dostępne w ramach istniejących działań związanych z zarządzaniem incydentami w celu ustalenia, czy doświadczyły naruszenia cyberbezpieczeństwa związanego z łańcuchem dostaw oraz w celu analizy takich naruszeń. Podmioty powinny określić kryteria określające miary naruszenia zasad cyberbezpieczeństwa łańcucha dostaw, aby zapewnić możliwość identyfikacji takich zdarzeń w ramach działań podejmowanych po wystąpieniu incydentu, w tym dochodzeń. Ponadto podmioty powinny analizować inne źródła informacji o incydentach w podmiocie w celu ustalenia, czy doszło do naruszenia zasad bezpieczeństwa łańcucha dostaw.

Analiza zagrożeń związanych z łańcuchem dostaw powinna obejmować co najmniej następujące informacje:

- obserwacje ataków dotyczących cyberbezpieczeństwa w łańcuchu dostaw w czasie ich trwania;
- dane o incydentach zebrane po naruszeniu zasad bezpieczeństwa łańcucha dostaw;
- obserwacje taktyk, technik i procedur stosowanych w konkretnych atakach, niezależnie od tego, czy zostały one zaobserwowane, czy też zebrane w czasie kontroli po ataku;
- informacje o klęskach żywiołowych i katastrofach spowodowanych przez człowieka przed, w trakcie i po wystąpieniu.

Analiza podatności

Na potrzeby obszaru C-SCRM, podatność to słabość systemu informacyjnego, procedur bezpieczeństwa systemu, zabezpieczeń wewnętrznych lub wdrożenia, która może zostać wykorzystana lub uruchomiona przez źródło zagrożenia [NSC 800-53].

Analiza podatności jest procesem iteracyjnym, który wpływa na ocenę ryzyka i wybór środków przeciwdziałania ryzyku. Analiza podatności współgra z analizą zagrożeń, przekłada się na analizę wpływu oraz pomaga w określeniu zakresu podatności, które powinny zostać ograniczone.

Analiza podatności w ramach etapu oceny ryzyka powinna opierać się na podejściach opracowanych w trakcie etapu określania ram ryzyka w celu aktualizacji i dopracowania założeń dotyczących podatności łańcucha dostaw na zagrożenia związane z cyberbezpieczeństwem.

Analiza podatności powinna rozpocząć się od zidentyfikowania podatności, które dotyczą kluczowych misji i procesów biznesowych oraz systemów lub komponentów systemu wskazanych w ramach analizy krytyczności. Badanie podatności może skutkować potrzebą podniesienia lub przynajmniej ponownej analizy poziomów krytyczności procesów i komponentów określonych we wcześniejszych analizach krytyczności. Późniejsze wersje analizy podatności mogą również pomóc w określeniu dodatkowych zagrożeń lub możliwości ich wystąpienia, które nie zostały uwzględnione we wcześniejszych ocenach zagrożeń.

Tabela G-8 zawiera przykłady podatności związanych z cyberbezpieczeństwem w całym łańcuchu dostaw, które można dostrzec na trzech poziomach.

Tabela G-8: Przykłady podatności związanych z cyberbezpieczeństwem w całym łańcuchu dostaw na poszczególnych poziomach podmiotu

Poziom	Podatność	Metody
Poziom 1 – Podmiot	1. Braki lub nieprawidłowości w strukturach lub procesach zarządzania podmiotem, na przykład brak planu C-SCRM. 2. Podatności w samym łańcuchu dostaw (np. podmioty podatne na zagrożenia, nadmierna zależność od niektórych podmiotów).	1. Opracowanie wytycznych dotyczących uznawania zależności od zewnętrznych podmiotów jako podatności. 2. Poszukiwanie alternatywnych źródeł nowych technologii, w tym opracowywanie ich we własnym zakresie i wykorzystywanie zaufanych usług wspólnych i powszechnych rozwiązań.

Poziom	Podatność	Metody
Poziom 2 – Misja i działalność	1. Brak procesu wykrywania podróbek. 2. Brak budżetu przeznaczonego na wdrożenie analiz technicznych oraz testów akceptacyjnych dostarczanych komponentów systemu wchodzących do cyklu życia systemu jako części zamienne. 3. Podatność na problemy ze strony źródeł dostaw innowacyjnych technologii (np. technologia należąca do podmiotu zewnętrznego lub przez niego zarządzana zawiera błędy).	1. Opracowanie programu wykrywania zmanipulowanych lub podrobionych produktów oraz przeznaczenie odpowiedniego budżetu na zasoby i szkolenia. 2. Przeznaczenie budżetu na testy akceptacyjne i weryfikację komponentów wprowadzanych do cyklu życia systemu.
Poziom 3 – Operacyjny	1. Niespełnianie wymagań przez funkcje systemu, co skutkuje znacznym wpływem na wydajność.	1. Inicjowanie zmian inżynieryjnych w celu rozwiązania problemu braku odpowiednich funkcjonalności oraz testowanie poprawek pod kątem wpływu na wydajność. Złośliwe modyfikacje mogą zostać wprowadzone do systemu podmiotu w całym cyklu życia systemu. 2. Śledzenie informacji na temat podatności publikowanych przez producentów oprogramowania.

OKREŚLENIE RYZYKA

ZADANIE 2-2: Określenie ryzyka dla operacji i aktywów podmiotu, osób fizycznych, innych podmiotów i państwa, jeśli wykryte zagrożenia wykorzystają zidentyfikowane podatności.

Wytyczne uzupełniające

Podmioty identyfikują ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw, biorąc pod uwagę prawdopodobieństwo wykorzystania przez znane zagrożenia znanych podatności w łańcuchu dostaw i za jego pośrednictwem, a także wynikające z tego konsekwencje lub negatywne skutki i szkody, gdy dojdzie do realizacji ryzyka. Podmioty wykorzystują informacje o zagrożeniach i podatnościach wraz z informacjami o prawdopodobieństwie i konsekwencjach oraz wpływie, aby określić ryzyko w sposób jakościowy lub ilościowy. Dane wyjściowe z procesu określania ryzyka na poziomach 1 oraz 2 powinny odpowiadać bezpośrednio zadaniom z etapu przygotowania w procesie ram zarządzania ryzykiem na poziomie podmiotu opisanych w dokumencie [NSC 800-37], natomiast oceny ryzyka przeprowadzone na poziomie 3 powinny odpowiadać bezpośrednio zadaniom z etapu przygotowania w procesie ram zarządzania ryzykiem na poziomie operacyjnym.

Prawdopodobieństwo

Prawdopodobieństwo jest czynnikiem ważonym opartym na subiektywnej analizie, że dane zagrożenie będzie w stanie wykorzystać daną podatność [CNSSI 4009]. Określenie tego prawdopodobieństwa wymaga uwzględnienia charakterystyki źródeł zagrożeń, zidentyfikowanych podatności oraz podatności podmiotu na zagrożenie związane z cyberbezpieczeństwem w całym łańcuchu dostaw przed i w trakcie wdrażania zabezpieczeń lub środków ograniczających ryzyko. Analiza prawdopodobieństwa powinna opierać się na metodach określonych w ramach etapu określania ram ryzyka oraz aktualizować, udoskonalać i rozszerzać wszelkie założenia dotyczące prawdopodobieństwa dokonane na tym etapie. W przypadku wrogich zagrożeń analiza ta powinna uwzględniać stopień zdolności i zamiaru napastnika do wpływania na misję podmiotu. Ocena ryzyka związanego z cyberbezpieczeństwem w łańcuchu dostaw powinna uwzględniać dwie perspektywy:

1. Prawdopodobieństwo, że jeden lub więcej elementów w samym łańcuchu dostaw jest zagrożony. Może to wpłynąć na przykład na dostępność wysokiej jakości komponentów lub zwiększyć ryzyko kradzieży własności intelektualnej.
2. Prawdopodobieństwo, że system lub komponent w ramach łańcucha dostaw zostanie naruszony, na przykład przez złośliwy kod wprowadzony do systemu lub zjawiska atmosferyczne uszkadzające komponent.

W niektórych przypadkach te dwie perspektywy mogą być zbieżne, jednocześnie obie mogą wpływać na zdolność podmiotu do wykonywania jej misji.

Analiza prawdopodobieństwa powinna uwzględniać:

- Założenia dotyczące zagrożeń, które określają rodzaje zagrożeń, na jakie może być narażony system lub komponent, takie jak zagrożenia związane z cyberbezpieczeństwem, katastrofy naturalne lub zagrożenia bezpieczeństwa fizycznego.
- Informacje o rzeczywistym zagrożeniu dla łańcucha dostaw, takie jak możliwości, narzędzia, zamiary i cele napastników.
- Dane historyczne dotyczące częstotliwości występowania zdarzeń w łańcuchu dostaw w podobnych podmiotach.
- Punkt widzenia wewnętrznych ekspertów na temat prawdopodobieństwa naruszenia zasad ochrony systemu lub procesu w łańcuchu dostaw.
- Narażenie komponentów na dostęp z zewnątrz (spoza granic autoryzacji systemu).
- Zidentyfikowane podatności w systemie, procesie lub komponencie.
- Dane empiryczne dotyczące słabości i podatności ustalone w ramach analiz w celu określenia prawdopodobieństwa wystąpienia zagrożenia związanego z cyberbezpieczeństwem w łańcuchu dostaw.

Czynniki, które należy wziąć pod uwagę to łatwość lub trudność przeprowadzenia skutecznego ataku dzięki wykorzystaniu podatności oraz możliwość wykrycia metody wykorzystanej do wprowadzenia lub wykorzystania podatności. Celem jest ocena

wpływu podatności, który zostanie połączony z informacjami o zagrożeniach, aby określić prawdopodobieństwo dokonania skutecznego ataku w określonych ramach czasowych w ramach procesu oceny ryzyka. Prawdopodobieństwo może być oparte na założeniach dotyczących zagrożeń lub na rzeczywistych danych dotyczących zagrożeń, takich jak poprzednie naruszenia zasad ochrony łańcucha dostaw, określone możliwości przeciwników, historyczne trendy oraz częstotliwość naruszeń. Podmiot może korzystać z danych empirycznych i analiz statystycznych w celu określenia prawdopodobieństw wystąpienia naruszeń w zależności od rodzaju danych dostępnych dla podmiotu.

Wpływ

Podmioty powinny rozpocząć analizę wpływu od wykorzystania metodologii i założeń dotyczących potencjalnego wpływu określonych w ramach procesu określania ram ryzyka, aby określić wpływ naruszenia zasad bezpieczeństwa oraz środków ograniczających wpływ. Podmioty muszą określić różne negatywne skutki naruszenia zasad bezpieczeństwa, w tym 1) charakterystykę źródeł zagrożeń, które mogą być przyczyną zdarzeń, 2) zidentyfikowane podatności oraz 3) wrażliwość podmiotu na takie zdarzenia w oparciu o planowane lub wdrożone środki zaradcze. Analizy wpływu jest procesem iteracyjnym wykonywanym w przypadku wystąpienia naruszenia zasad bezpieczeństwa, gdy podejmowane są decyzje dotyczące środków zaradczych mających na celu ocenę skutków zmian, a także w trakcie cyklu życia systemu, gdy zmienia się sytuacja lub kontekst systemu lub środowiska.

Podmioty powinny wykorzystać wyniki analizy wpływu w celu określenia akceptowalnego poziomu ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw związanym z konkretnym systemem. Wpływ ryzyka jest określany na podstawie analiz krytyczności, zagrożeń i podatności i powinien dotyczyć wpływu utraty poufności, integralności lub dostępności informacji lub systemu na działania organizacyjne, aktywa organizacyjne, osoby fizyczne, inne organizacje lub państwo – w tym interesy bezpieczeństwa narodowego. [NSC 800-53]. Wpływ jest czynnikiem jakościowym wymagającym oceny analitycznej. Osoby odpowiedzialne za podejmowanie decyzji wykorzystują wpływ w procesie podejmowania decyzji dotyczących ryzyka i jego akceptacji, unikania, ograniczania lub dzielenia ryzyk i konsekwencji takich decyzji.

Podmioty powinny dokumentować ogólne wyniki ocen ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw w swoich sprawozdaniach z oceny ryzyka[87]. Sprawozdania z oceny ryzyka związanego z cyberbezpieczeństwem w łańcuchu dostaw powinny obejmować ryzyko na wszystkich trzech poziomach podmiotu. W zależności od struktury i wielkości podmiotu może być wymagane sporządzenie wielu sprawozdań oceniających ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw. Podmioty zachęca się do opracowywania indywidualnych raportów na poziomie 1. W przypadku poziomu 2 podmioty powinny włączyć ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw do odpowiedniej analizy skutków dla działalności na poziomie misji oraz mogą opracować oddzielne sprawozdania dotyczące ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw w obrębie poszczególnych misji. W przypadku poziomu 3 podmioty mogą uwzględnić ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw do odpowiednich ram reakcji na ryzyko. Ramy reagowania na ryzyko na wszystkich trzech poziomach powinny być wzajemnie powiązane, w razie potrzeby powinny się do siebie odwoływać, być uwzględnione w planach C-SCRM i stanowić część pakietów autoryzacyjnych.

Zestawienie ryzyka

Podmioty mogą stosować zestawienia ryzyka w celu połączenia kilku ryzyk niższego poziomu w pojedyncze bardziej ogólne ryzyko wyższego poziomu [NSC 800-30]. Zestawienia ryzyka są szczególnie ważne dla działań w obszarze C-SCRM, ponieważ umożliwiają podmiotom lepszą analizę narażenia na ryzyko związane z łańcuchem dostaw w kontekście aktywów na różnych poziomach organizacji. Podmioty mogą zestawiać i normalizować wyniki ocen ryzyka związanego z obszarem C-SCRM z innymi ocenami ryzyka w celu zrozumienia całościowego narażenia na ryzyko oraz rodzajów ryzyk. Takie zestawienie może nastąpić na poziomie podmiotu, w przypadku gdy podmiot składa się z wielu podległych jednostek. Każdy podmiot niższego

[87] Sprawdzony dostawca to dostawca, w relacjach z którym organizacja czuje się bezpiecznie i pewnie. Ten poziom poczucia bezpieczeństwa osiągany jest zazwyczaj poprzez opracowanie przez organizację zbioru kryteriów dotyczących łańcucha dostaw, a następnie weryfikację dostawców pod kątem spełniania tych kryteriów.

szczebla zestawia i normalizuje ryzyko w ramach pojedynczego rejestru ryzyka podmiotu. Zestawienie może również nastąpić na poziomie misji i procesów biznesowych, aby utworzyć jedno zestawienie ryzyka na poziomie podmiotu. Aby ułatwić ten proces, podmioty powinny maksymalnie wykorzystać wspólne ramy oraz dokumenty z innych procesów związanych z ryzykiem, na przykład z procesu zarządzania ryzykiem w podmiocie.

Mając do czynienia z odrębnymi ryzykami (nie nakładającymi się na siebie), podmioty mogą łatwiej opracować zestawienia narażeń na ryzyko na poziomach 1 oraz 2. W wielu przypadkach podmioty mogą uznać, że ryzyka przeprowadzone na niższych poziomach zawierają pokrywające się szacunki prawdopodobieństwa i wpływu. W takich przypadkach suma elementów (tj. Ocen narażenia na ryzyko na niższych poziomach) jest większa niż całość (tj. Łączne narażenie na ryzyko podmiotu). W celu rozwiązania tego problemu, podmioty mogą stosować różne techniki. Mogą zdecydować się na wykorzystanie wizualizacji lub map w celu przedstawienia względnego prawdopodobieństwa i wpływu ryzyk. Przedstawiając zestawienie ryzyka w postaci liczb, podmioty powinny zapewnić, że oceny ryzyka skutkują specyficznymi wynikami poprzez przyjęcie wzajemnie się wykluczających i łącznie wyczerpujących ram (*ang. mutually exclusive and collectively exhaustive* - MECE). Ramy MECE ukierunkowują analizę danych wejściowych (np. zagrożeń, podatności, skutków) i pozwalają podmiotowi zminimalizować liczbę zbieżnych założeń i szacunków. Zamiast sumować ryzyka z niższych poziomów, podmioty mogą zdecydować się na przeprowadzenie nowej całościowej oceny na wyższym poziomie, która wykorzystuje połączone wyniki ocen z niższych poziomów. Takie postępowanie może pomóc podmiotom uniknąć podwójnego wliczania ryzyka, co skutkuje przeszacowaniem narażenia na ryzyko. Podmioty powinny zachować ostrożność przy zestawianiu ryzyk, by uniknąć trudnych do wyjaśnienia zestawień, zakładających na przykład połączenie zróżnicowanych rodzajów ryzyka.

Metody ilościowe zapewniają szereg korzyści w zakresie zestawiania ryzyka. Dzięki zastosowaniu technik probabilistycznych (np. metody Monte Carlo, analizy bayesowskiej) podmioty mogą połączyć podobne ryzyka i ująć je w formie łatwej do zrozumienia liczby (np. kwoty) uzasadnionej matematycznie. Ramy MECE powinny być stosowane w przypadku wykorzystywania metod ilościowych.

Rezultaty i warunki końcowe

Rezultaty tego etapu obejmują:

- informacje na temat krytyczności misji i procesów biznesowych;
- ustalenie zależności pomiędzy krytycznymi aspektami infrastruktury łańcucha dostaw systemu (np. cyklu życia systemu) a zagrożeniami i podatnościami;
- ustalenie prawdopodobieństwa i wpływu potencjalnego naruszenia zasad ochrony cyberbezpieczeństwa łańcucha dostaw;
- ustalenie ryzyka dotyczącego misji i systemu;
- udokumentowanie oceny ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw, dotyczące misji i procesów biznesowych lub poszczególnych systemów;
- uwzględnienie wyników odpowiednich ocen ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw w procesie zarządzania ryzykiem w podmiocie.

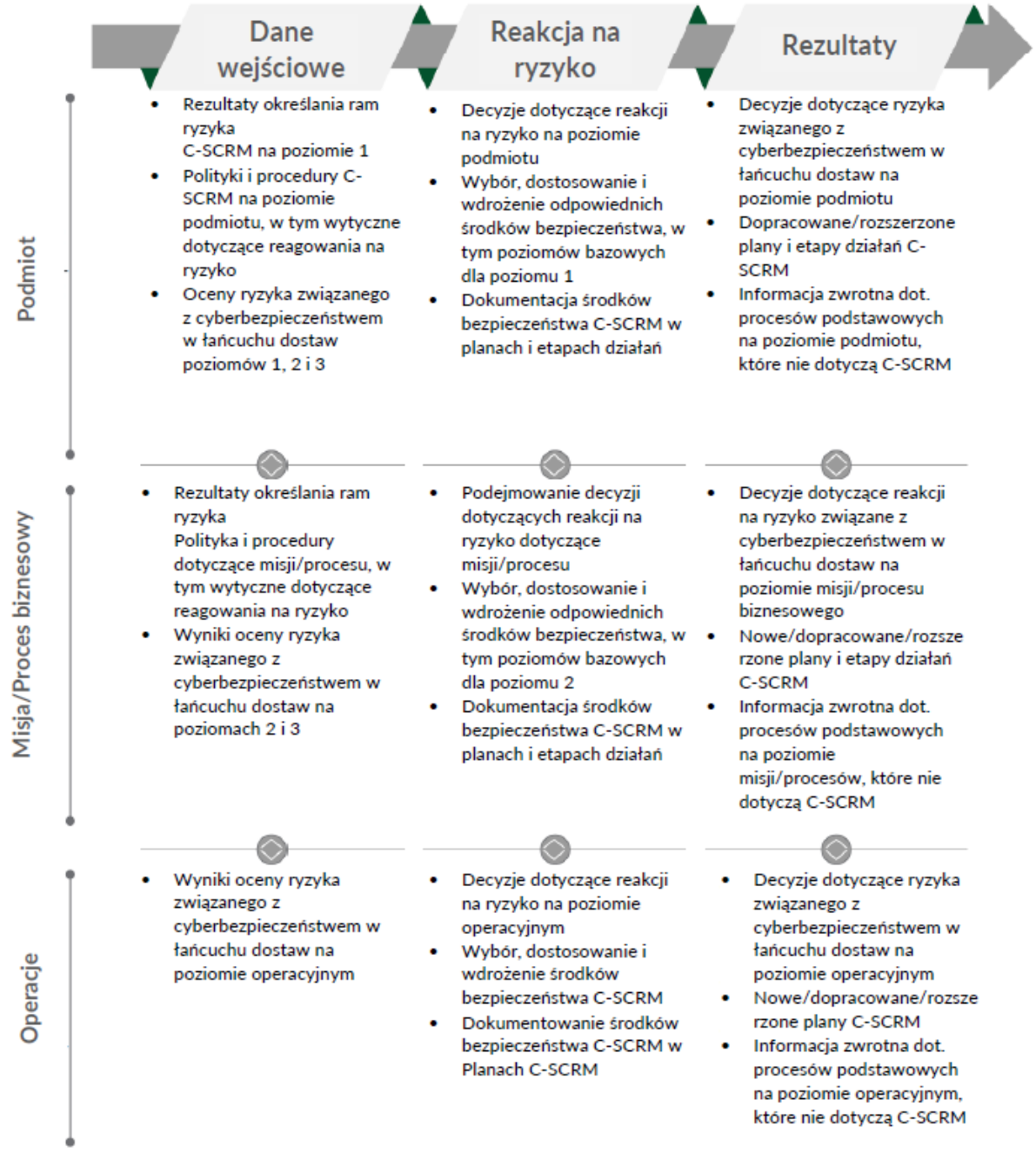
REAKCJA NA RYZYKO

Dane wejściowe i warunki wstępne

Reakcja na ryzyko to etap, w którym osoby przeprowadzające ocenę ryzyka przekazują decydentom wyniki oceny, proponowane środki bezpieczeństwa oraz odpowiadający im akceptowalny poziom ryzyka dla każdej proponowanej opcji. Informacje te powinny być przedstawione w sposób pozwalający na wykorzystanie ich do podejmowania decyzji dotyczących ryzyka. Pozwoli to decydentom na opracowanie odpowiednich reakcji na ryzyko w oparciu o dostępne opcje oraz odpowiadające im czynniki ryzyka związane z ich wyborem. Czasami odpowiednią

reakcją jest wyłącznie monitorowanie działań i zachowań napastników, aby lepiej zrozumieć jego taktykę i działania.

Reakcja na ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw powinna być związana z ogólną reakcją na ryzyko w podmiocie. Rysunek G-7 przedstawia etap reakcji na ryzyko oraz jego dane wejściowe i rezultaty na trzech poziomach.



Rysunek G-7: Działania dotyczące obszaru C-SCRM na etapie reakcji na ryzyko[88]

[88] Bardziej szczegółowe informacje na temat procesu zarządzania ryzykiem można znaleźć w Załączniku C.

Działania

OKREŚLENIE REAKCJI NA RYZYKO

ZADANIE 3-1: Określenie alternatywnych sposobów działania w reakcji na ryzyko określone na etapie oceny ryzyka.

Strategie reakcji podmiotu na ryzyko będą oparte na strategiach zarządzania ryzykiem opracowanych dla podmiotu (na poziomie 1) oraz misji i procesów biznesowych (na poziomie 2). Strategie reagowania na ryzyko obejmują ogólne kierunki działań, które podmiot może podjąć w ramach reagowania na ryzyko. W ramach działań ograniczających ryzyko, podmioty powinny wybrać środki bezpieczeństwa związane z obszarem C-SCRM i dostosować je do ustalonych ryzyk. Środki bezpieczeństwa związane z obszarem C-SCRM powinny być wybrane dla każdego z trzech poziomów i dostosowane do wyników oceny ryzyka.

Wiele środków bezpieczeństwa związanych z obszarem C-SCRM zawartych w niniejszym dokumencie może być częścią planu bezpieczeństwa IT, powinny być także włączone jako wymagania do umów zawartych z dostawcami usług zewnętrznych. Środki bezpieczeństwa zostały uwzględnione, ponieważ dotyczą one obszaru C-SCRM.

Proces powinien rozpocząć się od określenia dopuszczalnego ryzyka w celu wsparcia oceny rozwiązań alternatywnych, czyli analizy kompromisów.

OCENA ROZWIĄZAŃ ALTERNATYWNYCH

ZADANIE 3-2: Ocena zróżnicowanych działań w ramach reakcji na ryzyko.

Po określeniu akceptowalnego poziomu ryzyka należy określić i ocenić sposoby reagowania na ryzyko pod kątem skuteczności w umożliwieniu podmiotowi osiągnięcia zdefiniowanego progu ryzyka. Ocena rozwiązań alternatywnych odbywa się zazwyczaj na poziomie 1 lub 2, ze szczególnym uwzględnieniem przewidywanego w skali całego podmiotu wpływu C-SCRM na jego zdolność do skutecznego realizowania misji i procesów. Gdy przeprowadzana jest na poziomie 3, skupia się na cyklu życia systemu lub czasie potrzebnym na wdrożenie danego rozwiązania.

Każdy analizowany kierunek działania może obejmować połączenie akceptacji ryzyka, unikania, łagodzenia, przenoszenia i dzielenia się ryzykiem. Na przykład podmiot może zdecydować się na przekazanie części ryzyka dostawcy strategicznemu poprzez dobór odpowiednich środków bezpieczeństwa uwzględnionych w umowie. Podmiot może podjąć też decyzję o ograniczeniu ryzyka do akceptowalnego poziomu poprzez wybór i wdrożenie środków bezpieczeństwa po swojej stronie. W wielu przypadkach strategie dotyczące ryzyka będą wykorzystywać wiele sposobów reagowania na ryzyko.

Podczas tej analizy podmiot przeanalizuje dostępne sposoby reagowania na ryzyko w odniesieniu do zidentyfikowanych zagrożeń cyberbezpieczeństwa w całym łańcuchu dostaw. Celem tego procesu jest umożliwienie podmiotowi osiągnięcia odpowiedniej równowagi pomiędzy działaniami w obszarze C-SCRM a potrzebami związanymi z działalnością. W pierwszej kolejności podmioty powinny zapewnić, że gotowość do podejmowania ryzyka i tolerancja ryzyka, a także priorytety, kompromisy, obowiązujące wymagania i ograniczenia zostały przeanalizowane przy współudziale interesariuszy, którzy znają wymagania podmiotu, takie jak koszty, harmonogram, wydajność, polityki oraz przepisy. W ramach tego procesu podmiot określi implikacje związane z reagowaniem na ryzyko oraz wpływ na jego wymagania. Mając pełną wiedzę na temat wpływu reakcji na ryzyko, podmiot powinien przeprowadzić analizę kompromisów dotyczących obszaru C-SCRM na poziomie misji i operacyjnym, aby ustalić właściwe środki bezpieczeństwa związane z obszarem C-SCRM. Na poziomie 3 proces FARM wpisuje się w proces wyboru procesu ram zarządzania ryzykiem opisany w dokumencie [NSC 800-37].

Wybrane środki bezpieczeństwa związane z obszarem C-SCRM będą zróżnicowane w zależności od miejsca ich zastosowania w ramach poziomów podmiotu i procesów cyklu życia systemu. Na przykład, środki bezpieczeństwa mogą obejmować stosowanie strategii ślepych zakupów w celu ukrycia informacji na temat zastosowania kluczowego komponentu oraz informacji na temat projektu, a także zapobiegania potencjalnym manipulacjom czy weryfikacji komponentu. W przypadku każdego wdrożonego środka bezpieczeństwa podmiot powinien określić osobę odpowiedzialną za realizację jego wdrożenia oraz opracować plan czasowy lub

zdarzeniowy dla całego cyklu życia systemu. Wiele zabezpieczeń może dotyczyć szerokiego zakresu możliwych zagrożeń. Z tego powodu ustalenie w jaki sposób środki bezpieczeństwa wpływają na ogólne ryzyko ma zasadnicze znaczenie i musi być przeprowadzone przed wyborem i dostosowaniem środków bezpieczeństwa, ponieważ przed sfinalizowaniem listy zabezpieczeń może być potrzebna kolejna analiza kompromisów. Podmiot może bowiem nieświadomie zastępować mniejsze ryzyko większym, jeżeli zależności między proponowanymi środkami bezpieczeństwa i ogólnym ryzykiem nie są dobrze zrozumiane i uwzględnione.

DECYZJE DOTYCZĄCE REAKCJI NA RYZYKO

ZADANIE 3-3: Podejmowanie decyzji o właściwym sposobie reagowania na ryzyko.

Jak czytamy w dokumencie [NSC 800-39], podmioty powinny dobierać oraz dostosować środki bezpieczeństwa związane z obszarem C-SCRM na podstawie oceny alternatywnych rozwiązań i ogólnego zrozumienia zagrożeń, ryzyka i priorytetów łańcucha dostaw. W ramach poziomów 1 i 2 decyzja oraz wybrane poziomy bazowe zabezpieczeń powinny być udokumentowane w ramach reakcji na ryzyko dotyczących obszaru C-SCRM[89]. W ramach poziomu 3, wynikająca z tego decyzja oraz wybrane i dostosowane środki bezpieczeństwa powinny być udokumentowane w ramach planu C-SCRM, który stanowi część pakietu autoryzacji.

Decyzje dotyczące reakcji na ryzyko mogą być podejmowane przez osobę odpowiedzialną za zarządzanie ryzykiem lub delegowane przez nią do innej osoby w podmiocie. Chociaż decyzja może zostać oddelegowana na poziom 2 lub 3, znaczenie i zasięg oddziaływania powinny decydować o poziomie, na którym jest ona podejmowana. Decyzje dotyczące reakcji na ryzyko mogą być podejmowane we współpracy z osobami zarządzającymi ryzykiem w podmiocie, osobami odpowiedzialnymi za misje oraz systemy, stosownie do sytuacji. Na decyzje dotyczące reakcji na ryzyko wpływają parametry dotyczące gotowości na ryzyko oraz jego tolerancji. Na podstawie tych parametrów decydenci mogą zapewnić spójność decyzji dotyczących ryzyka w podmiocie oraz dostosowanie do jego celów strategicznych. Parametry te mogą również umożliwić podmiotom przekazanie

[89] Więcej informacji na temat ram reakcji na ryzyko oraz przykłady można znaleźć w Załączniku B.

odpowiedzialności za decyzje dotyczące ryzyka na niższe poziomy i zapewnienie większej autonomii na wszystkich poziomach.

W ramach poziomów 1 i 2, wynikające z nich decyzje powinny być udokumentowane wraz z wszelkimi zmianami wymagań oraz zabezpieczeniami bazowymi na poziomie podmiotu lub misji i procesów biznesowych) w ramach reakcji na ryzyko dotyczących obszaru C-SCRM. Ramy reagowania na ryzyko dotyczące obszaru C-SCRM mogą wpływać na inne powiązane ramy reagowania na ryzyko.

Ramy reakcji na ryzyko powinny zawierać:

- opis źródła zagrożenia, zdarzenia powodującego zagrożenie, wykorzystanej luki i rezultatu zdarzenia;
- analizy prawdopodobieństwa i wpływu ryzyka oraz narażenia na ryzyko;
- opis wybranych strategii i zabezpieczeń wraz z szacunkowym kosztem i skutecznością.

W ramach poziomu 3, wynikająca z tego decyzja oraz wybrane i dostosowane środki bezpieczeństwa powinny być udokumentowane w ramach planu C-SCRM. Chociaż plan C-SCRM powinien być opracowany proaktywnie, może być również opracowany w odpowiedzi na naruszenie zasad ochrony cyberbezpieczeństwa łańcucha dostaw. Plan C-SCRM powinien obejmować pełny cyklu życia systemu, poziom bazowy działań w obszarze C-SCRM oraz określać wymagania i środki bezpieczeństwa w łańcuchu dostaw na poziomie operacyjnym. Plan C-SCRM powinien być weryfikowany i aktualizowany w oparciu o wyniki monitorowania cyberbezpieczeństwa w łańcuchu dostaw. Plany C-SCRM powinny:

- obejmować opis środowiska określony na pierwszym etapie procesu, w tym informacje na temat polityk, procesów i procedur oparte na wymogach podmiotu i misji realizowanych przez podmiot;
- zawierać role odpowiedzialne za opracowanie planu, na przykład funkcja: ds. zarządzania ryzykiem, r ds. finansowych; CIO; menadżer programu lub osoba odpowiedzialna za system;

- określać kluczowe osoby – dyrektorów, osoby odpowiedzialne za zamówienia i zaopatrzenie, biuro zarządzania programem C-SCRM, inżynierów systemu, inżynierów bezpieczeństwa systemu, deweloperów, osoby odpowiedzialne za utrzymanie, kierowników operacyjnych oraz architektów systemu;
- przedstawiać właściwe dla każdego poziomu środki ograniczające ryzyko oraz środki bezpieczeństwa wynikające z oceny rozwiązań alternatywnych;
- opisywać decyzje dotyczące dostosowania wybranych zabezpieczeń wraz z uzasadnieniami;
- opisać procesy przekazywania informacji zwrotnych między poziomami w celu zapewnienia uwzględnienia współzależności w zakresie cyberbezpieczeństwa w łańcuchu dostaw;
- opisać działania związane z monitorowaniem i egzekwowaniem (w tym informacje dotyczące audytu) mające zastosowanie do zakresu każdego konkretnego planu dotyczącego obszaru C-SCRM;
- w razie potrzeby podać jakościowe lub ilościowe środki wspierające wdrożenie planu C-SCRM i ocenić skuteczność wdrożenia[90];
- określać częstotliwości przeglądów i aktualizacji planu;
- uwzględniać kryteria wprowadzania zmian, takich jak etapy cyklu życia, przeglądy lub znaczące działania w ramach umowy;
- włączać dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT do planów C-SCRM, jeśli są one udostępniane w ramach umów.

Podmioty mogą chcieć włączyć środki bezpieczeństwa związane z obszarem C-SCRM do odpowiednich planów bezpieczeństwa systemu lub opracować oddzielne plany

[90] NIST SP 800-55, Rev. 1, *Performance Measurement Guide for Information Security* (July 2008) zapewnia wytyczne dotyczące opracowywania działań w zakresie bezpieczeństwa informacji. Podmioty mogą wykorzystać ogólne wytyczne zawarte w tej publikacji do opracowania działań na potrzeby swoich planów C-SCRM. Patrz: http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.

C-SCRM na poziomie operacyjnym. Na poziomie 3 plan C-SCRM dotyczy systemów o wysokim i umiarkowanym stopniu wpływu określonym na podstawie dokumentu [NSC 199]. Wymagania i dane wejściowe ze strategii C-SCRM podmiotu na poziomie 1 oraz strategii C-SCRM dotyczącej misji i planu wdrożenia na poziomie 2 powinny być wykorzystywane do rozwoju planów C-SCRM na poziomie 3. Z kolei środki bezpieczeństwa i wymogi C-SCRM na poziomie 3 powinny być uwzględnione przy opracowywaniu i aktualizacji wymogów i zabezpieczeń stosowanych na pozostałych poziomach. Plany C-SCRM powinny być wzajemnie połączone i w razie potrzeby powinny się do siebie odwoływać.

Tabela G-9 podsumowuje środki bezpieczeństwa, które należy zawrzeć w ramach reagowania na ryzyko na poziomach 1 i 2, w planach C-SCRM na poziomie 3, a także opisuje ich przykłady.

Tabela G-9: Środki bezpieczeństwa na poziomach 1, 2 i 3

Poziom	Środek bezpieczeństwa	Przykłady
Poziom 1	Zapewnia wspólne zabezpieczenia bazowe dla poziomów 2 i 3.	• Minimalne zestawy środków bezpieczeństwa dotyczące wszystkich dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT. • Zestawy środków bezpieczeństwa wdrażane przez podmiot dotyczące przetwarzania i przechowywania danych dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT. • Szkolenie i zwiększanie świadomości zagadnień dotyczących cyberbezpieczeństwa w łańcuchu dostaw dla pracowników odpowiedzialnych za zamówienia na poziomie podmiotu.

Poziom	Środek bezpieczeństwa	Przykłady
Poziom 2	• Wdrożenie zabezpieczeń wspólnych określonych na poziomie 1. • Zapewnia wspólne poziomy zabezpieczeń bazowych dotyczące misji i procesów biznesowych dla poziomu 3. • Przekazuje informacje zwrotne na poziomie 1 na temat ustalonych środków bezpieczeństwa oraz ich skuteczności.	• Minimalne zestawy środków bezpieczeństwa dotyczące wszystkich dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT związanych z konkretną misją oraz procesami biznesowymi. • Dopracowanie zarządzania tożsamością i dostępem w celu zniwelowania obaw dotyczących obszaru C-SCRM. • Szkolenia i działania zwiększające świadomość zagadnień dotyczących łańcucha dostaw dla poszczególnych programów.
Poziom 3	• Wdrożenie zabezpieczeń wspólnych określonych na poziomach 1 i 2. • Określa środki bezpieczeństwa dotyczące systemów na poziomie 3.	• Minimalne zestawy środków bezpieczeństwa dotyczące dostawców usług lub konkretnego sprzętu i oprogramowania w kontekście poszczególnych systemów. • Odpowiednio rygorystyczne kryteria akceptacji dla zarządzania zmianami w systemach, które wspierają łańcuch dostaw, takie jak środowiska testowe lub zintegrowane środowiska rozwojowe. • Szkolenia i działania zwiększające świadomość zagadnień dotyczących łańcucha dostaw dla poszczególnych systemów.

Poziom	Środek bezpieczeństwa	Przykłady
	• Przekazuje informacje zwrotne poziomom 1 i 2 na temat ustalonych środków bezpieczeństwa oraz ich skuteczności.	• Powiązania z cyklem życia systemu.

Załącznik C zawiera przykładowy szablon planu C-SCRM z rozdziałami i rodzajami informacji, które podmioty powinny uwzględnić w swoich działaniach związanych z planowaniem C-SCRM.

WDROŻENIE REAKCJI NA RYZYKO

ZADANIE 3-4: Wdrożenie wybranego sposobu działania w reakcji na ryzyko.

Podmioty powinny wdrażać plan C-SCRM w sposób, który łączy środki bezpieczeństwa związane z obszarem C-SCRM z ogólnymi procesami zarządzania ryzykiem.

Rezultaty i warunki końcowe

Wynikiem tego etapu jest zestaw środków bezpieczeństwa związanych z obszarem C-SCRM, które odnoszą się do wymagań podmiotu dotyczących obszaru C-SCRM i mogą być uwzględnione jako wymogi bazowe dla systemów oraz zapisy umów z dostawcami. Te wymagania i wynikające z nich środki bezpieczeństwa zostaną włączone do cyklu życia systemu i innych procesów podmiotu na wszystkich trzech poziomach.

Dla ogólnych typów ryzyka oznacza to:

- Wybór, ocenę i dostosowanie środków bezpieczeństwa związanych z obszarem C-SCRM, które dotyczą określonych ryzyk.
- Określenie konsekwencji wdrożenia lub zaniechania wdrożenia działań.
- Opracowanie i wdrożenie planu C-SCRM.

MONITOROWANIE RYZYKA

Dane wejściowe i warunki wstępne

Monitorowanie ryzyka to etap, podczas którego podmioty 1) weryfikują zgodność, 2) określają bieżącą skuteczność środków reagowania na ryzyko oraz 3) określają zmiany wpływające na ryzyko w systemach informacyjnych podmiotu i środowiskach.

Zmiany w podmiocie, misji i procesach biznesowych, operacjach lub łańcuchu dostaw mogą mieć bezpośredni wpływ na cyberbezpieczeństwo łańcucha dostaw podmiotu. Etap monitorowania zapewnia możliwość śledzenia takich zmian i zapewnienia, że są one odpowiednio oceniane pod kątem wpływu. Jeżeli w wyniku monitorowania nastąpi ponowne określenie zagadnień dotyczących cyberbezpieczeństwa w łańcuchu dostaw, podmioty powinny koordynować nowe działania ze swoimi dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych oraz innymi dostawcami usług związanych z ICT/OT w celu rozwiązania problemów i ustalenia wzajemnych zobowiązań. Kluczowym elementem etapu monitorowania ryzyka jest przekazywanie informacji wpływających na oceny ryzyka na wyższym poziomie. Dzięki temu liderzy podmiotu mają pełny wgląd na ryzyko w całym podmiocie.

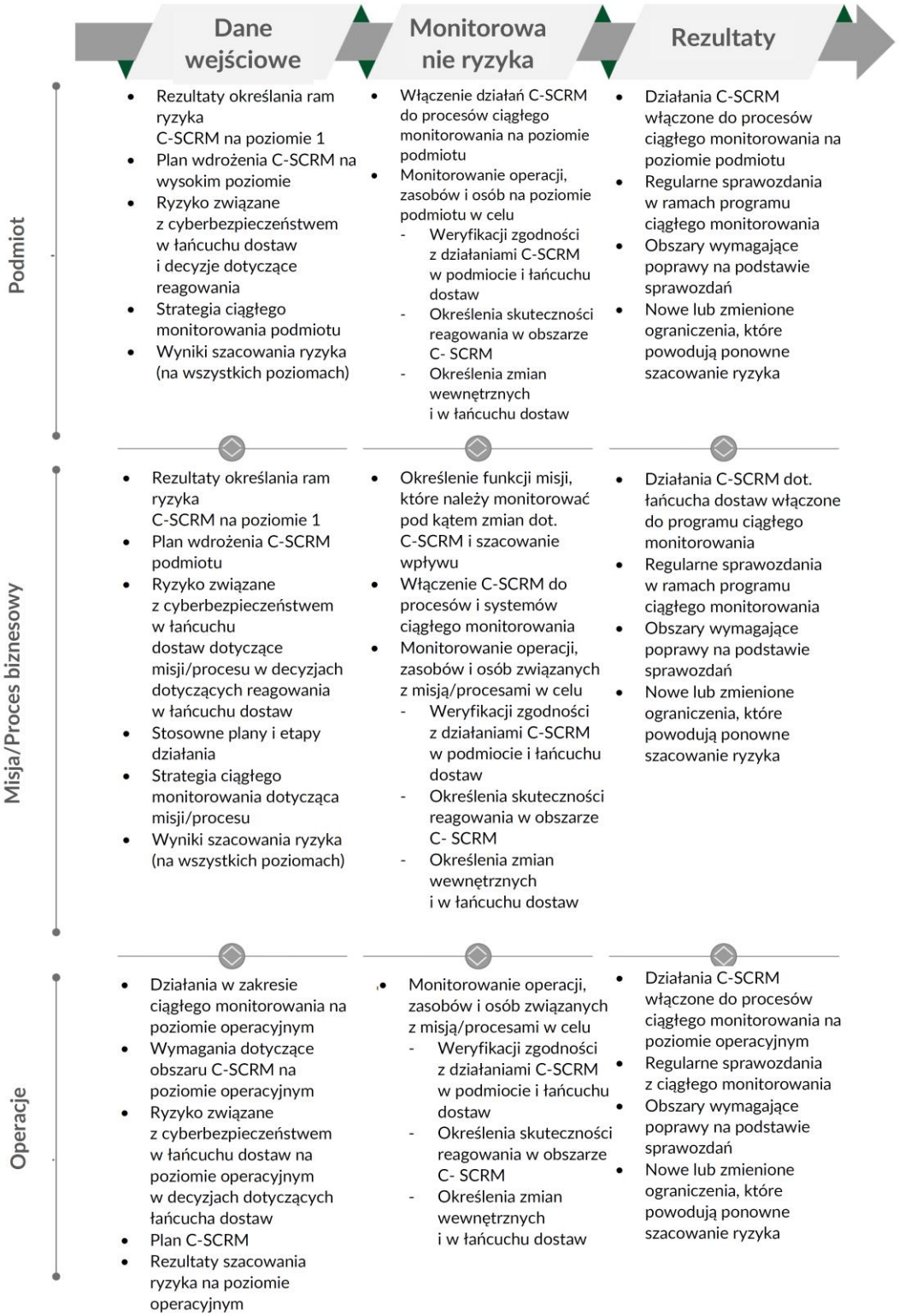
Podmioty powinny monitorować zdarzenia związane z ryzykiem w łańcuchu dostaw, aby stale oceniać ryzyko i określać odpowiednie reakcje. Monitorowanie powinno obejmować określenie, czy dane zdarzenie wywołało incydent lub wymusza potrzebę przekazania informacji. Przykłady zdarzeń związanych z ryzykiem w łańcuchu dostaw obejmują:

- fuzje, przejęcia, zmiany właścicieli podmiotów;
- przerwy w łańcuchu dostaw;
- zdarzenie związane z zachowaniem ciągłości lub zdarzenie awaryjne, które ma wpływ na dostawcę lub jego łańcuch dostaw;
- atak przy pomocy oprogramowania ransomware lub inny cyberatak, który ma wpływ na dostawcę lub jego łańcuch dostaw;

- nowe informacje o krytycznej podatności, która może mieć lub ma wpływ na technologię wykorzystywaną przez dostawcę lub jego łańcuch dostaw;
- wykrycie podrobionego lub niezgodnego z wymaganiami produktu lub komponentu;
- zmiana miejsca produkcji lub rozwoju oprogramowania, w szczególności zmiany z miejsc krajowych na zagraniczne;
- zaprzestanie produkcji lub wsparcia produktu lub krytycznego komponentu przez producenta;
- dowody na nieujawnioną funkcjonalność produktu;
- wszelkie informacje wymagające dodatkowego dochodzenia w celu ustalenia, czy poufność, integralność i dostępność danych i systemów informacyjnych podmiotu może być zagrożona w związku z atakiem obejmującym manipulację lub podrobienie produktów ICT;
- występowanie produktów wyprodukowanych przez producenta objętego sankcjami lub nieautoryzowanego;
- informacje o własności zagranicznej, kontroli lub wpływach obcych państw;
- inne zmiany, które mogą mieć negatywny wpływ na profil ryzyka dostawcy, produktu lub powiązanego łańcucha dostaw (np. utrata kluczowych pracowników, pogorszenie kondycji finansowej podmiotu, itd.).

Podmioty powinny włączyć działania dotyczące obszaru C-SCRM do istniejących programów ciągłego monitorowania[91]. W przypadku, gdy program ciągłego monitorowania nie istnieje, obszar C-SCRM może stanowić impuls dla ustanowienia kompleksowego programu ciągłego monitorowania. Rysunek G-7 przedstawia etap monitorowania ryzyka oraz jego dane wejściowe i rezultaty na trzech poziomach.

[91] NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (September 2011) opisuje proces opracowania i wdrożenia programu ciągłego monitorowania. Patrz http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf.



Rysunek G-8: Działania dotyczące obszaru C-SCRM na etapie monitorowania ryzyka[92]

[92] Bardziej szczegółowe informacje na temat procesu zarządzania ryzykiem można znaleźć w Załączniku C.

Działania

STRATEGIA MONITOROWANIA RYZYKA

ZADANIE 4-1: Opracowanie strategii monitorowania ryzyka dla podmiotu, która obejmuje cel, rodzaj i częstotliwość działań monitorujących.

Wytyczne uzupełniające

Podmioty powinny włączyć zagadnienia dotyczące obszaru C-SCRM do swojej ogólnej strategii monitorowania ryzyka. Monitorowanie zagrożeń dla cyberbezpieczeństwa w całym łańcuchu dostaw może wymagać dostępu do informacji, których podmioty mogą nie gromadzić. Niektóre informacje będą musiały zostać zebrane spoza podmiotu, w tym z ogólnodostępnych źródeł, od dostawców lub integratorów. Strategia powinna obejmować rodzaje gromadzonych danych, określać wskaźniki opracowywane na podstawie danych (np. liczba naruszeń postanowień umowy przez dostawcę), określać istniejące założenia dotyczące wymaganych narzędzi potrzebnych do gromadzenia danych, określać sposób ochrony danych oraz określać formaty raportowania danych. Potencjalne źródła danych mogą obejmować:

- Działania podmiotu w zakresie zarządzania podatnościami i incydentami.
- Przeglądy materiałów podmiotu.
- Wymianę informacji między podmiotami.
- Wymianę informacji z dostawcami, deweloperami, integratorami systemów, dostawcami zewnętrznych usług systemowych oraz innymi dostawcami usług związanych z ICT/OT.
- Wymianę informacji przez dostawców.
- Przeglądy dostawców, deweloperów, integratorów systemów, dostawców zewnętrznych usług systemowych oraz innych dostawców usług związanych z ICT/OT.

Podmioty powinny zapewnić odpowiednią ochronę danych dostawców, jeżeli dane te są gromadzone i przechowywane przez podmiot. Podmioty mogą również wymagać dodatkowych narzędzi do gromadzenia danych i analizy, aby odpowiednio analizować dane w celu monitorowania zagrożeń dla cyberbezpieczeństwa w całym łańcuchu dostaw.

MONITOROWANIE RYZYKA

ZADANIE 4-2: Bieżące monitorowanie systemów informacyjnych podmiotu i środowisk działania w celu weryfikacji zgodności, określenia skuteczności działań opracowanych w ramach reakcji na ryzyko oraz obserwacji zmian.

Zgodnie z dokumentem [NSC 800-39] podmioty powinny monitorować zgodność z politykami, skuteczność działań oraz zmiany. Monitorowanie zgodności w kontekście C-SCRM polega na monitorowaniu procesów realizowanych przez podmiot oraz dostarczanych produktów i usług pod kątem zgodności z ustalonymi wymogami bezpieczeństwa i C-SCRM. Monitorowanie skuteczności polega na monitorowaniu powstałego ryzyka w celu ustalenia, czy ustanowione wymagania w zakresie bezpieczeństwa i C-SCRM przynoszą zamierzone rezultaty. Monitorowanie zmian obejmuje monitorowanie środowiska pod kątem wszelkich zmian, które sygnalizowałyby konieczność dostosowania wymagań i środków bezpieczeństwa w celu utrzymania poziomu ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw na dopuszczalnym poziomie.

Aby monitorować zmiany, podmioty powinny określić częstotliwość regularnych przeglądów dostawców oraz dostarczanych przez nich produktów i usług. Częstotliwość przeglądów powinna być określona zgodnie z potrzebami podmiotu. Podmioty muszą również określić i udokumentować zestaw zdarzeń wskazujących na zmianę stanu ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw. Choć kategorie takich zdarzeń będą prawdopodobnie obejmować zmiany ograniczeń określonych w Tabeli D-6, takich jak polityka, misja, zmiany w środowisku zagrożeń, architektura korporacyjna, cykl życia systemu lub wymagania, konkretne zdarzenia w ramach tych kategorii mogą być różne dla różnych podmiotów.

Przykładem zmiany w łańcuchu dostaw w zakresie cyberbezpieczeństwa jest wyjście z rynku dwóch kluczowych dostawców[93], co prowadzi do niedoboru kluczowych komponentów. Takie zdarzenie wywołuje potrzebę oceny czy zmniejszenie liczby dostawców może prowadzić do podatności związanych z dostępnością i integralnością komponentów. W tym scenariuszu potencjalny deficyt komponentów może wynikać

[93] Sprawdzony dostawca to dostawca, z którym organizacja może swobodnie prowadzić interesy. Taki poziom komfortu osiąga się zwykle poprzez opracowanie określonego przez organizację zestawu kryteriów łańcucha dostaw, a następnie *weryfikację* dostawców pod kątem spełniania wymagań i kryteriów.

z niewystarczającej podaży. Jeśli żaden z pozostałych dostawców nie zostanie zweryfikowany, niedobór ten może skutkować obniżeniem integralności pozostałych komponentów. Jeżeli polityka podmiotu nakazuje stosowanie zweryfikowanych komponentów, zdarzenie to może spowodować, że podmiot nie będzie w stanie spełnić swoich potrzeb związanych z realizacją misji. Zmiana w łańcuchu dostaw może również wynikać ze zmiany właściciela podmiotu. Zmiana własności może nieść za sobą istotne konsekwencje, zwłaszcza w przypadkach, gdy zmiana ta wiąże się z przeniesieniem własności na osoby będące obywatelami innego kraju niż pierwotni właściciele.

Oprócz regularnego uaktualniania istniejących ocen ryzyka na wszystkich poziomach na podstawie wyników bieżącego monitorowania, podmiot powinien określić czynniki powodujące konieczność ponownego przeprowadzenia oceny. Niektóre z nich mogą obejmować dostępność zasobów, zmiany dotyczące ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw, klęski żywiołowe lub brak możliwości realizacji misji.

Aby monitorowanie było skuteczne, stan zarządzania ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw musi być przekazywany decydentom w całym podmiocie w postaci sprawozdań z działań C-SCRM. Sprawozdawczość powinna być dostosowana do potrzeb odbiorców. Sprawozdania dla decydentów poziomu 1 mogą podsumowywać zakres wdrożenia działań w obszarze C-SCRM, efektywność, skuteczność i ogólne poziomy narażenia na ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw na poszczególnych poziomach podmiotu. W stosownych przypadkach sprawozdawczość może koncentrować się na określonych obszarach poziomów 2 i 3, które wymagają uwagi kierownictwa wyższego szczebla. Aby pomóc w dostosowaniu sprawozdań do potrzeb odbiorców, wymogi dotyczące sprawozdawczości powinny być określane we współpracy z docelowymi odbiorcami i okresowo aktualizowane w celu zapewnienia, że są skuteczne i efektywne.

Rezultaty i warunki końcowe

Podmioty powinny uwzględniać rezultaty etapu monitorowania ryzyka w planach C-SCRM. Plany te stanowią element kolejnych iteracji poszczególnych kroków procesu FARM w zależności od potrzeb.

ZAŁĄCZNIK H SŁOWNIK

Załącznik H zawiera definicje pojęć z zakresu cyberbezpieczeństwa stosowane w publikacji.

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

Termin angielski	Termin polski	Definicja
acceptable risk	**akceptowalne ryzyko**	Poziom ryzyka szczątkowego dla operacji, aktywów lub pracowników organizacji, który mieści się w ramach apetytu na ryzyko i deklarowanej tolerancji ryzyka ustalonych przez organizację.
acquirer [ISO/IEC/IEEE 15288, adapted]	**nabywca** [ISO/IEC/IEEE 15288, termin dostosowany]	Organizacja /podmiot / organizacja nabywająca lub zamawiająca produkt lub usługę.
acquisition [NIST SP 800-64, adapted]	**nabycie/zamówienie** [NIST SP 800-64, termin dostosowany]	Obejmuje wszystkie etapy procesu nabywania produktów lub usług, począwszy od procesu określania zapotrzebowania na produkt lub usługi, a skończywszy na zawarciu i podpisaniu umowy.
agreement	**umowa**	Wzajemne uznanie warunków, na których odbywa się stosunek pracy lub przekazywanie towarów między stronami. Na przykład: kontrakt, porozumienie, uzgodnienie.
authorization boundary [NIST SP 800-53 Rev. 5]	**granica autoryzacji** [NIST SP 800-53 Rev. 5]	Wszystkie składniki systemu informacyjnego dopuszczone do eksploatacji przez osobę autoryzującą. Pojęcie to nie obejmuje systemów, do których podłączony jest dany system informacyjny.

Tłumaczenie

Termin angielski	Termin polski	Definicja
authorizing official [NIST SP 800-53 Rev. 5]	**osoba autoryzująca** [NIST SP 800-53 Rev. 5]	Osoba upoważniona do autoryzacji (tj. przyjmowania odpowiedzialności) działania systemu informacyjnego lub stosowania wyznaczonego zestawu wspólnych zabezpieczeń na akceptowalnym poziomie ryzyka dla działalności podmiotu (w tym misji, funkcji, wizerunku lub reputacji), aktywów podmiotu, osób, innych organizacji i państwa.
authorization to operate [NIST SP 800-53 Rev. 5]	**upoważnienie do działania** [NIST SP 800-53 Rev. 5]	Oficjalna decyzja wydana przez osobę autoryzującą, zezwalająca na działanie systemu informacyjnego i jednoznacznie akceptująca ryzyko dla działalności podmiotu (w tym misji, funkcji, wizerunku lub reputacji), aktywów podmiotu, osób, innych organizacji i państwa na podstawie wdrożenia uzgodnionego zestawu środków bezpieczeństwa i ochrony prywatności. Autoryzacja dotyczy również zabezpieczeń wspólnych dziedziczonych przez systemy informacyjne agencji.
baseline [CNSSI 4009]	**poziom bazowy** [CNSSI 4009]	Sprzęt, oprogramowanie, bazy danych i odpowiednia dokumentacja systemu informacyjnego w danym momencie.

Termin angielski	Termin polski	Definicja
C-SCRM control	**środek bezpieczeństwa związany z obszarem C-SCRM**	Zabezpieczenie lub środki przeciwdziałania mające na celu zmniejszenie lub wyeliminowanie prawdopodobieństwa bądź wpływu i konsekwencji ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw.
cybersecurity compromise in the supply chain	**naruszenie zasad ochrony cyberbezpieczeństwa w łańcuchu dostaw**	Zdarzenie związane z cyberbezpieczeństwem w łańcuchu dostaw (także naruszenie zasad ochrony / kompromitacja), w wyniku którego zagrożona jest poufność, integralność lub dostępność systemu lub informacji, które system przetwarza, przechowuje lub przesyła. Incydent w łańcuchu dostaw może wystąpić w dowolnym punkcie cyklu życia systemu, produktu lub usługi.
cybersecurity risks throughout the supply chain	**ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw**	Potencjał wyrządzenia szkód lub naruszenia zasad ochrony wynikający z działalności dostawców, ich łańcuchów dostaw, produktów lub usług. Ryzyko związane z cyberbezpieczeństwem w całym łańcuchu dostaw wynika z zagrożeń wykorzystujących podatności lub zagrożenia występujące w produktach i usługach, które przemieszczają się w całym łańcuchu dostaw, a także z zagrożeń wykorzystujących podatności lub zagrożenia występujące w samym łańcuchu dostaw.

Termin angielski	Termin polski	Definicja
cybersecurity supply chain risk assessment	**ocena ryzyka dotyczącego cyberbezpieczeństwa w łańcuchu dostaw**	Systematyczne badanie ryzyka związanego z cyberbezpieczeństwem w całym łańcuchu dostaw, prawdopodobieństwa jego wystąpienia oraz potencjalnych skutków.
cybersecurity supply chain risk management	**Zarządzanie ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw**	Systematyczny proces zarządzania ekspozycją na ryzyko związane z cyberbezpieczeństwem na każdym etapie łańcucha dostaw oraz opracowywania odpowiednich strategii reagowania, polityk, procesów i procedur. *Uwaga:* Na potrzeby publikacji NSC terminy SCRM i C-SCRM odnoszą się do tego samego pojęcia. Wynika to z faktu, że NSC 800-161 odnosi się jedynie do aspektów cyberbezpieczeństwa w ramach zarządzania ryzykiem w łańcuchu dostaw. Inne organizacje mogą stosować inną definicję zarządzania ryzykiem w łańcuchu dostaw, której nie obejmuje zakres niniejszej publikacji. Niniejsza publikacja nie omawia wielu aspektów SCRM, które nie są związane z cyberbezpieczeństwem.

Termin angielski	Termin polski	Definicja
defense-in-breadth [NIST SP 800-53 Rev. 5]	**rozszerzona ochrona** [NIST SP 800-53 Rev. 5]	Planowany, systematyczny zestaw działań w wielu obszarach, które mają na celu określenie ryzyka związanego z podatnościami możliwymi do wykorzystania na każdym etapie cyklu życia systemu, sieci lub komponentu, zarządzanie ryzykiem i jego ograniczanie; które obejmuje projektowanie i rozwój systemu, sieci lub produktu, produkcję, pakowanie, montaż, integrację, dystrybucję, eksploatację, utrzymanie oraz wycofanie z eksploatacji.
degradation	**degradacja**	Spadek jakości lub wydajności, w wyniku którego dochodzi do pogorszenia procesu.
developer [NIST SP 800-53 Rev. 5, adapted]	**deweloper** [NIST SP 800-53 Rev. 5, termin dostosowany]	Termin ogólny, który obejmuje twórców lub producentów systemów, komponentów systemowych lub usług systemowych; integratorów systemów; dostawców oraz sprzedawców produktów. Tworzenie systemów, komponentów systemów lub usług może odbywać się wewnętrznie w podmiotach lub za pośrednictwem podwykonawców zewnętrznych.
element	**element**	Patrz *element łańcucha dostaw*.
enhanced overlay	**rozszerzona nakładka**	Nakładka, która uwzględnia procesy, środki bezpieczeństwa, zabezpieczenia rozszerzone i dodatkowe wytyczne wdrożeniowe związane z jej celem.

Termin angielski	Termin polski	Definicja
exposure [ISO Guide 73, adapted]	**narażenie** [ISO Guide 73, termin dostosowany]	Zakres, w jakim organizacja lub interesariusz podlegają ryzyku.
external system service [NIST SP 800-53 Rev. 5]	**zewnętrzna usługa systemowa** [NIST SP 800-53 Rev. 5]	Usługa systemowa, która jest dostarczana przez dostawcę zewnętrznych usług i w przypadku której organizacja nie dysponuje środkami bezpieczeństwa i zabezpieczeniami prywatności lub oceną skuteczności zabezpieczeń.
External system service provider [NIST SP 800-53 Rev. 5]	**dostawca zewnętrznych usług systemowych** [NIST SP 800-53 Rev. 5]	Dostawca zewnętrznych usług systemowych na rzecz organizacji w ramach relacji między konsumentem i producentem, w tym przez wspólne przedsięwzięcia, partnerstwa biznesowe, umowy dotyczące outsourcingu (tj. umowy międzyorganizacyjne, ustalenia dotyczące linii biznesowych), umowy licencyjne i/lub wymiany w ramach łańcucha dostaw.
fit for purpose [ITIL Service Strategy, adapted]	**odpowiednie do celu [ITIL Service Strategy, termin dostosowany]**	Termin wykorzystywany do nieformalnego opisania procesu, elementu konfiguracji, usługi IT lub innych rozwiązań zdolnych do spełnienia swoich celów lub zapewnienia usługi na odpowiednim poziomie. Spełnienie tego wymogu wymaga odpowiedniego projektu, wdrożenia, zabezpieczeń oraz utrzymania.

Termin angielski	Termin polski	Definicja
ICT/OT-related service providers	**dostawcy usług związanych z ICT/OT**	Każda organizacja lub osoba fizyczna świadcząca usługi, które mogą obejmować autoryzowany dostęp do systemu ICT lub OT.
impact [NIST SP 800-53 Rev. 5]	**wpływ** [NIST SP 800-53 Rev. 5]	Wpływ utraty poufności, integralności lub dostępności informacji lub systemu na działania organizacyjne, aktywa organizacyjne, osoby fizyczne, inne organizacje lub państwo – w tym interesy bezpieczeństwa narodowego.
Information and Communications Technology [ISO/IEC 2382, adapted]	**technologie informacyjne i komunikacyjne (ICT)** [ISO/IEC 2382, termin dostosowany]	Obejmuje gromadzenie, przechowywanie, wyszukiwanie, przetwarzanie, wyświetlanie, reprezentację, prezentację, organizację, zarządzanie, bezpieczeństwo, przekazywanie i wymianę danych i informacji.
Information system [NIST SP 800-53 Rev. 5]	**system informacyjny** [NIST SP 800-53 Rev. 5]	Zestaw zasobów informacyjnych zorganizowanych w celu gromadzenia, przetwarzania, utrzymywania, wykorzystywania, udostępniania, rozpowszechniania oraz dysponowania informacjami.
life cycle [ISO/IEC/IEEE 15288, adapted]	**cykl życia** [ISO/IEC/IEEE 15288, termin dostosowany]	Rozwój systemu, produktu, usługi, projektu lub innej jednostki.
likelihood [ISO/IEC 27000]	**prawdopodobieństwo** [ISO/IEC 27000]	Szansa na wystąpienie danego wydarzenia.

Termin angielski	Termin polski	Definicja
materiality 1) U.S. Supreme Court in TSC Industries v. Northway, 426 U.S. 438, 449 (1976) 2) Commission Statement and Guidance on Public Company Cybersecurity Disclosures), SECURITIES AND EXCHANGE COMMISSION 17 CFR Parts 229 and 249 [Release Nos. 33-10459; 34-82746]	**istotność** 1) Sąd Najwyższy Stanów Zjednoczonych w sprawie TSC Industries v. Northway, 426 U.S. 438, 449 (1976) 2) Commission Statement and Guidance on Public Company Cybersecurity Disclosures), SECURITIES AND EXCHANGE COMMISSION 17 CFR Parts 229 and 249 [Release Nos. 33-10459; 34-82746]	1) Standard istotności opisany przez Sąd Najwyższy Stanów Zjednoczonych w sprawie TSC Industries v. Northway, 426 U.S. 438, 449 (1976) (fakt jest istotny, „jeżeli istnieje znaczne prawdopodobieństwo, że rozsądny akcjonariusz uznałby go za ważny" przy podejmowaniu decyzji inwestycyjnej lub jeżeli „byłby on postrzegany przez rozsądnego inwestora jako mający znaczący wpływ na ogół informacji udostępnionych akcjonariuszowi"). 2) Istotność ryzyk lub incydentów związanych z cyberbezpieczeństwem zależy od ich charakteru, zakresu oraz rozmiaru zniszczeń związanych z informacjami oraz działalnością podmiotu. Istotność ryzyka i incydentów związanych z cyberbezpieczeństwem zależy również od zakresu szkód, jakie takie incydenty mogą wyrządzić w systemach. Obejmuje on między innymi uszczerbek na reputacji firmy, wpływ na wyniki finansowe oraz relacje z klientami i sprzedawcami, a także ryzyko sporów sądowych lub dochodzeń, działań regulacyjnych podejmowanych przez organy publiczne oraz organy innych państw.
organizational user [NIST SP 800-53 Rev. 5, adapted]	**użytkownik organizacyjny** [NIST SP 800-53 Rev. 5, termin dostosowany]	Pracownik organizacji lub osoba fizyczna, którą organizacja uznała za posiadającą status zbliżony do pracownika, taki jak wykonawca, naukowiec lub pracownik innej organizacji w delegacji.

Termin angielski	Termin polski	Definicja
overlay [NIST SP 800-53 Rev. 5]	**nakładka** [NIST SP 800-53 Rev. 5]	Specyfikacja środków bezpieczeństwa lub prywatności, zabezpieczenia rozszerzone, dodatkowe wytyczne i inne informacje pomocnicze stosowane podczas procesu dostosowywania zabezpieczeń, które mają na celu uzupełnienie (i dalsze udoskonalenie) bazowych środków bezpieczeństwa. Specyfikacja nakładki może być bardziej lub mniej rygorystyczna niż pierwotna specyfikacja bazowa środków bezpieczeństwa i może być stosowana do wielu systemów informacyjnych.
pedigree	**rodowód**	Weryfikacja składników i pochodzenia technologii, produktów i usług. W przypadku urządzeń mikroelektronicznych obejmuje to wykaz elementów. W przypadku oprogramowania obejmuje to kod otwartoźródłowy oraz zastrzeżony, a także wersje komponentów w danym momencie w czasie. Rodowód zwiększa pewność, że zapewnienia dostawców dotyczące składu i pochodzenia dostarczanych przez nich produktów, usług i technologii są rzetelne.
program manager	**menadżer programu**	Patrz *osoba odpowiedzialna za system*.

Termin angielski	Termin polski	Definicja
provenance [NIST SP 800-53 Rev. 5]	**pochodzenie** [NIST SP 800-53 Rev. 5]	Chronologia pochodzenia, rozwoju, własności, lokalizacji i zmian systemu lub komponentu systemu oraz związanych z nim danych. Może również obejmować personel i procesy wykorzystywane do interakcji z systemem, komponentem lub powiązanymi danymi albo do wprowadzania w nich modyfikacji.
residual risk [NIST SP 800-16, adapted]	**ryzyko szczątkowe** [NIST SP 800-16, termin dostosowany]	Ryzyko istniejące po zastosowaniu zabezpieczeń/środków ograniczających ryzyko.
risk [NIST SP 800-39]	**ryzyko** [NIST SP 800-39]	Stopień, w jakim dany podmiot jest zagrożony przez potencjalne wystąpienie danej okoliczności lub danego zdarzenia, zwykle stanowiący wypadkową: (I) niekorzystnych skutków, które zaistniałyby w przypadku wystąpienia danej okoliczności lub danego zdarzenia; oraz (II) prawdopodobieństwa jego wystąpienia.
risk appetite [NISTIR 8286]	**apetyt na ryzyko** [NISTIR 8286]	Także gotowość do podejmowania ryzyka, poziom i rodzaje ryzyka, jakie organizacja jest skłonna zaakceptować w swoim dążeniu do osiągnięcia wartości.
risk framing [NIST SP 800-39]	**określanie ram ryzyka** [NIST SP 800-39]	Zbiór założeń, ograniczeń, tolerancji na ryzyko oraz priorytetów/wyborów, które kształtują podejście podmiotu do zarządzania ryzykiem.

Termin angielski	Termin polski	Definicja
risk management [NIST SP 800-53 Rev. 5]	**zarządzanie ryzykiem** [NIST SP 800-53 Rev. 5]	Program i procesy wspierające zarządzanie ryzykiem dla działalności podmiotu (w tym misji, funkcji, wizerunku, reputacji), aktywów podmiotu, osób, innych organizacji i państwa, obejmujące ustanowienie kontekstu dla działań związanych z ryzykiem, ocenę ryzyka, reagowanie na ryzyko po jego stwierdzeniu oraz monitorowanie ryzyka w czasie.
risk mitigation [NIST SP 800-53 Rev. 5]	**ograniczanie ryzyka** [NIST SP 800-53 Rev. 5]	Ustalanie priorytetów, ocena i wdrażanie odpowiednich zabezpieczeń/środków ograniczających ryzyko określonych w procesie zarządzania ryzykiem.
risk response [NIST SP 800-53 Rev. 5, adapted]	**reakcja na ryzyko** [NIST SP 800-53 Rev. 5, termin dostosowany]	Celowe i świadome decyzje oraz działania mające na celu akceptację, uniknięcie, złagodzenie, podział lub przeniesienie ryzyka.
risk response plan	**plan reakcji na ryzyko**	Podsumowanie potencjalnych konsekwencji udanego wykorzystania konkretnej podatności przez zagrożenie, a także strategie ograniczania ryzyka i środki bezpieczeństwa związane z obszarem C-SCRM.
risk tolerance [NIST 8286, adapted]	**tolerowanie ryzyka** [NIST 8286, termin dostosowany]	Gotowość organizacji lub interesariusza do ponoszenia ryzyka szczątkowego po realizacji reakcji na ryzyko z myślą o realizacji celów.
secondary market	**rynek wtórny**	Nieoficjalny, nieautoryzowany lub niezamierzony kanał dystrybucji.

Termin angielski	Termin polski	Definicja
security control **[NIST SP 800-53 Rev. 5]**	**środki bezpieczeństwa** [NIST SP 800-53 Rev. 5]	Zabezpieczenia lub środki zaradcze dotyczące systemu informacyjnego lub organizacji w celu ochrony poufności, integralności i dostępności systemu i jego informacji.
software bill of materials Exec. Order No. 14028, supra note 1, § 10(j)	**specyfikacje materiałowe komponentów oprogramowania** Exec. Order No. 14028, supra note 1, § 10(j)	Formalny dokument zawierający szczegóły i relacje w łańcuchu dostaw różnych komponentów używanych do opracowania danego oprogramowania. Twórcy i sprzedawcy oprogramowania często tworzą produkty poprzez łączenie istniejących otwartoźródłowych oraz komercyjnych komponentów oprogramowania. Specyfikacje materiałowe komponentów oprogramowania stanową listę komponentów wykorzystanych w produkcie.
supplier [ISO/IEC/IEEE 15288, adapted] [NIST SP 800-53 Rev. 5, adapted from definition of “developer”]	**dostawca** [ISO/IEC/IEEE 15288, termin dostosowany] [NIST SP 800-53 Rev. 5, termin dostosowany z definicji terminu „developer”]	Organizacja lub osoba, która zawiera umowę z nabywcą lub integratorem na dostawę produktu lub usługi. Pojęcie to obejmuje wszystkich dostawców w łańcuchu dostaw, twórców lub producentów systemów, komponentów systemu lub usług systemowych; integratorów systemów; dostawców; sprzedawców produktów; oraz partnerów zewnętrznych.

Termin angielski	Termin polski	Definicja
supply chain [ISO 28001, adapted]	**łańcuch dostaw** [ISO 28001, termin dostosowany]	Powiązany zestaw zasobów i procesów, a także wielu poziomów podmiotu. Każdy z nich jest nabywcą rozpoczynającym działania od pozyskania stosownych produktów i usług. Łańcuch dostaw rozciąga się na cały cykl życia produktu bądź usługi.
supply chain element	**element łańcucha dostaw**	Organizacje, podmioty lub narzędzia biorące udział w badaniach i rozwoju, projektowaniu, produkcji, nabywaniu, dostarczaniu, integracji, eksploatacji i konserwacji i/lub utylizacji systemów oraz ich komponentów.
supply chain risk information [FASCA]	**informacje o ryzyku związanym z łańcuchem dostaw** [FASCA]	Obejmuje, ale nie ogranicza się do informacji, które opisują lub identyfikują: 1) Funkcjonalność produktów, w tym dostęp do danych i przywileje systemu informacyjnego; 2) Informacje o środowisku użytkownika, w którym produkt jest używany lub instalowany 3) Zdolność dostawcy do wyprodukowania i dostarczenia produktów zgodnie z oczekiwaniami (tj. zapewnienie łańcucha dostaw); 4) Zagraniczna kontrola nad dostawcą lub wpływ na dostawcę (np. własność zagraniczna, powiązania osobiste i zawodowe między dostawcą a jakimkolwiek podmiotem zagranicznym, system prawny jakiegokolwiek obcego kraju, w którym dostawca ma siedzibę lub prowadzi działalność); 5) wpływ na bezpieczeństwo

Termin angielski	Termin polski	Definicja
		narodowe, bezpieczeństwo wewnętrzne lub kluczowe funkcje związane ze skorzystaniem z usług dostawcy; 6) podatność systemów, programów lub obiektów; 7) alternatywy rynkowe dla dostawcy; 8) potencjalny wpływ lub szkody spowodowane ewentualną utratą, uszkodzeniem lub kompromitacją produktu bądź usługi na misję organizacji; 9) prawdopodobieństwo wystąpienia potencjalnego wpływu lub szkody, a także możliwości wykorzystania podatności systemu 10) bezpieczeństwo, autentyczność i integralność produktu oraz łańcucha dostaw i kompilacji; 11) zdolność do ograniczenia zidentyfikowanego ryzyka; 12) wiarygodność i zaufanie do innych informacji dotyczących ryzyka w łańcuchu dostaw; 13) wszelkie inne informacje, które mogą być wykorzystane w analizie bezpieczeństwa, integralności, odporności, jakości, wiarygodności lub autentyczności produktów i dostawców; 14) podsumowanie powyższych informacji oraz wszelkie inne informacje uznane za istotne z punktu widzenia ryzyka łańcucha dostaw.

Termin angielski	Termin polski	Definicja
system [NIST SP 800-53 Rev. 5, adapted]	**system** [NIST SP 800-53 Rev. 5, termin dostosowany]	Połączenie współdziałających elementów zorganizowanych w celu realizacji jednego lub kilku określonych celów. *Uwaga 1:* Istnieje wiele rodzajów systemów. Przykłady obejmują systemy informacyjne ogólnego i specjalnego przeznaczenia; systemy dowodzenia, sterowania i łączności; moduły kryptograficzne; jednostki centralne oraz procesory graficzne; systemy sterowania przemysłowego; systemy kontroli lotu; systemy broni, celowania i kierowania ogniem; urządzenia medyczne i systemy leczenia; finansowe, bankowe i handlowe systemy transakcyjne; oraz systemy sieci społecznościowych. *Uwaga 2:* Występujące w definicji systemu współdziałające elementy obejmują sprzęt, oprogramowanie, dane, osoby fizyczne, procesy, obiekty, materiały i naturalnie występujące jednostki fizyczne. *Uwaga 3:* Pojęcie systemu systemów (*ang. System-of-systems*) jest ujęte w definicji systemu.
system assurance [NDIA]	**wiarygodność systemu** [NDIA]	Uzasadniona pewność, że system działa zgodnie z przeznaczeniem i jest wolny od podatności możliwych do wykorzystania, celowo lub niecelowo zaprojektowanych lub wprowadzonych do systemu w dowolnym momencie cyklu życia.

Termin angielski	Termin polski	Definicja
system component	**komponent systemu**	Oddzielny, możliwy do określenia element lub składnik systemu informacyjnego lub operacyjnego, który stanowi element składowy systemu. Może obejmować sprzęt, oprogramowanie i oprogramowanie sprzętowe.
system development life cycle [NIST SP 800-34 Rev. 1, adapted]	**cykl życia systemu** [NIST SP 800-34 Rev. 1, termin dostosowany]	Zakres działań związanych z systemem, obejmujący jego projektowanie, opracowanie i pozyskanie, wdrożenie, eksploatację i utrzymanie, a także utylizację.
system integrator	**integrator systemów**	Organizacje świadczące na rzecz podmiotów nabywających usługi dostosowane do ich potrzeb, w tym opracowywanie rozwiązań na zamówienie, testowanie, obsługę i konserwację.
system owner (or program manager) [NIST SP 800-53 Rev. 5]	**osoba odpowiedzialna za system (lub menadżer programu)** [NIST SP 800-53 Rev. 5]	Osoba odpowiedzialna za zaopatrzenie, rozwój, integrację, modyfikację lub eksploatację i utrzymanie systemu.
threat [NIST SP 800-53 Rev. 5]	**zagrożenie** [NIST SP 800-53 Rev. 5]	Wszelkie okoliczności lub zdarzenia mogące mieć negatywny wpływ na działalność organizacji, jej aktywa, pracowników, inne organizacje lub państwo w wyniku nieautoryzowanego dostępu, zniszczenia, ujawnienia, modyfikacji informacji lub odmowy świadczenia usługi.
threat analysis	**analiza zagrożeń**	Patrz *ocena zagrożenia*.

Termin angielski	Termin polski	Definicja
threat assessment [NIST SP 800-53 Rev. 5, adapted]	**ocena zagrożenia** [NIST SP 800-53 Rev. 5, termin dostosowany]	Formalny opis i ocena zagrożenia dla systemu lub organizacji.
threat event [NIST SP 800-30 Rev. 1]	**zdarzenie powodujące zagrożenie** [NIST SP 800-30 Rev. 1]	Zdarzenie lub sytuacja, które mogą potencjalnie spowodować niepożądane konsekwencje lub wpływ.
threat event outcome	**rezultat zdarzenia powodującego zagrożenie**	Wpływ zagrożenia związanego z podatnością na poufność, integralność bądź dostępność działań, aktywów oraz pracowników/ współpracowników podmiotu.
threat scenario [NIST SP 800-30 Rev. 1]	**scenariusz zagrożenia** [NIST SP 800-30 Rev. 1]	Zbiór częściowo uporządkowanych w czasie zdarzeń związanych z określonym potencjalnym lub zidentyfikowanym istniejącym źródłem zagrożenia lub wieloma źródłami zagrożenia.
threat source [NIST SP 800-53 Rev. 5]	**źródło zagrożenia** [NIST SP 800-53 Rev. 5]	Zamiar i metoda ukierunkowane na celowe wykorzystanie podatności lub sytuacja i metoda prowadząca do jej przypadkowego użycia.
transparency	**przejrzystość**	Patrz *widoczność*.
trust **[SwA]**	**ufność** [SwA]	Przekonanie, że inny element zachowa się zgodnie z oczekiwaniami.

Tłumaczenie

Termin angielski	Termin polski	Definicja
trustworthiness [NIST SP 800-53 Rev. 5, adapted]	**zaufanie** [NIST SP 800-53 Rev. 5, termin dostosowany]	Powiązanie cech osób, systemów lub podmiotów, które daje innym pewność co do kwalifikacji, możliwości i wiarygodności tego podmiotu w zakresie wykonywania określonych zadań i realizacji obowiązków. Stopień, w jakim można oczekiwać, że system i jego komponenty zachowają poufność, integralność i dostępność informacji przetwarzanych, przechowywanych lub przekazywanych przez system.
validation [ISO 9000]	**walidacja** [ISO 9000]	Potwierdzenie, że określone wymagania zostały spełnione, poprzez dostarczenie obiektywnych dowodów na konkretne działanie lub zastosowanie. *Uwaga:* Wymagania zostały spełnione.
verification [CNSSI 4009] [ISO 9000, adapted]	**weryfikacja** [CNSSI 4009] [ISO 9000, termin dostosowany]	Potwierdzenie, że określone wymagania zostały spełnione, poprzez dostarczenie obiektywnych dowodów. *Uwaga:* Zakładane dane wyjściowe są prawidłowe.
visibility [ISO/IEC 27036, adapted]	**widoczność** [ISO/IEC 27036, termin dostosowany]	Ilość informacji, które można zebrać o dostawcy, produkcie lub usłudze oraz możliwość uzyskania tych informacji w łańcuchu dostaw.
vulnerability [NIST SP 800-53 Rev. 5]	**podatność** [NIST SP 800-53 Rev. 5]	Słabość systemu informacyjnego, procedur bezpieczeństwa systemu, zabezpieczeń wewnętrznych lub wdrożenia, która może zostać wykorzystana lub uruchomiona przez źródło zagrożenia.

Termin angielski	Termin polski	Definicja
vulnerability assessment [NIST SP 800-53 Rev. 5, adapted]	**ocena podatności** [NIST SP 800-53 Rev. 5, termin dostosowany]	Systematyczne badanie systemu, produktu lub elementu łańcucha dostaw w celu określenia adekwatności środków bezpieczeństwa, identyfikacji braków w zakresie bezpieczeństwa, dostarczenia danych, na podstawie których można przewidzieć skuteczność proponowanych środków bezpieczeństwa oraz potwierdzenia adekwatności takich środków po ich wdrożeniu.

ZAŁĄCZNIK I AKRONIMY

Wybrane akronimy i skróty użyte w niniejszej publikacji zostały rozwinięte poniżej.

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

Akronim	Terminologia angielska	Terminologia polska
A&A	Assessment and Authorization	Ocena i autoryzacja
AO	Authorizing Official	Osoba autoryzująca
API	Application Programming Interface	Interfejs programistyczny aplikacji
APT	Advanced Persistent Threat	Zaawansowane zagrożenie trwałe
BIA	Business Impact Analysis	Analizy wpływu na działalność
BYOD	Bring Your Own Device	Przynieś własne urządzenie
CAC	Common Access Card	Karta dostępu
CAO	Chief Acquisition Officer	Kluczowa osoba w jednostce organizacyjnej odpowiedzialna za. zamówienia
CEO	Chief Executive Officer	Dyrektor generalny
CFO	Chief Financial Officer	Kluczowa osoba w jednostce organizacyjnej odpowiedzialna za. finanse
CIO	Chief Information Officer	Kluczowa osoba w jednostce organizacyjnej odpowiedzialna za technologie informacyjne
CISA	Cybersecurity and Infrastructure Security Agency	Agencja ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury
CISO	Chief Information Security Officer	Kluczowa osoba w jednostce organizacyjnej odpowiedzialna za

Akronim	Terminologia angielska	Terminologia polska
		bezpieczeństwo informacji
CISS	Cyber Incident Severity Schema	Schemat istotności incydentu związanego z cyberbezpieczeństwem
CLO	Chief Legal Officer	Kluczowa osoba w jednostce organizacyjnej odpowiedzialna za aspekty prawne
COO	Chief Operating Officer	Kluczowa osoba w jednostce organizacyjnej odpowiedzialna za Sprawy operacyjne
CPO	Chief Privacy Officer	Inspektor ochrony danych
CRO	Chief Risk Officer	Kluczowa osoba w jednostce organizacyjnej odpowiedzialna za określanie ryzyka
CSO	Chief Security Officer	Wyższe stanowisko kierownicze ds. bezpieczeństwa informacji
CTO	Chief Technology Officer	Wyższe stanowisko kierownicze technologii
CNSS	Committee on National Security Systems	Komitet ds. Krajowych Systemów Bezpieczeństwa
CNSSI	Committee on National Security Systems Instruction	Instrukcje wydawane przez CNSS
CUS	Continental United States	Kontynentalne Stany Zjednoczone
COSO	Committee of Sponsoring Organizations of the Treadway Commission	Dobrowolna organizacja sektora prywatnego

Akronim	Terminologia angielska	Terminologia polska
COTS	Commercial Off-The-Shelf	Rozwiązania komercyjne
CRO	Chief Risk Officer	Dyrektor ds. ryzyka
C-SCRM	Cybersecurity Supply Chain Risk Management	Zarządzanie ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw
CSF	Cybersecurity Framework	Ramy cyberbezpieczeństwa
CTO	Chief Technology Officer	Dyrektor ds. technologii
CUI	Controlled Unclassified Information	Kontrolowane informacje jawne
CVE	Common Vulnerability Enumeration	Słownik identyfikatorów odpowiadających powszechnie znanym podatnościom oraz zagrożeniom, a także standard ich nazewnictwa
CVSS	Common Vulnerability Scoring System	Wspólny system oceny podatności
CWE	Common Weakness Enumeration	Zestawienie typowych słabości
DHS	Department of Homeland Security	Departament Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych
DMA	Defense Microelectronics Activity	Defense Microelectronics Activity – laboratorium Departamentu Bezpieczeństwa Stanów Zjednoczonych
DoD	Department of Defense	Departament Obrony Stanów Zjednoczonych

Akronim	Terminologia angielska	Terminologia polska
DoDI	Department of Defense Instruction	Instrukcja Departamentu Obrony Stanów Zjednoczonych
ERM	Enterprise Risk Management	Zarządzanie ryzykiem w podmiocie
ERP	Enterprise Resource Planning	------
FAR	Federal Acquisition Regulation	Przepisy federalne dotyczące zamówień
FARM	Frame, Assess, Respond, Monitor	Program FARM dotyczący ryzyka
FASC	Federal Acquisition Security Council	Federalna rada ds. Bezpieczeństwa zamówień
FASCSA	Federal Acquisition Supply Chain Security Act	Federalna ustawa dotycząca bezpieczeństwa łańcuchów dostaw i zamówień
FBI	Federal Bureau of Investigation	Federalne Biuro Śledcze
FRAP	Federal Risk and Authorization Program	Federalny program dot. ryzyka i autoryzacji
FIPS	Federal Information Processing Standards	Federalne standardy przetwarzania informacji
FISMA	Federal Information Security Management Act	Federalna ustawa dotycząca zarządzania bezpieczeństwem informacji
FITARA	Federal Information Technology Acquisition Reform Act	Federalna ustawa dotycząca reformy systemu zamówień rozwiązań w zakresie technologii informacyjnych

Akronim	Terminologia angielska	Terminologia polska
FOCI	Foreign Ownership, Control or Influence	Zagraniczna własność, kontrola lub wpływy
FSCFP	Financial Services Cybersecurity Framework Profile	Profil ram cyberbezpieczeństwa usług finansowych
GAO	Government Accountability Office	Biuro Odpowiedzialności Rządu
GIDEP	Government-Industry Data Exchange Program	Rządowo-przemysłowy program wymiany danych
GOTS	Government Off-The-Shelf	Rozwiązania rządowe
GPS	Global Positioning System	Globalny system pozycjonowania
HR	Human Resources	Zasoby ludzkie, także kadry
IA	Information Assurance	Wiarygodność informacji
ICT	Information and Communication Technology	Technologie informacyjne i komunikacyjne
ICT/OT	Information, communications, and operational technology	Technologie informacyjne, komunikacyjne i operacyjne
IDE	Integrated Development Environment	Zintegrowane środowisko programistyczne
IDS	Intrusion Detection System	System wykrywania włamań
IEC	International Electrotechnical Commission	Międzynarodowa Komisja Elektrotechniczna
IOT	Internet of Things	Internet rzeczy
IP	Internet Protocol/Intellectual Property	Protokół internetowy/własność intelektualna
ISA	Information Sharing Agency	Agencja ds. wymiany informacji

Akronim	Terminologia angielska	Terminologia polska
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission	Międzynarodowa Organizacja Normalizacyjna/Międzynarodowa Komisja Elektrotechniczna
IT	Information Technology	Technologia informacyjna
ITIL	Information Technology Infrastructure Library	Biblioteka infrastruktury informatycznej
ITL	Information Technology Laboratory (NIST)	Laboratorium Technologii Informacyjnych (NIST)
JWICS	Joint Worldwide Intelligence Communications System	Wspólny światowy system łączności wywiadowczej
KPI	Key Performance Indicators	Kluczowy wskaźnik efektywności
KRI	Key Risk Indicators	Kluczowy wskaźnik ryzyka
KSA	Knowledge, Skills, and Abilities	Wiedza, umiejętności i zdolności
MECE	Mutually Exclusive and Collectively Exhaustive	Wzajemnie wykluczające się i wyczerpujące
NISPOM	National Industrial Security Program Operating Manual	Podręcznik operacyjny krajowego programu bezpieczeństwa przemysłowego
NIST	National Institute of Standards and Technology	Narodowy Instytut Standardów i Technologii
NCCIC	National Cybersecurity and Communications Integration Center	Krajowe Centrum Integracji Cyberbezpieczeństwa i Łączności
NDI	Non-developmental Items	Produkty nierozwojowe

Akronim	Terminologia angielska	Terminologia polska
NDIA	National Defense Industrial Association	Krajowe Stowarzyszenie Przemysłu Obronnego
NIAP	National Information Assurance Partnership	Krajowe partnerstwo na rzecz bezpieczeństwa informacji
NICE	National Initiative for Cybersecurity Education	Krajowa inicjatywa na rzecz edukacji w zakresie cyberbezpieczeństwa
NISTIR	National Institute of Standards and Technology Interagency or Internal Report	Raport międzyagencyjny lub wewnętrzny Narodowego Instytutu Standardów i Technologii
OCONUS	Outside of Continental United States	Poza kontynentalnymi Stanami Zjednoczonymi
OEM	Original Equipment Manufacturer	Producent oryginalnego wyposażenia
OGC	Office of the General Counsel	Biuro Prokuratora Generalnego
OMB	Office of Management and Budget	Office of Management and Budget – Biuro Zarządzania i Budżetu
OPSEC	Operations Security	Bezpieczeństwo operacyjne
OSS	Open Source Solutions	Rozwiązania otwartoźródłowe
OSY	Office of Security	Office of Security – Biuro Bezpieczeństwa
OT	Operations Technology	Technologia operacyjna
OTS	Off-The-Shelf	Rozwiązanie komercyjne

Akronim	Terminologia angielska	Terminologia polska
OTTF	Open Group Trusted Technology Forum	Open Group Trusted Technology Forum – nazwa własna organizacji
O-TTPS	Open Trusted Technology Provider™ Standard	Open Trusted Technology Provider™ Standard – nazwa własna normy
OWASP	Open Web Application Security Project	Open Web Application Security Project – nazwa własna projektu
PACS	Physical Access Control System	System kontroli dostępu fizycznego
PII	Personally Identifiable Information	Dane osobowe
PIV	Personal Identity Verification	Weryfikacja tożsamości
PM	Program Manager	Menedżer programu
PMO	Program Management Office	Biuro Zarządzania Programu
POA&M	Plan of Action & Milestones	Plan i etapy działania
QA/QC	Quality Assurance/Quality Control	Zapewnienie jakości/kontrola jakości
R&D	Research and Development	Badania i rozwój
RFI	Request for Information	Wniosek o udzielenie informacji
RFP	Request for Proposal	Zapytanie ofertowe
RFQ	Request for Questions	Zapytanie ofertowe
RMF	Risk Management Framework	Ramy zarządzania ryzykiem
SAFECode	Software Assurance Forum for Excellence in Code	Software Assurance Forum for Excellence in Code – nazwa organizacji

Akronim	Terminologia angielska	Terminologia polska
SBOM	Software Bill of Materials	Specyfikacja materiałowa komponentów oprogramowania
SCIF	Sensitive Compartmented Information Facility	Obiekt zawierający informacje szczególnie chronione
SCRI	Supply Chain Risk Information	Informacje o ryzyku związanym z łańcuchem dostaw
SCRM	Supply Chain Risk Management	Zarządzanie ryzykiem w łańcuchu dostaw
SCRSS	Supply Chain Risk SeveritySchema	Schemat istotności ryzyka w łańcuchu dostaw
SDLC	System Development Life Cycle	Cykl życia systemu
SECURE	Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (Technology Act)	Wzmocnienie i zwiększenie zdolności cybernetycznych poprzez wykorzystanie narażenia na ryzyko (ustawa technologiczna)
SLA	Service-Level Agreement	Umowa o gwarancji świadczenia usług
SME	Subject Matter Expert	Specjalista
SOO	Statement of Objective	Oświadczenie o celu
SOW	Statement of Work	Wykaz prac
SP	Special Publication (NIST)	Publikacja specjalna NIST
SSP	System Security Plan	Plan bezpieczeństwa systemu
SWA	Software Assurance	Zapewnianie jakości oprogramowania
SWID	Software Identification Tag	Identyfikator oprogramowania

Akronim	Terminologia angielska	Terminologia polska
TTP	Tactics, Techniques, and Procedures	Taktyki, Techniki i Procedury
USA	United States (of America)	Stany Zjednoczone Ameryki Północnej
US CERT	United States Computer Emergency Readiness Team	Zespół Reagowania na Incydenty Komputerowe Stanów Zjednoczonych
VDR	Vulnerability Disclosure Report	Sprawozdanie z ujawnienia podatności

ZAŁĄCZNIK J ŹRÓDŁA

Związek z innymi programami i publikacjami[94]

NSC 800-161 opiera się na koncepcjach opisanych w szeregu publikacji NIST oraz innych dokumentach, aby ułatwić integrację z innymi działaniami jednostek w skali całych podmiotów. Materiały te wzajemnie się uzupełniają i pomagają podmiotom w budowaniu programów bezpieczeństwa informacji opartych na ryzyku w celu ochrony ich operacji i aktywów przed szeregiem różnorodnych i coraz bardziej wyrafinowanych zagrożeń. Niniejsza publikacja będzie weryfikowana w celu zachowania spójności z katalogiem zabezpieczeń NSC 800-53 przy użyciu procesu iteracyjnego w miarę rozwoju obszaru C-SCRM.

PUBLIKACJE NIST

W niniejszym dokumencie wykorzystano najnowsze wersje publikacji i programów, które stanowiły podstawę do jego opracowania, a także nowe publikacje, które pojawiły się po pierwotnym wydaniu niniejszego dokumentu:

- NIST Cybersecurity Framework (CSF) Version 1.1,
- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, w celu przeprowadzenia analizy krytyczności oraz określenia zakresu działań w obszarze C-SCRM dla kluczowych komponentów i systemów [FIPS 199][95].
- NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments*, w celu włączenia zagadnień związanych z zarządzaniem ryzykiem w łańcuchu dostaw ICT/OT do procesu oceny ryzyka [NIST SP 800-30, Rev. 1][96].
- NIST SP 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy [NIST SP 800-37, Rev. 2][97].

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

[95] Publikacja w języku polskim -NSC 199.

[96] Publikacja w języku polskim -NSC 800-30.

[97] Publikacja w języku polskim - NSC 800-37.

- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, to integrate ICT/OT SCRM into the risk management levels and risk management process [NIST SP 800-39][98].
- NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, w celu zapewnienia środków bezpieczeństwa informacji na potrzeby ich dostosowania do kontekstu zagadnień C-SCRM [NIST SP 800-53, Rev. 5][99].
- NIST SP 800-53B, *Control Baselines for Information Systems and Organizations* w celu określenia poziomów bazowych środków bezpieczeństwa oraz dodatkowych wytycznych dla zagadnień C-SCRM [NIST SP 800-53B][100].
- NIST SP 800-150, *Guide to Cyber Threat Information Sharing*, w celu ustanowienia wytycznych dotyczących tworzenia oraz uczestnictwa w relacjach dotyczących przekazywania informacji o zagrożeniach [NIST SP 800-150],
- NIST SP 800-160 Vol. 1, *Systems Security Engineering* [NIST SP 800-160 Vol. 1] oraz NIST SP 800-160 Vol. 2, Rev. 1, *Developing Cyber Resilient Systems: A Systems Security Engineering Approach* [NIST SP 800-160 Vol. 2] w celu pozyskania wytycznych dotyczących inżynierii bezpieczeństwa w zakresie zagadnień C-SCRM,
- NIST SP 800-171, Rev. 2, *Protecting Controlled Information in Non-federal Systems and Organizations*, w celu pozyskania zalecanych wymogów dotyczących bezpieczeństwa w celu ochrony poufności CUI [NIST SP 800-171, Rev. 2],
- NIST SP 800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information* - A Supplement to NIST Special Publication 800-171, w celu ustalenia zalecanych zabezpieczeń rozszerzonych na potrzeby ochrony poufności CUI [NIST SP 800-172],

[98] Publikacja w języku polskim - NSC 800-39.

[99] Publikacja w języku polskim - NSC 800-53.

[100] Publikacja w języku polskim - NSC 800-53B.

- NIST SP 800-181, Rev. 1, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* w celu utworzenia wspólnego glosariusza dotyczącego zagadnień C- SCRM dla pracowników [NIST SP-800-181, Rev. 1],
- NISTIR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems*, jako źródło materiałów dodatkowych dotyczących stosowania publikacji do konkretnych procesów zamówień [NISTIR 7622],
- NISTIR 8179, *Criticality Analysis Process Model: Prioritizing Systems and Components*, w celu wspierania oceny krytyczności dostawców [NISTIR 8179],
- NISTIR 8276, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*, aby wyjaśnić najnowsze trendy w zakresie zagadnień C-SCRM w sektorze prywatnym [NISTIR 8276],
- NISTIR 8286, *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (ERM)*, w celu uzupełnienia treści dotyczących włączenia zagadnień C-SCRM do procesów zarządzania ryzykiem podmiotu [NISTIR 8286].

PRAWO ORAZ WYTYCZNE LEGISLACYJNE[101]

Niniejszy dokument jest w dużym stopniu oparty na wydanych prawach oraz wydanych regulacjach, w tym:

- Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Internal Control*,
- Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*,
- The Federal Acquisition Supply Chain Security Act (FASCA), Title II of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE) Technology Act of 2018,
- Public Law 115-232 § 889, Prohibition on Contracting Certain

[101] Akty obowiązujące w amerykańskim systemie prawnym i nie mają odpowiednika w polskim porządku prawnym. Treść aktów może być pomocna przy tworzeniu stosownych polityk.

Telecommunications and Video Surveillance Services or Equipment,

- Federal Register, Vol. 84, No. 156, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment, August 13, 2019,
- FAR Part 4, Subpart 4.20, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab,
- (GAO), Challenges and Policy Considerations Regarding Offshoring and Foreign Investment Risks, September 2019,
- Executive Order 14028, Improving the Nation's Cybersecurity, May 12, 2021,
- Securities and Exchange Commission 17 CFR Parts 229 and 249 [Release Nos. 3310459; 34-82746] *Commission Statement and Guidance on Public Company Cybersecurity Disclosures.*

INNE SPRAWOZDANIA OPRACOWANE PRZEZ RZĄD STANÓW ZJEDNOCZONYCH

Dokument jest oparty na sprawozdaniach rządowych:

- Government Accountability Office (GAO) Report, Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks, December 2020, GAO-21-171 [GAO],
- Department of Defense and Department of Homeland Security Software Assurance Acquisition Working Group, Software Assurance in Acquisition: Mitigating Risks to the Enterprise [SwA],
- National Defense Industrial Association (NDIA), Engineering for System Assurance [NDIA].

NORMY, WYTYCZNE I NAJLEPSZE PRAKTYKI

Dodatkowo dokument [NSC 800-161] czerpie inspirację z wielu międzynarodowych standardów, wytycznych i dokumentów dotyczących najlepszych praktyk, w tym:

- The Federal Risk and Authorization Management Program (FedRAMP), *Securing Cloud Services For The Federal Government* [https://www.fedramp.gov/],

- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15288 - *Systems and software engineering - System Life Cycle Processes* [ISO/IEC 15288],
- ISO/IEC 27036 - Information Technology - Security Techniques - Information Security for Supplier Relationships [ISO/IEC 27036],
- ISO/IEC 20243 - Information Technology - Open Trusted Technology Provider™ Standard (O-TTPS) - Mitigating maliciously tainted and counterfeit products [ISO/IEC 20243],
- ISO/IEC 27000 - Information Technology - Security Techniques - Information Security Management System - Overview and Vocabulary [ISO/IEC 27000],
- ISO/IEC 27002 - Information Technology - Security Techniques - Code of Practice for Information Security Controls [ISO/IEC 27002],
- Software Assurance Forum for Excellence in Code (SAFECode) *Software Integrity Framework* [SAFECode 2] oraz *Software Integrity Best Practices* [SAFECode 1],
- Cyber Risk Institute, Financial Services Cybersecurity Framework Profile Version 1.1 [FSP].