Ministerstwo Cyfryzacji

NARODOWY STANDARD CYBERBEZPIECZEŃSTWA
NSC 800-12

4 sierpnia 2023

Bezpieczeństwo informacji — wprowadzenie

Publikacja dostępna pod adresem:

Narodowe Standardy Cyberbezpieczeństwa

PREAMBUŁA

Szanowni Państwo,

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

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

Niniejszy podręcznik NSC 800-12, ***Bezpieczeństwo informacji — wprowadzenie***, opracowany został za zgodą National Institute of Science and Technology na podstawie publikacji NIST SP 800-12, *An Introduction to Information Security*.

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

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

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

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

WSPÓLNE FUNDAMENTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

National Institute of Standards and Technology (NIST) opracował szereg standardów i wytycznych w celu zapewnienia jednolitego podejścia do problematyki bezpieczeństwa informacji i systemów informacyjnych administracji federalnej USA. Podstawową rolę w podejściu do zagadnień związanych z zapewnieniem bezpieczeństwa informacji i systemów informacyjnych oraz ochrony prywatności odgrywa elastyczny i spójny sposób zarządzania ryzykiem związanym z bezpieczeństwem ,prywatnością działalności i majątku organizacji. Dotyczy to również osób fizycznych i państwa.

Zarządzanie ryzykiem stanowi podstawę do wdrożenia stosownych zabezpieczeń w systemach informacyjnych, ocenę tych zabezpieczeń, wzajemną akceptację dowodów oceny bezpieczeństwa i ochrony prywatności oraz decyzji autoryzacyjnych. Dzięki jednolitemu podejściu do zarządzania ryzykiem ułatwia także wymianę informacji i współpracę pomiędzy różnymi podmiotami.

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

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

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

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

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

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

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

 Narodowe Standardy Cyberbezpieczeństwa

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

 +48222455922

 sekretariat.dc@cyfra.gov.pl

Raporty dotyczące technologii systemów komputerowych

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

Streszczenie

Organizacje w swojej codziennej działalności w dużym stopniu wykorzystują produkty i usługi z zakresu technologii informatycznych. Zapewnienie bezpieczeństwa tych produktów i usług ma ogromne znaczenie dla sukcesu organizacji. W niniejszej publikacji przedstawiono zasady bezpieczeństwa informacji, które organizacje mogą wykorzystać do określenia potrzeb związanych z osiąganiem bezpieczeństwa informacji w swoich systemach.

Słowa kluczowe

Wiarygodność (*ang. assurance*); bezpieczeństwo komputerowe (*ang. computer security*) bezpieczeństwo informacji (*ang. information security*); wprowadzenie (*ang. introduction*) ; zarządzanie ryzykiem (*ang. risk management*); zabezpieczenia (*ang. security controls*); wymagania bezpieczeństwa (*ang. security requirements*)

Spis treści

Spis ilustracji

1. WPROWADZENIE

1.1 Cel

Publikacja ta służy jako punkt wyjścia dla osób początkujących w dziedzinie bezpieczeństwa informacji, jak również dla osób nieznających wytycznych i rekomendacji dotyczących bezpieczeństwa informacji. Celem tej specjalnej publikacji jest zapewnienie ogólnego przeglądu zasad bezpieczeństwa informacji poprzez przedstawienie powiązanych koncepcji i grup środków bezpieczeństwa (określonych w publikacji NSC 800-53 wer. 2[2]), które organizacje mogą wykorzystać do skutecznego zabezpieczenia swoich systemów[3] i informacji. Aby pomóc w lepszym zrozumieniu znaczenia i celu opisanych kategorii środków bezpieczeństwa, niniejsza publikacja rozpoczyna się od zapoznania czytelnika z różnymi zasadami bezpieczeństwa informacji.

Po wprowadzeniu do zasad bezpieczeństwa w kolejnych częściach publikacji opisano szczegółowo wiele kategorii środków bezpieczeństwa, a także zalety każdej z nich. Celem nie jest narzucenie organizacjom wymogów, ale zbadanie możliwości wykorzystania dostępnych technik do zastosowania określonej grupy środków bezpieczeństwa w systemie organizacji oraz wyjaśnienie korzyści wynikających z zastosowania wybranych środków.

Ponieważ niniejsza publikacja stanowi wprowadzenie do bezpieczeństwa informacji, nie uwzględniono w niej szczegółów dotyczących sposobu wdrażania środków bezpieczeństwa ani sprawdzania ich skuteczności. Zamiast tego zamieszczono w niej odniesienia do innych publikacji, które zawierają bardziej szczegółowe informacje na dany temat.

[2] NSC 800-53 bazuje na publikacji specjalnej NIST 800-53 rev. 5, *Security and Privacy Controls for Federal Information Systems and Organizations*.

[3] System został zdefiniowany w publikacji NSC 800-53 jako każdy zorganizowany zespół zasobów i procedur połączonych i regulowanych przez interakcję lub współzależność w celu osiągnięcia zestawu określonych funkcji.

1.2 Docelowi odbiorcy

Docelowymi odbiorcami tej publikacji są osoby, które dopiero poznają zasady i założenia bezpieczeństwa informacji, niezbędne do ochrony informacji i systemów w sposób współmierny do ryzyka. Publikacja ta może stanowić podstawę koncepcji i pomysłów dla każdej osoby, której zadaniem jest zabezpieczanie systemów lub która chce zrozumieć sposoby zabezpieczania systemów.

Dlatego publikacja ta jest dobrym źródłem informacji dla każdego, kto szuka lepszego zrozumienia podstaw bezpieczeństwa informacji lub ogólnego przeglądu tego zagadnienia. Wskazówki i techniki opisane w tej publikacji mogą być stosowane do każdego rodzaju informacji lub systemu w każdym rodzaju organizacji. Mogą istnieć różnice w sposobie przetwarzania, przechowywania i rozpowszechniania informacji w systemach organizacji publicznych, akademickich i sektora prywatnego, jednak podstawowe zasady bezpieczeństwa informacji mają zastosowanie w każdym z nich.

1.3 Organizacja publikacji

Niniejsza publikacja ma następującą strukturę:

- W rozdziale 1 opisano cel, docelowych odbiorców, ważne terminy, podstawy prawne bezpieczeństwa informacji oraz listę publikacji NIST[4] związanych z bezpieczeństwem informacji i zarządzaniem ryzykiem dotyczącym informacji.
- W rozdziale 2 wymieniono osiem głównych elementów dotyczących bezpieczeństwa informacji.
- W rozdziale 3 przedstawiono szereg ról, ról pomocniczych oraz przypisanych im obowiązków związanych z zapewnieniem bezpieczeństwa informacji w organizacji.
- W rozdziale 4 przedstawiono zagrożenia i podatności na zagrożenia, różnice między nimi oraz podano przykłady różnych źródeł zagrożeń i niebezpiecznych zdarzeń.

[4] Przedstawione w tym poradniku wszelkie odniesienia do dodatkowych publikacji skierowane są do osób zainteresowanych chcących poszerzyć swoją wiedzę.

- W rozdziale 5 omówiono polityki bezpieczeństwa informacji oraz różnice między polityką programową, polityką dotyczącą konkretnych zagadnień i polityką dotyczącą konkretnych systemów.
- W rozdziale 6 opisano, jak zarządzać ryzykiem i krótko scharakteryzowano sześć kroków zarządzania ryzykiem (ang. *Risk Management Framework – RMF*).
- W rozdziale 7 skupiono się na zapewnieniu bezpieczeństwa informacji oraz na tym, jakie środki można podjąć w celu ochrony informacji i systemów.
- W rozdziale 8 przedstawiono obsługę, wsparcie i operacje systemowe, które wspólnie funkcjonują, aby zapewnić sprawne działanie systemu.
- W rozdziale 9 przedstawiono krótki przegląd zagadnień związanych z kryptografią, a także kilka publikacji NIST z serii 800, które zawierają dodatkowe, bardziej szczegółowe informacje na temat konkretnych technologii kryptograficznych.
- W rozdziale 10 przedstawiono 20 kategorii środków bezpieczeństwa informacji i prywatności.
- Załącznik A zawiera bibliografię.
- Załącznik B zawiera słownik terminów używanych w dokumencie.
- Załącznik C zawiera listę akronimów i skrótów stosowanych w publikacji.

1.4 Ważne terminy

Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2023 r. poz. 913), system informacyjny to system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy z dnia z dnia 1 grudnia 2022 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2023 r. poz. 57 z późn. zm.), wraz z przetwarzanymi w nim danymi w postaci elektronicznej.

W publikacji termin *system informacyjny* (dalej: *system)*, definiowany jest jako dyskretny zbiór zasobów informacyjnych o dowolnej wielkości i złożoności, zorganizowanych w celu gromadzenia informacji, ich przetwarzania, wykorzystywania, udostępniania, rozpowszechniania, utrzymywania albo dysponowania danymi lub informacjami.

Kilka innych kluczowych terminów, z którymi należy się zapoznać, to:

- Informacja – (1) fakty lub idee, które mogą być wyrażone (zakodowane) w postaci różnych form danych; (2) wiedza (np. dane, instrukcje) zapisana na dowolnym nośniku i dowolnej formie, która może być przekazywana między jednostkami systemu.
- Bezpieczeństwo informacji – ochrona informacji i systemów informacyjnych przed nieuprawnionym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem działania, modyfikacją lub zniszczeniem w celu zapewnienia poufności, integralności i dostępności.
- Poufność – stosowanie zatwierdzonych ograniczeń w dostępie do informacji i ich ujawnianiu, w tym środków ochrony prywatności i informacji wrażliwych.
- Integralność – zabezpieczenie przed niewłaściwą modyfikacją lub zniszczeniem informacji oraz zapewnienie ich niezaprzeczalności i autentyczności.
    - ✓ Integralność danych – właściwość polegająca na tym, że dane nie zostały zmienione w nieuprawniony sposób. Integralność danych dotyczy danych przechowywanych, przetwarzanych i przesyłanych.
    - ✓ Integralność systemu – właściwość, którą ma system, gdy wykonuje on swoją zamierzoną funkcję w sposób niezakłócony, bez możliwości nieautoryzowanej manipulacji, zarówno celowej, jak i przypadkowej.
- Dostępność – zapewnienie terminowego i niezawodnego dostępu do informacji i ich wykorzystania.
- Środki bezpieczeństwa[5] – przedsięwzięcia zarządcze, operacyjne i technologiczne (tj. zabezpieczenia lub środki zaradcze) przewidziane dla systemu w celu ochrony poufności, dostępności i integralności systemu i zawartych w nim informacji.

[5] W dokumencie terminy środki bezpieczeństwa (*ang. security controls*), zabezpieczenia (*ang. safeguards*) i środki ochrony (*ang. security measures*) są stosowane zamiennie.

1.5 Powiązane publikacje NSC i NIST[6]

W zakresie bezpieczeństwa informacji i zarządzania ryzykiem rekomenduje się zestaw Narodowych Standardów Cyberbezpieczeństwa opracowany na bazie standardów przetwarzania informacji (ang. *Federal Information Processing Standard – FIPS*) oraz publikacji specjalnych (ang. *Special Publications – SP*) NIST. Obejmują one[7]:

- NSC 199, *Standardy kategoryzacji bezpieczeństwa*, opracowany na podstawie FIPS 199 - *Standards for Security Categorization of Federal Information and Information Systems*. Zawiera listę standardów kategoryzacji informacji i systemów, która zapewnia wspólne ramy i zrozumienie wyrażania bezpieczeństwa w sposób, który sprzyja skutecznemu zarządzaniu i spójnej sprawozdawczości.
- NSC 200, *Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych*, opracowany na podstawie FIPS 200 - *Minimum Security Requirements for Federal Information and Information Systems*. Określa minimalne wymagania bezpieczeństwa dla informacji i systemów, które są wykorzystywane przez organizacje wykonawcze, oraz oparty na ryzyku proces wyboru środków bezpieczeństwa niezbędnych do spełnienia minimalnych wymagań bezpieczeństwa.
- NSC 800-18, *Przewodnik do opracowywania planów bezpieczeństwa systemów informacyjnych w podmiotach publicznych*, opracowany na podstawie NIST SP 800-18 – *Guide for Developing Security Plans for Systems*. Zawiera procedury opracowywania planu bezpieczeństwa systemu i przegląd wymagań dotyczących bezpieczeństwa systemu oraz opisuje istniejące lub planowane środki mające na celu spełnienie tych wymagań.
- NSC 800-30, *Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne*, opracowany na podstawie NIST SP 800-30 – *Guide for Conducting Risk Assessments*. Zawiera wskazówki dotyczące szacowania ryzyka dla systemów i organizacji.

[6] Publikacje zostały podane w celach uzupełniających dla osób zainteresowanych.
[7] Publikacje zawarte w sekcji 1.5 mają swoje polskie odpowiedniki wydane jako Narodowe Standardy Cyberbezpieczeństwa - Baza wiedzy - Portal Gov.pl (www.gov.pl)

- NSC 800-34, *Poradnik planowania awaryjnego*, opracowany na podstawie NIST SP 800-34 – *Contingency Planning Guide for Federal Information Systems*. Zapewnia pomoc organizacji w zrozumieniu celu, procesu i formatu opracowywania planu awaryjnego dla systemów informacyjnych (*Information System Contingency Plan – ISCP*) prezentując praktyczne, sprawdzone instrukcje.
- NSC 800-37, Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu, opracowany na podstawie NIST SP 800-37 – *Guide for Applying the Risk Management Framework to Systems: A Security Life Cycle Approach*. Zawiera rekomendacje dotyczące stosowania zarządzania ryzykiem w systemach, w tym prowadzenia działań w zakresie kategoryzacji zabezpieczeń, wyboru i wdrażania środków bezpieczeństwa, oceny środków bezpieczeństwa, autoryzacji systemu oraz monitorowania środków bezpieczeństwa.
- NSC 800-39, Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego, na podstawie NIST SP 800-39- *Managing Information Security Risk: Organization, Mission, and Information System View*. Zawiera rekomendacje umożliwiające przygotowanie zintegrowanego, obejmującego całą organizację programu zarządzania ryzykiem związanym z bezpieczeństwem informacji dla działalności organizacji (np. misji, funkcji, wizerunku i reputacji), aktywów, osób, innych organizacji i państwa, wynikającego z działania i użytkowania systemów.
- NSC 800-53, Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji, opracowany na podstawie NIST SP 800-53 – Security and Privacy Controls for Systems and Organizations. Zawiera wytyczne dotyczące wyboru i określenia środków bezpieczeństwa dla organizacji i systemów w celu spełnienia wymagań opisanych w publikacji NSC 200.

- NSC 800-53 A, *Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informacyjnych oraz organizacji*. Tworzenie skutecznych planów oceny, opracowany na podstawie NIST SP 800-53A – *Assessing Security and Privacy Controls in Systems and Organizations: Building Effective Assessment Plans*. Zawiera: (I) wytyczne dotyczące tworzenia skutecznych planów oceny bezpieczeństwa i planów oceny prywatności; oraz (II) kompleksowy zestaw procedur oceny skuteczności środków bezpieczeństwa informacji i zapewnienia prywatności stosowanych w systemach i organizacjach.
- NSC 800-60, *Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informacyjnego*, opracowany na podstawie NIST SP 800-60 – *Guide for Mapping Types of Information and Information Systems to Security Categories*. Zawiera informacje przydatne podczas spójnego odzwierciedlania poziomów wpływu na bezpieczeństwo następujących rodzajów danych: (I) informacje (np. prywatne, medyczne, zastrzeżone, finansowe, wrażliwe dla kontrahentów, tajemnice handlowe, dotyczące dochodzeń); oraz (II) systemy (np. krytyczne dla misji, wspierające misję, administracyjne).
- NIST SP 800-128 – *Guide for Security-Focused Configuration Management of Information Systems*, zawiera wytyczne dla organizacji odpowiedzialnych za zarządzanie i administrowanie bezpieczeństwem systemów i powiązanych środowisk operacyjnych.
- NIST SP 800-137 - *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, stanowi pomoc dla organizacji w zakresie opracowywania strategii ciągłego monitorowania bezpieczeństwa informacji (*ang. Information Security Continuous Monitoring – ISCM)* oraz wdrażania programu ISCM, który umożliwia zwiększenie świadomości zagrożeń i podatności na zagrożenia, widoczności zasobów organizacyjnych oraz skuteczności wdrożonych środków bezpieczeństwa.

2. ELEMENTY BEZPIECZEŃSTWA INFORMACJI

W niniejszej publikacji omówiono osiem głównych elementów dotyczących bezpieczeństwa informacji, aby pomóc czytelnikowi lepiej zrozumieć, jak wymagania i środki bezpieczeństwa omówione w rozdziale 10 całościowo wspomagają działalność organizacji. Te osiem koncepcji to:

1. Bezpieczeństwo informacji sprzyja realizacji misji organizacji.
2. Bezpieczeństwo informacji jest integralnym elementem prawidłowego zarządzania[8].
3. Środki bezpieczeństwa informacji są wdrażane tak, aby były współmierne do ryzyka.
4. Jasno określa się role i obowiązki w zakresie bezpieczeństwa informacji.
5. Zakres odpowiedzialności właścicieli systemów za bezpieczeństwo informacji wykracza poza ich własną organizację.
6. Bezpieczeństwo informacji wymaga kompleksowego i zintegrowanego podejścia.
7. Bezpieczeństwo informacji jest regularnie oceniane i monitorowane.
8. Bezpieczeństwo informacji zależy od czynników społecznych i kulturowych.

2.1 Bezpieczeństwo informacji sprzyja realizacji misji organizacji

W rozdziale 1 bezpieczeństwo informacji zostało zdefiniowane jako ochrona informacji i systemów przed nieuprawnionym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem działania, modyfikacją lub zniszczeniem w celu zapewnienia poufności, integralności i dostępności. Staranne wdrożenie środków bezpieczeństwa informacji jest kluczowe dla ochrony aktywów informacyjnych organizacji, jak również jej reputacji, pozycji prawnej, personelu oraz innych aktywów materialnych i niematerialnych.

[8] W kontekście niniejszej publikacji prawidłowe zarządzanie polega na należytej staranności w podejmowaniu wszelkich praktycznych działań mających na celu zapewnienie, że decyzje dotyczące zarządzania bezpieczeństwem informacji są podejmowane w taki sposób, aby nie tylko chronić informacje przechowywane, przetwarzane i przekazywane przez organizację, lecz także systemy znajdujące się pod kontrolą organizacji.

Niezdolność organizacji do wyboru i wdrożenia odpowiednich zasad i procedur bezpieczeństwa z dużym prawdopodobieństwem będzie miało negatywny wpływ na realizację misji organizacji. Dobrze dobrane zasady i procedury bezpieczeństwa, wprowadzone w celu ochrony ważnych aktywów, wspierają realizację ogólnej misji organizacji. W dobie złośliwych kodów, naruszeń systemów i zagrożeń wewnętrznych, ujawnione problemy wiązane z bezpieczeństwem mogą mieć tragiczne konsekwencje, zwłaszcza dla rentowności i reputacji organizacji. Wdrażając odpowiednie zabezpieczenia, organizacje sektora prywatnego i publicznego poprawiają zarówno efektywność, jak i jakość usług świadczonych klientom. Bezpieczeństwo informacji jest więc środkiem do celu, a nie celem samym w sobie.

Kluczowe jest zrozumienie misji organizacji i tego, w jaki sposób każdy system wspiera jej realizację. Po zdefiniowaniu roli systemu można również określić związane z nią wymagania bezpieczeństwa. Umożliwi to ujęcie bezpieczeństwa w ramy misji organizacji.

Role i funkcje systemu nie muszą być ograniczone do jednej organizacji. W systemie międzyorganizacyjnym każda organizacja odnosi korzyści z zabezpieczenia systemu. Na przykład, aby handel elektroniczny przebiegał pomyślnie, każdy z jego uczestników potrzebuje środków bezpieczeństwa, które chronią jego zasoby. Dobre zabezpieczenie systemu kupującego przynosi korzyści również sprzedającemu, ponieważ jest mniej prawdopodobne, że system kupującego zostanie wykorzystany do oszustwa, stanie się niedostępny lub w inny sposób negatywnie wpłynie na sprzedającego. Działa to również w drugą stronę.

2.2 Bezpieczeństwo informacji jest integralnym elementem prawidłowego zarządzania

Za określenie poziomu akceptowalnego ryzyka dla konkretnego systemu i organizacji, jako całości, ostatecznie odpowiedzialny jest personel zarządzający, biorąc przy tym pod uwagę koszty środków bezpieczeństwa. Ponieważ ryzyka związanego z bezpieczeństwem informacji nie da się całkowicie wyeliminować, celem jest znalezienie optymalnej równowagi pomiędzy ochroną informacji lub systemu, a wykorzystaniem dostępnych zasobów. Istotne jest, aby systemy i powiązane z nimi procesy miały wbudowaną zdolność do ochrony informacji, zasobów finansowych,

zasobów fizycznych i pracowników, zapewniając jednocześnie dostępność zasobów. Jeżeli informacje i systemy organizacji są powiązane z systemami zewnętrznymi, zakres odpowiedzialności kadry zarządzającej wykracza poza granice organizacji. Dlatego członkowie kadry zarządzającej powinni: (1) wiedzieć, jaki ogólny poziom lub rodzaj zabezpieczeń jest stosowany w systemie zewnętrznym i/lub (2) zadbać, aby system zewnętrzny zapewniał odpowiednie bezpieczeństwo informacji i systemu organizacji. Na przykład dostawca usług w chmurze (*Cloud Service Provider – CSP*) i uczestnicy łańcucha dostaw w chmurze mogą przejąć rolę zarządzania przechowywaniem, przetwarzaniem i przekazywaniem informacji organizacji. Nie zwalnia to jednak organizacji[9] z odpowiedzialności za bezpieczeństwo. To organizacja musi dbać, aby CSP i uczestnicy łańcucha dostaw w chmurze zapewnili odpowiedni poziom bezpieczeństwa dla przechowywanych, przetwarzanych i przesyłanych informacji.

2.3 Wdrażane środki bezpieczeństwa informacji powinny być współmierne do ryzyka

W systemie nigdy nie można całkowicie wyeliminować ryzyka. Dlatego tak ważne jest zarządzanie ryzykiem poprzez zachowanie równowagi pomiędzy funkcjonalnością, a wdrażaniem zabezpieczeń. Podstawowym celem zarządzania ryzykiem jest wdrożenie zabezpieczeń współmiernych do ryzyka. Stosowanie niepotrzebnych zabezpieczeń może spowodować marnowanie zasobów i utrudnienia w użytkowaniu i utrzymaniu systemów. Z drugiej strony, niestosowanie zabezpieczeń niezbędnych do ochrony systemu może sprawić, że system i dostępne w nim informacje będą narażone na naruszenia poufności, integralności i dostępności, co może utrudnić lub nawet zatrzymać realizację misji organizacji.

Organizacje powinny określać poziomy wpływu (wysoki, umiarkowany i niski) na atrybuty bezpieczeństwa systemu, aby określić i skategoryzować wpływ, jaki utrata poufności, integralności lub dostępności informacji i/lub systemu może mieć na działalność organizacji oraz aby dobrać odpowiednie zabezpieczenia. Dokładna

[9] Organizacja – wyspecjalizowana jednostka organizacyjna o dowolnej wielkości, złożoności lub pozycjonowaniu w ramach struktury organizacyjnej (np. przedsiębiorstwo, urząd, itp., lub w stosownych przypadkach, którykolwiek z elementów operacyjnych przedsiębiorstwa, urzędu, itp.).

kategoryzacja informacji i systemów jest niezbędna do określenia sposobu ochrony informacji współmiernego do ryzyka. Kategorie bezpieczeństwa odzwierciedlają wpływ, jaki utrata poufności, integralności lub dostępności może mieć na realizację misji organizacji. Aby określić poziom wpływu systemu, organizacje mogą skorzystać z wytycznych zawartych w publikacjach NSC 199, NSC 800-30 oraz NSC 800-60.

Dokładne określenie poziomu wpływu systemu dostarcza informacji potrzebnych do wyboru odpowiedniego zestawu środków bezpieczeństwa z publikacji NSC 800-53. Proces wyboru obejmuje ocenę kosztów wdrożenia i utrzymania środków bezpieczeństwa oraz oczekiwanych korzyści w zakresie bezpieczeństwa (tj. zmniejszenia ryzyka) wynikających z zastosowania tych środków.

Korzyści w zakresie bezpieczeństwa niosą ze sobą zarówno koszty bezpośrednie, jak i pośrednie. Koszty bezpośrednie obejmują zakup, instalację i administrowanie zabezpieczeniami (np. oprogramowaniem do kontroli dostępu lub systemami przeciwpożarowymi). Koszty pośrednie mogą być związane zarówno z wydajnością systemu, jak i biznesu, morale pracowników lub koniecznością ich przeszkolenia. W niektórych przypadkach koszty pośrednie mogą być wyższe od bezpośrednich kosztów danego środka. Kierownictwo organizacji jest odpowiedzialne za rozważenie kosztów w stosunku do korzyści wynikających z wdrożenia odpowiedniego zabezpieczenia i podjęcie decyzji w oparciu o ocenę ryzyka.

2.4 Jasne określenie ról i obowiązków w zakresie bezpieczeństwa informacji

Role i obowiązki właścicieli systemu, dostawców zabezpieczeń wspólnych, osób zatwierdzających, personel ds. bezpieczeństwa systemu, użytkowników i innych osób powinny być jasno określone i udokumentowane. Jeśli obowiązki nie zostaną jasno określone, w przyszłości kadra zarządzająca może mieć trudności z rozliczaniem personelu z wyników pracy.

Konieczność udokumentowania obowiązków z zakresu bezpieczeństwa informacji nie zależy od wielkości organizacji. Nawet w małych organizacjach można przygotować dokument określający politykę organizacyjną oraz identyfikujący role i obowiązki

w zakresie bezpieczeństwa informacji dotyczące systemu lub całej organizacji[10].

Role i obowiązki zostały krótko omówione w rozdziale 3 niniejszej publikacji. Bardziej szczegółowe informacje dotyczące kluczowych uczestników procesu bezpieczeństwa informacji znajdują się w załączniku D do publikacji NSC 800-37.

2.5 Zakres odpowiedzialności właścicieli systemów za bezpieczeństwo informacji wykracza poza ich własną organizację

Użytkownicy systemu nie zawsze znajdują się w obrębie systemu, z którego korzystają lub do którego mają dostęp. Na przykład, gdy istnieje połączenie między dwoma lub większą liczbą systemów, obowiązki związane z bezpieczeństwem informacji mogą być dzielone między uczestniczące organizacje. W takim przypadku właściciele systemu są odpowiedzialni za udostępnienie środków bezpieczeństwa stosowanych przez organizację, aby zapewnić użytkowników, że system jest odpowiednio zabezpieczony i spełnia wymagania bezpieczeństwa. Oprócz udostępniania informacji związanych z bezpieczeństwem, zespół reagowania na incydenty ma obowiązek odpowiednio szybko reagować na incydenty dotyczące bezpieczeństwa, aby zapobiec szkodom dla organizacji, personelu i innych organizacji.

2.6 Bezpieczeństwo informacji wymaga kompleksowego i zintegrowanego podejścia

Skuteczna ochrona informacji wymaga kompleksowego podejścia, które uwzględnia wiele aspektów zarówno z dziedziny bezpieczeństwa informacji, jak i spoza niej. Takie podejście należy stosować przez cały okres użytkowania systemu.

Na przykład „obrona w głąb" (*ang. defense-in-depth*) to strategia bezpieczeństwa stosowana w celu ochrony informacji i systemów organizacji przed zagrożeniami poprzez wdrożenie wielowarstwowych środków zapobiegawczych. Obrona w głąb wykorzystuje zabezpieczenia administracyjne (np. polityki, procedury) i technologie bezpieczeństwa (np. systemy wykrywania włamań, zapory sieciowe, ustawienia konfiguracyjne i oprogramowanie antywirusowe) w połączeniu z zabezpieczeniami fizycznymi (np.

[10] Są to funkcje wypełniane przez personel, a nie etaty, z tym zastrzeżeniem, że te same osoby nie mogą pełnić funkcji stwarzających konflikt interesów.

bramy, strażnicy), aby zminimalizować prawdopodobieństwo udanego ataku na system. Środki te nie tylko umożliwiają zmniejszenie prawdopodobieństwa, że naruszenie bezpieczeństwa zagrozi dostępowi do zasobów systemu lub będzie miało szkodliwy wpływ na poufność, integralność lub dostępność, ale także zapewniają organizacji powiadomienie w czasie zbliżonym do rzeczywistego po rozpoczęciu ataku.

2.6.1 Współzależności środków bezpieczeństwa

Rzadko kiedy środki bezpieczeństwa są wprowadzane jako autonomiczne rozwiązania problemu. Zazwyczaj są one skuteczniejsze, gdy są połączone z innym środkiem lub zestawem środków. Środki bezpieczeństwa, jeśli są odpowiednio dobrane, mogą mieć synergiczny wpływ na ogólne bezpieczeństwo systemu. Dla każdego środka bezpieczeństwa opisanego w publikacji NSC 800-53 wymieniono powiązane zabezpieczenia, które uzupełniają jego działanie. Jeśli użytkownicy nie zrozumieją tych współzależności, skutki mogą być szkodliwe dla systemu.

2.6.2 Inne współzależności

Współzależności w ramach i między środkami bezpieczeństwa nie są jedynym czynnikiem, który może wpływać na ich skuteczność. Zarządzanie systemem, ograniczenia prawne, zapewnienie jakości, kwestie dotyczące prywatności oraz środki wewnętrzne i zarządcze również mogą mieć wpływ na działanie wybranych środków bezpieczeństwa. Osoby zarządzające systemem muszą być w stanie określić, w jaki sposób bezpieczeństwo informacji wiąże się z innymi dziedzinami bezpieczeństwa, takimi jak bezpieczeństwo fizyczne i środowiskowe. Zrozumienie działania tych zależności może okazać się korzystne i umożliwić wdrożenie bardziej holistycznej strategii bezpieczeństwa. Publikacja NIST SP 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, zawiera dużo bardziej szczegółowe informacje na temat zasad projektowania systemów godnych zaufania.

Zrozumienie zależności między środkami bezpieczeństwa jest szczególnie ważne, gdy systemy są połączone z innymi systemami lub z ogólnoświatowym ekosystemem łańcucha dostaw. Łańcuchy dostaw składają się z podmiotów sektora publicznego i prywatnego i korzystają z geograficznie zróżnicowanych tras w celu dostarczenia

wysoce dopracowanych, opłacalnych i nadających się do ponownego wykorzystania rozwiązań w zakresie technologii informacyjnych i komunikacyjnych (*Information and Communications Technology – ICT*). Więcej informacji na temat zarządzania ryzykiem w łańcuchu dostaw można znaleźć w publikacji NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*.

2.7 Bezpieczeństwo informacji jest regularnie oceniane i monitorowane

Bezpieczeństwo informacji nie jest procesem statycznym i wymaga ciągłego monitorowania i zarządzania w celu ochrony poufności, integralności i dostępności informacji, jak również zapewnienia, że nowe podatności i zmieniające się zagrożenia będą szybko identyfikowane, a reakcja na nie będzie odpowiednia. W obliczu stale zmieniającej się kadry i środowiska technologicznego istotne jest, aby organizacje zapewniały dokładne informacje w odpowiednim czasie, działając przy tym na akceptowalnym poziomie ryzyka.

Strategia ciągłego monitorowania bezpieczeństwa informacji (*Information Security Continuous Monitoring – ISCM*) według definicji w publikacji NIST SP 800-137 polega na utrzymywaniu stałej świadomości w zakresie bezpieczeństwa informacji, podatności na zagrożenia i zagrożeń w celu ułatwienia podejmowania decyzji dotyczących zarządzania ryzykiem w organizacji. ISCM umożliwia dokładne określenie tolerancji na ryzyko organizacyjne, co pomaga w ustalaniu priorytetów i spójnym zarządzaniu ryzykiem w całej organizacji. ISCM zapewnia, że wybrane środki bezpieczeństwa pozostają skuteczne, oraz utrzymuje w organizacji świadomość w zakresie zagrożeń i podatności na zagrożenia.

Bardziej szczegółowe informacje na temat podstaw i procesu ciągłego monitorowania można znaleźć w publikacji NIST SP 800-137. Można również skorzystać z publikacji NSC 800-53A, aby zapoznać się z procedurami oceny.

2.8 Bezpieczeństwo informacji jest zależne od czynników społecznych i kulturowych

Czynniki społeczne wpływają na to, jak poszczególne osoby rozumieją i wykorzystują systemy, co w konsekwencji wpływa na bezpieczeństwo informacji w systemie i organizacji. Jednostki w różny sposób postrzegają, rozumieją i podejmują decyzje

oparte na ryzyku. Aby temu zaradzić, organizacje dbają o to, aby funkcje bezpieczeństwa informacji były przejrzyste, łatwe w użyciu i zrozumiałe. Dodatkowo, przeprowadzanie regularnie zaplanowanych szkoleń zwiększających świadomość z zakresu bezpieczeństwa niweluje skutki indywidualnych różnic w postrzeganiu ryzyka. Oprócz czynników społecznych na sposób prowadzenia działalności przez organizację wpływa również czynnik kulturowy, który warto wziąć pod uwagę w kontekście bezpieczeństwa informacji. Kultura organizacji może mieć wpływ na jej podejście do bezpieczeństwa informacji. Dokładne wyjaśnienie ryzyka związanego z praktykami biznesowymi może przyczynić się do zwiększenia przejrzystości i akceptacji zalecanych praktyk z zakresu bezpieczeństwa informacji.

Na organizacjach spoczywa obowiązek znalezienia równowagi między wymaganiami dotyczącymi bezpieczeństwa informacji, a funkcjonalnością. Organizacje mogą korzystać z różnych narzędzi, które spełniają wymagania bezpieczeństwa ich systemu (systemów) bez nadmiernego obciążania użytkownika. Przykładem może być system, który wymaga od użytkownika wielokrotnego wprowadzania nazwy użytkownika i hasła w celu uzyskania dostępu do różnych aplikacji podczas jednej sesji. W takim scenariuszu organizacje (w ich imieniu – SSO) mogą wybrać, które typy aplikacji, jeśli w ogóle, będą umożliwiać zapisywanie haseł i skrótów haseł, w oparciu o analizę ryzyka i użyteczności dla użytkowników.

Dawniej uważano, że prywatność nie jest związana z bezpieczeństwem informacji – obie funkcje były omawiane tak, jakby nie mogły współistnieć w systemie. Obecnie symbiotyczna relacja między prywatnością a bezpieczeństwem informacji jest uważana za niezbędną. Organizacje nie mogą chronić prywatności osób bez zapewnienia podstawowego bezpieczeństwa informacji. Prywatność to jednak coś więcej niż bezpieczeństwo, ponieważ odnosi się również do problemów, których mogą doświadczyć osoby fizyczne w wyniku uprawnionego przetwarzania ich informacji podczas całego cyklu życia danych. Ochrona prywatności osób fizycznych jest podstawowym obowiązkiem organizacji, które gromadzą, wykorzystują, przechowują, udostępniają i usuwają dane osobowe (*Personally Identifiable Information – PII*). Bardziej szczegółowe informacje na temat prywatności można znaleźć w publikacji NISTIR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* oraz

NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).*

Ogólnie rzecz biorąc, związek między bezpieczeństwem, a normami społecznymi nie musi być antagonistyczny. Mogą one mieć zarówno pozytywny, jak i negatywny wpływ na bezpieczeństwo informacji. Przykładowo, o negatywnym wpływie na bezpieczeństwo informacji można mówić, kiedy użytkownik zapisuje hasła i trzyma je w pobliżu swojego komputera. Pozytywny wpływ można uzyskać poprzez wdrożenie bardziej rozbudowanego uwierzytelniania wieloskładnikowego, w ramach którego, aby użytkownik mógł zresetować hasło, wymagana jest więcej niż jedna forma uwierzytelnienia (np. wiadomość tekstowa do użytkownika, fizyczny token). Bezpieczeństwo może poprawić dostęp do danych i przepływ informacji, umożliwiając zapewnienie dokładniejszych i bardziej wiarygodnych informacji, jak również większej dostępności systemów. Mechanizmy bezpieczeństwa mogą także poprawić poziom prywatności osób fizycznych (np. szyfrowanie). Niektóre mechanizmy bezpieczeństwa mogą powodować powstawanie nowych podatności na zagrożenia (np. pojedyncze logowanie). Dlatego ważne jest, aby zastanowić się, jak wdrażać rozwiązania w zakresie bezpieczeństwa w sposób optymalizujący realizację szerszych celów społecznych.

Normy społeczne zmieniają się, a wraz z nimi powinny zmieniać się zabezpieczenia informacji w systemach. Środki bezpieczeństwa, które są obecnie wystarczające, mogą nie nadążać za stale zmieniającym się środowiskiem informatycznym. Istotną rolę w postrzeganiu ryzyka przez pracowników odgrywa również kultura i środowisko bezpieczeństwa organizacji. Niewystarczające standardy bezpieczeństwa lub ich brak może prowadzić do pogorszenia poziomu bezpieczeństwa organizacji. Zapewnienie aktualnych i powtarzających się szkoleń na temat tego, co jest, a co nie jest dopuszczalnym wykorzystaniem systemów organizacji, pomaga w zapewnieniu ogólnego bezpieczeństwa systemu.

3. ROLE I OBOWIĄZKI

W kolejnym rozdziale opisano poszczególne role w ramach organizacji i ich zakresy odpowiedzialności. Jasno zdefiniowane role i obowiązki pomagają organizacji i jej pracownikom działać w sposób bardziej efektywny poprzez wyznaczenie osób odpowiedzialnych za wykonywanie określonych zadań. W dużej organizacji jest to pomocne, gdyż gwarantuje, że żadne zadanie nie zostanie pominięte. W małej, mniej ustrukturyzowanej organizacji obciążenie pracą może być bardziej równomierne, ponieważ od pracownika można wymagać podjęcia więcej niż jednego zadania.

Przedstawiona poniżej lista nie jest wyczerpującym wykazem wszystkich możliwych ról w organizacji i nie w takim celu została utworzona. Każda organizacja może określić swoje własne specyficzne role lub przyjąć inną konwencję nazewnictwa w oparciu o swoją misję lub strukturę organizacyjną. Podstawowe funkcje pozostają jednak takie same. Bardziej szczegółowy opis obowiązków przypisanych do każdej roli znajduje się w załączniku D do publikacji NSC 800-37.

3.1 Funkcja zarządzania ryzykiem (kadra zarządzająca wyższego szczebla)

Funkcję zarządzania ryzykiem (*ang. Risk Executive Function – RE*) może pełnić osoba lub grupa (np. członkowie zarządu, CEO, CIO)[11] odpowiedzialna w organizacji za zapewnienie, że: (I) kwestie związane z ryzykiem dla poszczególnych systemów są postrzegane w kontekście całej organizacji, z uwzględnieniem jej ogólnych celów strategicznych w zakresie realizacji podstawowych misji i funkcji biznesowych, oraz (II) zarządzanie ryzykiem związanym z bezpieczeństwem systemu jest spójne w całej organizacji, odzwierciedla tolerancję na ryzyko organizacyjne i jest rozpatrywane wraz z innymi rodzajami ryzyka w celu zapewnienia powodzenia realizacji misji/działalności.

Obowiązki RE obejmują między innymi:

- zdefiniowanie holistycznego podejścia do ryzyka dla całej organizacji;
- opracowanie strategii zarządzania ryzykiem organizacyjnym;

[11] Patrz: Załącznik C; NSC 800-37; NSC 7298.

- wspieranie wymiany informacji między osobami autoryzującymi[12] (*ang. authorizing officials – AO*) i innymi kierownikami wyższego szczebla w organizacji; oraz
- nadzorowanie działań związanych z zarządzaniem ryzykiem w całej organizacji.

3.2 Chief Executive Officer (CEO)

Osoba zarządzająca (*ang. Chief Executive Officer – CEO*) jest najwyższym rangą urzędnikiem lub dyrektorem wykonawczym w organizacji, który ponosi ogólną odpowiedzialność za zapewnienie ochrony informacji odpowiedniej do ryzyka i wielkości potencjalnych szkód (tj. wpływu) dla aktywów operacyjnych organizacji, osób fizycznych, innych organizacji i państwa, które mogą wynikać z nieuprawnionego dostępu, wykorzystania, ujawnienia, zakłócenia działania, modyfikacji lub zniszczenia: (I) informacji zebranych lub przechowywanych przez organizację lub w jej imieniu; oraz (II) systemów używanych lub obsługiwanych przez organizację, kontrahenta lub inny podmiot w imieniu organizacji.

Obowiązki CEO obejmują między innymi:

- integrację procesów zarządzania bezpieczeństwem informacji z procesami planowania strategicznego i operacyjnego;
- zapewnienie, że w przypadku informacji i systemów wykorzystywanych do wspierania działań organizacji stosowane są odpowiednie zabezpieczenia w zakresie bezpieczeństwa informacji; oraz
- sprawdzanie, czy przeszkolony personel przestrzega odpowiednich przepisów dotyczących bezpieczeństwa informacji, polityk, dyrektyw, instrukcji, standardów i wytycznych.

3.3 Chief Information Officer (CIO)

Kluczowa osoba w jednostce organizacyjnej (*ang. Chief Information Officer – CIO*) odpowiedzialna za: (I) wyznaczenie odpowiedniej osoby na stanowisko Senior Agency Information Security Officer (SAISO); (II) opracowanie i utrzymywanie polityki bezpieczeństwa, procedur i technik zabezpieczeń w celu spełnienia wszystkich

[12] Autoryzacja - przyznanie użytkownikowi, procesowi lub urządzeniu zezwolenia na wykonywanie określonych czynności.

obowiązujących wymagań; (III) nadzór nad personelem odpowiedzialnym za bezpieczeństwo informacji i zapewnienie, że personel ten jest odpowiednio przeszkolony; (IV) wspomaganie wyższy personel organizacji w zakresie wykonywania przez nich obowiązków związanych z bezpieczeństwem; oraz (V) we współpracy z innymi wyższym personelem, składanie corocznych sprawozdań na temat ogólnej skuteczności programu bezpieczeństwa informacji organizacji, w tym postępów w zakresie działań naprawczych.

Obowiązki CIO obejmują między innymi:

- przydzielanie zasobów służących do ochrony systemów wspierających realizację misji i funkcji biznesowych organizacji;
- zapewnienie, że systemy są chronione zgodnie z zatwierdzonymi planami bezpieczeństwa, których wdrożenie autoryzowano; oraz
- zapewnienie, że istnieje program bezpieczeństwa informacji dla całej organizacji, który jest skutecznie realizowany.

3.4 Właściciel informacji/władający informacją

Właściciel/władający informacją (*ang. Information Owner/Steward – IO/S*) jest osobą w organizacji posiadającą uprawnienia statutowe, zarządcze lub operacyjne w odniesieniu do określonych informacji. Jest odpowiedzialny za opracowanie polityk i procedur regulujących ich generowanie, gromadzenie, przetwarzanie, rozpowszechnianie i usuwanie.

Obowiązki IO/S obejmują między innymi:

- ustanowienie zasad dotyczących właściwego wykorzystania i ochrony określonych informacji; oraz
- dostarczanie właścicielom systemów danych na temat wymagań i środków bezpieczeństwa potrzebnych do zapewnienia właściwej ochrony tych informacji.

3.5 Senior Agency Information Security Officer (SAISO)

Senior Agency Information Security Officer (SAISO) jest osobą w organizacji odpowiedzialną za: (I) wykonywanie obowiązków z zakresu bezpieczeństwa ciążących na

CIO; oraz (II) pełnienie funkcji głównego łącznika pomiędzy CIO a osobami autoryzującymi (AO) organizacji, właścicielami systemów, dostawcami zabezpieczeń wspólnych oraz osobami odpowiedzialnymi za bezpieczeństwo systemu. W niektórych organizacjach rola ta może być również znana pod nazwą Chief Information Security Officer (CISO) lub Senior Information Security Officer (SISO) – w zależności od kultury organizacyjnej jednostki organizacyjnej.

Obowiązki SAISO obejmują między innymi:

- wdrażanie programu bezpieczeństwa informacji w całej organizacji i zarządzanie nim; oraz
- przyjmowanie w razie potrzeby roli pełnomocnika osoby autoryzującej lub osoby oceniającej środki bezpieczeństwa.

3.6 Osoba autoryzująca (AO)

Osoba autoryzująca (*ang. Authorizing Official – AO*) jest wyższego szczebla pracownikiem lub kierownikiem posiadającym uprawnienia do formalnego przyjęcia odpowiedzialności za eksploatację systemu przy akceptowalnym poziomie ryzyka dla operacji i aktywów organizacji, osób fizycznych i innych organizacji.

Obowiązki AO obejmują między innymi:

- zatwierdzanie planów bezpieczeństwa, protokołów uzgodnień lub porozumień, planów działania i kamieni milowych, jak również określanie, czy istotne zmiany w systemie lub środowiskach działania wymagają ponownego zatwierdzenia; oraz
- zapewnienie, że pełnomocnicy osoby autoryzującej wykonują wszystkie działania i funkcje związane z autoryzacją bezpieczeństwa.

3.7 Authorizing Official Designated Representative (AODR)

Pełnomocnik osoby autoryzującej (*ang. Authorizing Official Designated Representative - AODR*) to osoba w organizacji, która działa w imieniu osoby autoryzującej w zakresie koordynowania i prowadzenia niezbędnych codziennych działań związanych z procesem autoryzacji bezpieczeństwa. Pełnomocnik wykonuje funkcje AO, ale nie może akceptować ryzyka dla systemu.

Obowiązki AODR obejmują między innymi:

- wykonywanie obowiązków AO w ramach przydzielonych zadań;
- podejmowanie decyzji w odniesieniu do planowania i pozyskiwania zasobów dla procesu autoryzacji bezpieczeństwa, zatwierdzanie planu bezpieczeństwa, zatwierdzanie i monitorowanie wdrażania planów działania i kamieni milowych oraz ocena i/lub określenie ryzyka; oraz
- przygotowanie ostatecznego pakietu autoryzacyjnego, uzyskanie podpisu osoby autoryzującej na dokumencie decyzji autoryzacyjnej oraz przekazanie pakietu autoryzacyjnego do właściwych osób w organizacji.

3.8 Inspektor Ochrony Danych (SAOP)

Inspektor Ochrony Danych (*ang. Senior Agency Official for Privacy - SAOP*) jest wyższym pracownikiem organizacji, który ponosi ogólną odpowiedzialność za zapewnienie wdrożenia przez organizację zabezpieczeń prywatności informacji, w tym pełnej zgodności z przepisami ustawowymi i wykonawczymi oraz politykami dotyczącymi prywatności informacji, w oparciu o ustawę o ochronie danych osobowych.

Obowiązki SAOP obejmują między innymi:

- nadzorowanie, koordynowanie i ułatwianie działań organizacji w zakresie zgodności z przepisami o ochronie danych osobowych;
- przegląd procedur organizacji dotyczących ochrony prywatności informacji w celu zapewnienia, że są one kompleksowe i aktualne; oraz
- zapewnienie pracownikom i podwykonawcom organizacji odpowiedniego szkolenia i programów edukacyjnych w zakresie przepisów ustawowych, wykonawczych, polityk i procedur dotyczących przetwarzania informacji osobowych przez organizację.

3.9 Dostawca zabezpieczeń wspólnych

Dostawca zabezpieczeń wspólnych (*ang. Common Control Provider - CCP*) jest osobą, grupą lub organizacją odpowiedzialną za opracowanie, wdrażanie, ocenę

i monitorowanie zabezpieczeń wspólnych (tj. zabezpieczeń dziedziczonych przez systemy).

Obowiązki CCP obejmują między innymi:

- dokumentowanie w planie bezpieczeństwa (lub równoważnym dokumencie zalecanym przez organizację) zidentyfikowanych dla organizacji zabezpieczeń wspólnych; oraz
- zapewnienie, że wymagane oceny zabezpieczeń wspólnych są przeprowadzane przez wykwalifikowane osoby oceniające o odpowiednim poziomie niezależności określonym przez organizację.

3.10 Właściciel systemu

Właściciel systemu (*ang. System Owner - SO*) to osoba w organizacji odpowiedzialna za zakup, rozwój, integrację, modyfikację, eksploatację, utrzymanie i utylizację systemu.

Obowiązki SO obejmują między innymi:

- uwzględnienie interesów operacyjnych społeczności użytkowników (tj. użytkowników, którzy potrzebują dostępu do systemu, aby spełnić wymagania związane z misją, działalnością lub operacjami);
- zapewnienie zgodności z wymaganiami bezpieczeństwa informacji; oraz
- opracowanie i utrzymanie planu bezpieczeństwa systemu oraz zapewnienie, że system jest wdrażany i eksploatowany z zachowaniem uzgodnionych środków bezpieczeństwa.

3.11 System Security Officer (SSO)

*Syste*m Security Officer (SSO) jest osobą odpowiedzialną za zapewnienie utrzymania odpowiedniego stanu bezpieczeństwa operacyjnego systemu i ściśle współpracuje z właścicielem systemu.

Obowiązki SSO obejmują między innymi:

- nadzorowanie codziennych operacji związanych z bezpieczeństwem systemu; oraz

- współudział w opracowywaniu polityki i procedur bezpieczeństwa oraz zapewnienie zgodności z tą polityką i procedurami.

3.12 Architekt bezpieczeństwa informacji

Architekt bezpieczeństwa informacji (*ang. Information Security Architect - ISA*) to osoba, grupa lub organizacja odpowiedzialna za zapewnienie, że wymagania dotyczące bezpieczeństwa informacji, niezbędne do ochrony głównej misji i procesów biznesowych organizacji, są odpowiednio uwzględnione we wszystkich aspektach architektury organizacyjnej, w tym w modelach referencyjnych, modelach segmentów i rozwiązań oraz w powstałych systemach wspierających te misje i procesy biznesowe.

Obowiązki ISA obejmują między innymi:

- pełnienie funkcji łącznika pomiędzy architektem organizacji a inżynierem bezpieczeństwa systemu (SSE); oraz
- koordynacja z właścicielami systemu, dostawcami zabezpieczeń wspólnych i SSO w zakresie przydziału środków bezpieczeństwa jako środków specyficznych dla danego systemu, hybrydowych lub wspólnych.

3.13 Inżynier bezpieczeństwa systemu (SSE)

Inżynier bezpieczeństwa systemu (*ang. System Security Engineer – SSE)* to osoba, grupa lub organizacja odpowiedzialna za przeprowadzenie działań związanych z inżynierią bezpieczeństwa systemów.

Obowiązki SSE obejmują między innymi:

- projektowanie i rozwój systemów organizacji lub modernizacja istniejących systemów; oraz
- koordynowanie działań związanych z bezpieczeństwem z architektami bezpieczeństwa informacji (ISA), SAISO, właścicielami systemów (SO), dostawcami zabezpieczeń wspólnych (CCP) i SSO.

3.14 Podmiot oceniający zabezpieczenia

Podmiot oceniający środki bezpieczeństwa (*ang. Security Control Assessor - SCA*) to osoba, grupa lub organizacja odpowiedzialna za przeprowadzenie kompleksowej oceny kierowniczych, operacyjnych i technicznych środków bezpieczeństwa oraz zabezpieczeń rozszerzonych zastosowanych w systemie lub odziedziczonych przez system w celu określenia ogólnej skuteczności tych środków (tj. stopnia, w jakim środki bezpieczeństwa są prawidłowo wdrożone, działają zgodnie z przeznaczeniem i przynoszą pożądane rezultaty w zakresie spełniania wymagań bezpieczeństwa dla systemu).

Obowiązki SCA obejmują między innymi:

- dokonywanie oceny w celu zidentyfikowania słabości lub braków w systemie i środowisku jego działania;
- zalecanie działań zaradczych w celu wyeliminowania zidentyfikowanych podatności na zagrożenia oraz
- sporządzanie raportu z oceny bezpieczeństwa zawierającego wyniki i wnioski z oceny.

3.15 Administrator systemu

Administrator systemu (*ang. System Administrator - SA*) to osoba, grupa lub organizacja odpowiedzialna za konfigurację i utrzymanie systemu lub określonych komponentów systemu.

Obowiązki SA obejmują między innymi:

- instalowanie, konfigurowanie oraz aktualizowanie sprzętu i oprogramowania;
- zakładanie kont użytkowników i zarządzanie nimi;
- nadzorowanie zadań związanych z tworzeniem kopii zapasowych i odzyskiwaniem danych; oraz
- wdrażanie zabezpieczeń technicznych.

3.16 Użytkownik

Użytkownik (*ang. User*) to osoba, grupa lub organizacja, której przyznano dostęp do informacji organizacji w celu wykonania powierzonych obowiązków.

Obowiązki użytkownika obejmują między innymi:

- przestrzeganie zasad określających dopuszczalny sposób korzystania z systemów organizacji;
- wykorzystanie zasobów informatycznych dostarczonych przez organizację tylko do określonych celów; oraz
- zgłaszanie anomalii lub podejrzanego zachowania systemu.

3.17 Role pomocnicze

- *Audytor*. Audytorzy są odpowiedzialni za badanie systemów w celu określenia: (I) czy system spełnia określone wymagania bezpieczeństwa i polityki organizacji; oraz (II) czy środki bezpieczeństwa są odpowiednie. Audyty nieformalne mogą być przeprowadzane przez osoby obsługujące badany system lub przez bezstronnych audytorów zewnętrznych.
- *Personel odpowiedzialny za bezpieczeństwo fizyczne.* Jest odpowiedzialny za opracowanie i egzekwowanie odpowiednich fizycznych środków bezpieczeństwa, często w porozumieniu z kierownictwem ds. bezpieczeństwa informacji, kierownikami programów i funkcji oraz innymi osobami. Bezpieczeństwo fizyczne dotyczy instalacji systemów centralnych, rezerwowych i środowisk biurowych. Personel ten jest często odpowiedzialny za przeprowadzanie kontroli tożsamości personelu i poświadczeń bezpieczeństwa.
- *Personel ds. usuwania skutków katastrof/ds. planowania awaryjnego.* Niektóre organizacje posiadają osobny personel ds. usuwania skutków katastrof/ds. planowania awaryjnego. W takich przypadkach personel jest zazwyczaj odpowiedzialny za planowanie awaryjne dla całej organizacji i w zależności od potrzeb, współpracuje z kierownikami programów i kierownikami funkcjonalnymi/właścicielami aplikacji, personelem ds. bezpieczeństwa informacji

i innymi osobami w celu uzyskania dodatkowego wsparcia w zakresie planowania awaryjnego.

- *Personel* ds. *zapewnienia jakości.* Wiele organizacji wprowadza programy zapewnienia jakości w celu poprawy produktów i usług, które dostarczają swoim klientom. Personel odpowiedzialny za zapewnienie jakości powinien posiadać praktyczną wiedzę na temat bezpieczeństwa informacji oraz tego, w jaki sposób można je wykorzystać do podniesienia jakości programu (np. zapewnienia integralności informacji zapisanych w komputerach, dostępności usług oraz poufności informacji o klientach).
- *Pracownicy działu zamówień publicznych*. Dział zamówień publicznych jest odpowiedzialny za zapewnienie, że zamówienia organizacji zostały sprawdzone przez odpowiedni personel. Pracownikom działu zamówień publicznych zazwyczaj brakuje wiedzy technicznej, aby zagwarantować, że towary i usługi spełniają oczekiwania w zakresie bezpieczeństwa informacji, jednak powinni oni posiadać wiedzę na temat standardów bezpieczeństwa informacji i powinni zwracać uwagę osobom zamawiającym taką technologię na potencjalne kwestie związane z bezpieczeństwem informacji.
- *Pracownicy działu szkoleń*. Organizacja określa, czy główna odpowiedzialność za szkolenie użytkowników, operatorów i kierowników w zakresie bezpieczeństwa informacji spoczywa na dziale szkoleń czy na dziale programu bezpieczeństwa informacji. W obu przypadkach oba działy powinny współpracować w celu opracowania skutecznego programu szkoleniowego.
- *Dział kadr*. Dział kadr jest często pierwszym punktem kontaktowym dla kierowników, którzy potrzebują pomocy w ustaleniu, czy dla danego stanowiska konieczne jest przeprowadzenie badania przeszłości pod kątem bezpieczeństwa. Działy kadr i bezpieczeństwa na ogół ściśle współpracują w kwestiach związanych z badaniem przeszłości pracowników. Dział kadr może być również odpowiedzialny za procedury bezpieczeństwa osobowego podczas zwalniania pracownika z zajmowanego stanowiska.

- *Personel odpowiedzialny za zarządzanie ryzykiem/planowanie.* Niektóre organizacje zatrudniają na pełny etat personel zajmujący się analizą wszelkiego rodzaju zagrożeń dla organizacji. Taki dział zwykle koncentruje się na kwestiach związanych z ryzykiem organizacyjnym, jednak powinien również uwzględniać zagrożenia związane z bezpieczeństwem informacji. Dział ten nie przeprowadza zazwyczaj analiz ryzyka dla konkretnych systemów.
- *Personel odpowiedzialny za infrastrukturę.* Dział ten jest odpowiedzialny za zapewnienie świadczenia usług niezbędnych do bezpiecznego działania systemów organizacji (np. energii elektrycznej i kontroli środowiska). Dział ten jest często powiększony o oddzielny personel medyczny, pożarowy, odpowiedzialny za odpady niebezpieczne lub bezpieczeństwo pracowników.
- *Personel ds. ochrony prywatności.* Dział ten odpowiada za utrzymanie kompleksowego programu ochrony prywatności, który zapewnia zgodność z obowiązującymi wymogami w tym zakresie, opracowuje i ocenia politykę ochrony prywatności oraz zarządza związanym z nią ryzykiem. W tym dziale pracują osoby autoryzujące ds. prywatności, specjaliści ds. zgodności z przepisami dotyczącymi prywatności i oceny ryzyka, specjaliści prawni i inni specjaliści zajmujący się zarządzaniem ryzykiem związanym z prywatnością, a w szczególności, w kontekście niniejszej publikacji, ryzykiem, które może wynikać ze środków bezpieczeństwa informacji.

4. ZAGROŻENIA I PODATNOŚCI NA ZAGROŻENIA: KRÓTKI PRZEGLĄD

Podatność na zagrożenie to słaby punkt systemu, jego procedur bezpieczeństwa, wewnętrznych środków bezpieczeństwa lub ich wdrożenia, który może zostać wykorzystany przez źródło zagrożenia[13]. Podatności na zagrożenia powodują, że systemy są narażone na wiele działań, które mogą spowodować znaczne, i czasem nieodwracalne, straty dla osoby, grupy lub organizacji. Straty te mogą mieć różny zasięg – od pojedynczego uszkodzonego pliku na laptopie lub urządzeniu przenośnym, po narażenie całych baz danych w centrum operacyjnym. Wykorzystując odpowiednie narzędzia i wiedzę, napastnik może wykorzystać podatności systemów na zagrożenia i uzyskać dostęp do przechowywanych w nich informacji. Szkody wyrządzone w zaatakowanych systemach mogą być różne w zależności od źródła zagrożenia.

Źródło zagrożenia może mieć charakter agresywny lub przypadkowy. **Źródła zagrożeń agresywnych** to osoby, grupy, organizacje lub podmioty, które dążą do wykorzystania zależności organizacji od zasobów informatycznych. Zdarza się, że nawet pracownicy oraz uprawnieni i zaufani użytkownicy dopuszczają się nieuprawnionych manipulacji w systemach organizacji. **Źródła zagrożeń losowych** to klęski żywiołowe lub błędne działania podejmowane przez osoby fizyczne w trakcie wykonywania codziennych obowiązków, a także losowe awarie sprzętu lub oprogramowania, przez nikogo nie zawinione.

Jeśli system jest podatny, źródła zagrożeń mogą prowadzić do powstania niebezpiecznych zdarzeń. Zdarzenie powodujące zagrożenie to incydent lub sytuacja, która może potencjalnie wywołać niepożądane konsekwencje lub skutki. Przykładem źródła zagrożenia prowadzącego do zdarzenia powodującego zagrożenie jest hacker instalujący w systemie organizacji program do monitorowania klawiatury. Szkody, jakie mogą wyrządzić w systemach zdarzenia powodujące zagrożenie, są bardzo

[13] Źródło zagrożenia – intencja i metoda ukierunkowane na celowe wykorzystanie podatności w zabezpieczeniach lub sytuacja i metoda, która może przypadkowo wykorzystać podatność na zagrożenie.

zróżnicowane. Niektóre z nich wpływają na poufność i integralność informacji przechowywanych w systemie, inne zaś tylko na dostępność systemu. Więcej informacji na temat źródeł zagrożeń i zdarzeń powodujących zagrożenia można znaleźć w publikacji NSC 800-30.

W niniejszym rozdziale dokonano szerokiego przeglądu środowiska, w którym działają obecnie systemy. Może on stanowić cenne źródło informacji dla organizacji pragnących lepiej zrozumieć specyficzne środowisko zagrożeń. Przytoczona tu lista nie jest wyczerpująca. Zakres podanych tu informacji może być zbyt szeroki, a zagrożenia dla konkretnych systemów mogą być zupełnie inne niż omawiane w tym rozdziale.

Aby chronić system przed ryzykiem i wdrożyć optymalne środki bezpieczeństwa, właściciele, kierownicy i użytkownicy systemu muszą znać i rozumieć jego podatności, jak również źródła zagrożeń i zdarzenia, które mogą wykorzystać te podatności na zagrożenia. Przy określaniu odpowiedniej reakcji na odkrytą podatność na zagrożenie należy zadbać o zminimalizowanie wydatków na usuniecie podatności, z którymi wiąże się niewielkie ryzyko lub jego brak. Bardziej szczegółowe informacje na temat powiązań między zagrożeniami, podatnościami na zagrożenia, wyborem zabezpieczeń i reagowaniem na ryzyko znajdują się w rozdziale 6 „*Zarządzanie ryzykiem bezpieczeństwa informacji*”.

4.1 Przykłady źródeł agresywnych zagrożeń i powiązanych z nimi zdarzeń

W poprzednim podrozdziale zdefiniowano źródła zagrożeń i zdarzenia powodujące zagrożenia. W tym podrozdziale znajduje się kilka przykładów wraz z opisem.

4.1.1 Oszustwa i kradzieże

Systemy mogą być wykorzystywane do dokonywania oszustw i kradzieży poprzez „automatyzację” tradycyjnych metod oszustwa lub poprzez wykorzystanie nowych metod. Oszustwa i kradzieże przy użyciu systemu mogą być popełniane przez osoby z wewnątrz (tj. autoryzowanych użytkowników) i z zewnątrz. Za oszustwa często są odpowiedzialni autoryzowani administratorzy oraz użytkownicy mający dostęp do systemu i znający go (np. zasoby, które kontroluje, wady). Byli pracownicy organizacji również stanowią zagrożenie ze względu na swoją wiedzę na temat jej działalności, zwłaszcza jeśli dostęp nie zostanie im niezwłocznie odebrany.

Jednym z głównych motywów oszustw i kradzieży jest chęć uzyskania korzyści finansowych, ale nie tylko systemy finansowe są zagrożone.

Istnieje kilka technik, które napastnik może wykorzystać do zebrania informacji, do jakich w innym przypadku nie miałby dostępu. Poniżej przedstawiono kilka takich technik.

Media społecznościowe. Wszechobecność mediów społecznościowych (np. Facebook, Twitter, LinkedIn) umożliwia cyberprzestępcom wykorzystanie tych platform do przeprowadzania ukierunkowanych ataków. Wykorzystując łatwe do utworzenia, fałszywe i niezweryfikowane konta w mediach społecznościowych, cyberprzestępcy mogą podszywać się pod współpracowników, przedstawicieli obsługi klienta lub inne zaufane osoby w celu wysłania łączy do złośliwego kodu, który wykrada dane osobowe lub wrażliwe informacje organizacji. Media społecznościowe pogłębiają stały problem oszustw, a organizacje powinny traktować je jako poważne zagrożenie podczas wdrażania systemów. Konta w mediach społecznościowych umożliwiają gromadzenie informacji kontaktowych, danych o zainteresowaniach i powiązaniach osobistych wybranej osoby, które z kolei mogą być wykorzystane do przeprowadzenia ataku socjotechnicznego.

Inżynieria społeczna. Inżynieria społeczna, w kontekście bezpieczeństwa informacji, jest techniką, która w dużym stopniu opiera się na interakcjach międzyludzkich. Ma ona na celu wpłynięcie na daną osobę, aby naruszyła ona protokół bezpieczeństwa i nakłonienie jej do ujawnienia wrażliwych informacji. Tego typu ataki są najczęściej przeprowadzane przez telefon lub Internet. Ataki dokonywane przez telefon są najpowszechniejszą formą ataków socjotechnicznych. Na przykład, atakujący może wprowadzać pracowników firmy w błąd, aby uwierzyli, że jest istniejącym klientem, i skłonić ich do ujawnienia informacji o tym kliencie. W Internecie technika ta nazywana jest wyłudzaniem informacji (*ang. phishing*) – atakiem z wykorzystaniem wiadomości email, którego celem jest nakłonienie kogoś do wykonania czynności korzystnej dla atakującego (np. kliknięcia łącza lub ujawnienia danych osobowych). Ataki online z wykorzystaniem inżynierii społecznej mogą być również dokonywane przy użyciu załączników zawierających złośliwy kod, którego celem jest książka adresowa danej

osoby. Uzyskane informacje umożliwiają atakującemu wysłanie złośliwego kodu do wszystkich kontaktów w książce adresowej ofiary, propagując szkody wyrządzone przez pierwotny atak.

Ataki typu APT (ang. Advanced Persistent Threat – APT) To długotrwałe włamanie, którego celem jest uzyskanie dostępu do określonych danych i informacji. Ataki typu APT, mają na celu zbieranie informacji z sieci lub od celów.[14] Niektóre ataki APT mogą być tak skomplikowane, że uzyskują uprawnienia administratora umożliwiające całkowite przepisania kodu, aby pozostać niewykryte przez system wykrywania włamań (ang. *Intrusion Detection System – IDS*) w sieci. Po zebraniu wystarczającej ilości informacji o sieci atakujący może stworzyć „tylną furtkę" (*ang. backdoor*), czyli sposób na obejście mechanizmów bezpieczeństwa w systemach i uzyskać niekontrolowany dostęp do sieci. Następnie atakujący wykorzystuje zewnętrzny system poleceń i kontroli (*ang. command and control system – C2 system*) do ciągłego monitorowania systemu w celu wydobycia informacji.

4.1.2 Zagrożenie wewnętrzne

Pracownicy mogą stanowić wewnętrzne zagrożenie dla organizacji ze względu na ich znajomość systemów i aplikacji pracodawcy, a także świadomość, jakie działania mogą spowodować najwięcej szkód, zniszczeń lub zakłóceń. Sabotaż dokonywany przez pracownika, często inicjowany po uzyskaniu informacji o możliwym zwolnieniu lub groźbie rozwiązania umowy, jest krytycznym problemem dla organizacji i ich systemów. W celu ograniczenia potencjalnych szkód spowodowanych sabotażem popełnionym przez pracownika, zwalniana osoba powinna zostać natychmiast pozbawiona dostępu do infrastruktury informatycznej i wejścia na teren organizacji.

Przykłady sabotażu dokonywanego przez pracowników związanych z systemem to między innymi:

[14] Ataki APT na samym początku nie wyrządzają szkód, ale w rezultacie atakującemu chodzi o wyrządzenie szkody i to zwykle dużej. Ataki APT uznawane są za jedne z najniebezpieczniejszych zagrożeń dużych sieci IT. Jednorazowa kradzież może być dużo mniej szkodliwa niż ataki o długotrwałym charakterze.

- niszczenie sprzętu lub instalacji;
- zainstalowanie złośliwego kodu, który niszczy programy lub dane;
- wprowadzanie danych w sposób nieprawidłowy, przetrzymywanie danych lub usuwanie danych;
- powodowanie awarii systemów; oraz
- zmienianie haseł administracyjnych w celu uniemożliwienia dostępu do systemu.

4.1.3 Złośliwy hacker

Złośliwy hacker (*ang. malicious hacker*) to termin używany do opisania osoby lub grupy, która wykorzystuje znajomość systemów, sieci i programowania w celu uzyskania nielegalnego dostępu do systemów, spowodowania szkód lub kradzieży informacji. Zrozumienie motywacji, którymi kieruje się złośliwy hacker, może umożliwić organizacji wdrożenie odpowiednich środków bezpieczeństwa, aby zapobiec prawdopodobieństwu naruszenia systemu. Złośliwi hackerzy stanowią szeroką kategorię agresywnych zagrożeń, którą można podzielić na kilka kategorii – w zależności od podejmowanych przez nich działań lub ich zamiarów. Niektóre podkategorie zostały zaczerpnięte z publikacji NSC 800-82, *w* tym:

- *Haktywiści.*[15] Haktywiści włamują się do sieci, aby przeżyć emocje, podjąć wyzwanie lub móc się pochwalić w społeczności atakujących. Zdalne hakowanie wymagało kiedyś znacznych umiejętności lub wiedzy informatycznej, jednak obecnie atakujący mogą pobierać skrypty i protokoły ataku z Internetu i uruchamiać je przeciwko witrynom ofiar. Takie narzędzia ataku stały się zarówno bardziej wyrafinowane, jak i łatwiejsze w użyciu. W niektórych przypadkach atakujący nie mają wystarczającego doświadczenia, aby zagrozić trudnym celom, takim jak kluczowe sieci administracji państwowej. Niemniej jednak, ogólnoświatowa społeczność atakujących stwarza stosunkowo wysokie zagrożenie wystąpienia pojedynczych lub krótkotrwałych zakłóceń, które mogą spowodować poważne szkody dla biznesu lub infrastruktury.

[15] Potocznie: haker działający z pobudek społecznych, dla pożytku publicznego.

- *Operatorzy botnetu.* Operatorzy botnetu przejmują kontrolę nad wieloma systemami, aby koordynować ataki, wyłudzać informacje, rozpowszechniać spam i złośliwe kody. Usługi świadczone przy pomocy zainfekowanych systemów i sieci można nabyć na „czarnych" rynkach online – np. ataki typu odmowa świadczenia usługi (*ang. Denial of Service – DoS*), wykorzystanie serwerów do rozsyłania spamu lub wyłudzania informacji.
- *Grupy przestępcze.* Grupy przestępcze atakują systemy w celu uzyskania korzyści finansowych. W szczególności zorganizowane grupy przestępcze wykorzystują spam, wyłudzanie informacji oraz oprogramowanie szpiegujące / złośliwe kody do kradzieży tożsamości i oszustw internetowych. Międzynarodowi szpiedzy biznesowi i zorganizowane organizacje przestępcze stanowią również zagrożenie dla kraju ze względu na ich zdolność do prowadzenia szpiegostwa przemysłowego, kradzieży pieniędzy na dużą skalę oraz rekrutacji nowych atakujących. Niektóre grupy przestępcze mogą próbować wyłudzić pieniądze od organizacji, grożąc cyberatakiem lub szyfrując i zakłócając działanie jej systemów dla okupu. Ataki polegające na wyłudzaniu okupu zakłóciły funkcjonowanie wielu firm, a przeciwdziałanie im wymaga znacznych zasobów i planowania. Wiele firm, które nie miały skutecznych planów tworzenia kopii zapasowych i procedur przywracania danych, zostało zmuszonych do płacenia kosztownych okupów w celu przywrócenia zaszyfrowanych systemów.
- *Zagraniczne służby wywiadowcze.* Zagraniczne służby wywiadowcze wykorzystują narzędzia cyfrowe w ramach swoich działań związanych z gromadzeniem informacji i szpiegostwem. Ponadto kilka państw prowadzi intensywne prace nad rozwojem doktryn, programów i zdolności w zakresie wojny informacyjnej. Zdolności te umożliwiają pojedynczemu podmiotowi osiągnięcie znacznego i poważnego wpływu zakłócającego infrastrukturę zaopatrzeniową, komunikacyjną i gospodarczą, która wspiera potencjał militarny – wpływu, który może mieć wpływ na codzienne życie obywateli. W niektórych przypadkach może występować zagrożenie ze strony służb wywiadowczych obcych państw. Podczas misji wywiadowczych, oprócz ewentualnego szpiegostwa gospodarczego obce służby wywiadowcze mogą obrać za cel systemy nieobjęte klauzulą tajności.

Niektóre jawne informacje, które mogą być przedmiotem ich zainteresowania, to na przykład programy podróży wyższych urzędników, plany obrony cywilnej i reagowania w sytuacjach kryzysowych, technologie produkcyjne, dane satelitarne, dane dotyczące personelu i płac oraz akta dotyczące egzekwowania prawa, dochodzeń i bezpieczeństwa.

- *Osoby wyłudzające informacje (ang. Phishers).* Pojedyncze osoby lub niewielkie grupy wyłudzają informacje w celu kradzieży tożsamości lub danych i uzyskania w ten sposób korzyści finansowych. Osoby wyłudzające informacje mogą również wykorzystywać spam i oprogramowanie szpiegujące / złośliwe kody do realizacji swoich celów.
- *Spamerzy.* Spamerzy to osoby lub organizacje, które rozsyłają niechciane wiadomości e-mail zawierające ukryte lub fałszywe informacje w celu sprzedaży produktów, wyłudzania informacji, dystrybucji oprogramowania szpiegującego / złośliwych kodów lub atakowania organizacji (np. DoS).
- *Autorzy oprogramowania szpiegującego / złośliwych kodów (ang. Spyware/Malicious Code Authors).* Osoby lub organizacje, które przeprowadzają ataki na użytkowników poprzez tworzenie i rozpowszechnianie oprogramowania szpiegującego i złośliwych kodów. Do niszczycielskich wirusów komputerowych i robaków, które uszkadzają pliki i dyski twarde, należą między innymi Melissa Macro Virus, robak Explore.Zip, wirus CIH (Chernobyl), Nimda, Code Red, Slammer i Blaster.
- *Terroryści.* Terroryści dążą do zniszczenia, obezwładnienia lub wykorzystania infrastruktury krytycznej, aby zagrozić bezpieczeństwu państwa, spowodować masowe ofiary, osłabić gospodarkę oraz naruszyć morale i zaufanie społeczeństwa. Terroryści mogą wyłudzać informacje lub wykorzystywać oprogramowanie szpiegujące / złośliwe kody w celu pozyskania środków finansowych lub gromadzenia poufnych danych. Mogą również atakować jeden cel, aby odwrócić uwagę lub przekierować zasoby od innych celów.
- *Szpiedzy przemysłowi.* Szpiegostwo przemysłowe ma na celu zdobycie własności intelektualnej i specjalistycznej wiedzy przy użyciu nielegalnych metod.

4.1.4 Złośliwy kod

Do złośliwych kodów (*ang. malicious code*) zalicza się wirusy, konie trojańskie, robaki, bomby logiczne i wszelkie inne oprogramowanie stworzone w celu atakowania platform.

- *Wirus.* Segment kodu, który replikuje się poprzez dołączanie kopii siebie do istniejących plików wykonywalnych. Nowa kopia wirusa jest tworzona w momencie, gdy użytkownik uruchamia nowy program będący hostem. Wirus może zawierać dodatkowy „ładunek" (*ang. payload*), który uruchamia się po spełnieniu określonych warunków.
- *Koń trojański – trojan.* Program, który wykonuje pożądane zadanie, ale zawiera również nieoczekiwane i niepożądane funkcje. Za przykład może posłużyć program do edycji w systemie dla wielu użytkowników. Program ten można zmodyfikować tak, aby losowo i niespodziewanie usuwał pliki użytkownika za każdym razem, gdy realizuje on użyteczną funkcję (np. edycję).
- *Robak.* Samopowielający się program, który jest autonomiczny i nie wymaga programu będącego hostem ani interwencji użytkownika. Robaki powszechnie wykorzystują usługi sieciowe do przenoszenia się na inne hosty w sieci.
- *Bomba logiczna.* Ten rodzaj złośliwego kodu to zestaw instrukcji potajemnie i celowo wprowadzonych do programu lub systemu oprogramowania w celu realizacji złośliwej funkcji w z góry ustalonym czasie i terminie lub w momencie spełnienia określonego warunku.
- *Ransomware.* Rodzaj złośliwego kodu, który blokuje lub ogranicza dostęp do systemu poprzez zablokowanie całego ekranu lub blokadę albo zaszyfrowanie określonych plików do czasu zapłacenia okupu. Istnieją dwa różne rodzaje ataków za pomocą ransomware – szyfratory i blokery. Programy szyfrujące blokują (szyfrują) pliki systemowe i żądają zapłaty za odblokowanie (lub odszyfrowanie) tych plików. Programy szyfrujące, czyli crypto-ransomware, są najpowszechniejsze i najbardziej uciążliwe (np. WannaCry). Blokery są wykorzystywane do uniemożliwiania użytkownikom dostępu do systemów operacyjnych. Użytkownik nadal ma dostęp do urządzenia i innych plików, ale

w celu odblokowania zainfekowanego komputera musi zapłacić okup. Co gorsza, nawet jeśli użytkownik zapłaci okup, nie ma gwarancji, że atakujący rzeczywiście udostępni mu klucz deszyfrujący lub odblokuje zainfekowany system.

4.2 Przykłady źródeł losowych zagrożeń i powiązanych z nimi zdarzeń

4.2.1 Błędy i zaniedbania

Błędy i zaniedbania mogą być nieumyślnie popełniane przez operatorów systemów, którzy przetwarzają setki transakcji dziennie, lub przez użytkowników, którzy tworzą i edytują dane w systemach organizacji. Te błędy i zaniedbania mogą pogarszać integralność danych i systemu. Programy komputerowe, niezależnie od poziomu zaawansowania, nie są w stanie wykryć wszystkich rodzajów błędów i przeoczeń przy wprowadzaniu danych. Dlatego obowiązkiem organizacji jest stworzenie solidnego programu podnoszenia świadomości i szkoleń w celu zmniejszenia liczby i dotkliwości błędów i zaniedbań.

Błędy popełnione przez użytkowników, operatorów systemu lub programistów mogą występować w całym okresie eksploatacji systemu i bezpośrednio lub pośrednio przyczyniać się do powstawania problemów związanych z bezpieczeństwem.
W niektórych przypadkach ten błąd jest zagrożeniem, np. przy wprowadzaniu danych lub programowaniu, które powoduje awarię systemu. W innych przypadkach błędy powodują powstawanie podatności na zagrożenia. Błędy w programowaniu i rozwoju oprogramowania, często określane mianem „bugów", mogą mieć różne skutki – od łagodnych po katastrofalne.

4.2.2 Utrata wsparcia fizycznego i infrastrukturalnego

Utrata infrastruktury wspierającej to m.in. awarie zasilania (np. zaniki, skoki napięcia, przerwy w dostawie prądu), utrata łączności, przerwy w dostawie wody i wycieki, awarie kanalizacji, zakłócenia usług transportowych, pożary, powodzie, niepokoje społeczne i strajki. Jej niedostępność lub ograniczony dostęp do infrastruktury wspierającej często powoduje nieoczekiwane przestoje systemu. Na przykład pracownicy mogą nie być w stanie dotrzeć do miejsca pracy podczas zamieci śnieżnej, chociaż znajdujące się w nim systemy mogłyby normalnie działać. Dodatkowe informacje można znaleźć w podrozdziale 10.13, „*Ochrona fizyczna i środowiskowa*".

4.2.3 Wpływ udostępniania informacji na prywatność

Gromadzenie ogromnych ilości danych osobowych przez organizacje publiczne i prywatne stworzyło wiele okazji, aby osoby fizyczne doświadczyły problemów związanych z prywatnością jako produktu ubocznego tego zjawiska lub niezamierzonej konsekwencji naruszenia bezpieczeństwa. Przykładowo, migracja informacji do dostawcy usług w chmurze stała się realną opcją, z której korzysta wiele osób fizycznych i organizacji. Łatwość dostępu do danych w chmurze sprawiła, że stała się ona bardziej atrakcyjnym rozwiązaniem do długoterminowego przechowywania danych. Wszystko, co zostało napisane, przesłane lub opublikowane, jest przechowywane w systemie chmury, nad którym użytkownicy indywidualni nie mają kontroli. Użytkownik usługi w chmurze nie wie, że do jego danych osobowych może uzyskać dostęp obca osoba posiadająca odpowiednie narzędzia i umiejętności techniczne.

Dobrowolne udostępnianie osobistych informacji za pośrednictwem mediów społecznościowych przyczyniło się również do powstania nowych zagrożeń. Złośliwi hackerzy wykorzystują te informacje do ataków socjotechnicznych lub do ominięcia powszechnie stosowanych środków uwierzytelniania. Łącząc wszystkie te informacje i technologie, złośliwi hackerzy mają możliwość tworzenia kont z wykorzystaniem cudzych danych lub uzyskiwania dostępu do sieci.

Organizacje mogą udostępniać informacje o cyberzagrożeniach, które dotyczą danych osobowych. Ujawnienie tych informacji może prowadzić do ich niepożądanego wykorzystania, w tym do prowadzenia inwigilacji lub innych działań organów ścigania.

5. POLITYKA BEZPIECZEŃSTWA INFORMACJI

W kontekście bezpieczeństwa informacji pojęcie „polityka ma więcej niż jedną definicję. W publikacji NIST SP 800-95, *Guide to Secure Web Services*, zdefiniowano politykę jako „stwierdzenia, reguły lub założenia, które określają prawidłowe lub oczekiwane zachowanie podmiotu". Na przykład, polityki autoryzacji mogą określać właściwe reguły kontroli dostępu do komponentu oprogramowania. Termin polityka (zasady) może również odnosić się do konkretnych reguł bezpieczeństw systemu, a nawet konkretnych decyzji kierowniczych, które narzucają organizacji politykę prywatności dla poczty elektronicznej lub politykę bezpieczeństwa dla zdalnego dostępu.

Polityka bezpieczeństwa informacji jest definiowana jako zbiór dyrektyw, przepisów, reguł i praktyk, które określają, w jaki sposób organizacja zarządza informacjami oraz chroni je i rozpowszechnia. Podejmując dotyczące ich decyzje, menadżerowie stają przed trudnymi wyborami dotyczącymi alokacji zasobów, konkurencyjnych celów i strategii organizacji, a wszystko to związane jest z ochroną zasobów technicznych i informacyjnych oraz kierowaniem zachowaniem pracowników. Menadżerowie wszystkich szczebli dokonują wyborów, które mogą wpływać na politykę, przy czym zakres zastosowania polityki jest różny w zależności od uprawnień kierownika.

Decyzje menadżerskie dotyczące kwestii bezpieczeństwa informacji są bardzo zróżnicowane. W celu rozróżnienia poszczególnych rodzajów polityk, w niniejszym rozdziale dokonano ich klasyfikacji na trzy podstawowe typy: politykę programową, politykę dotyczącą konkretnych zagadnień i politykę dotyczącą konkretnych systemów.

Polityki zabezpieczeń są adresowane w punktach „1" („Polityka i procedury) dla każdej kategorii środków bezpieczeństwa, które można znaleźć w publikacji NSC 800-53. Zabezpieczenia „1" ustanawiają politykę i procedury w celu skutecznego wdrożenia wybranego środka bezpieczeństwa i zabezpieczenia rozszerzonego.

5.1 Standardy, wytyczne i procedury

Ponieważ polityka ma szeroki zakres, organizacje opracowują również standardy, wytyczne i procedury, które zapewniają użytkownikom, menadżerom, administratorom systemów i innym osobom jasne metody wdrażania polityki i realizacji celów organizacji. Standardy i wytyczne określają technologie i metodologie, które należy stosować w celu zabezpieczenia systemów. Procedury to szczegółowo opisane kroki, które należy wykonać, aby zrealizować zadania związane z bezpieczeństwem. Standardy, wytyczne i procedury mogą być rozpowszechniane w całej organizacji w formie podręczników, regulaminów lub instrukcji.

- *Standardy organizacyjne* (nie należy ich mylić ze standardami branżowymi, ani innymi standardami krajowymi lub międzynarodowymi) określają jednolite zastosowanie określonych technologii, parametrów lub procedur, jeżeli takie jednolite zastosowanie będzie korzystne dla organizacji. Typowym przykładem jest standaryzacja identyfikatorów w całej organizacji, ułatwiająca mobilność pracowników i automatyzację systemów wejścia/wyjścia. Stosowanie się do standardów jest zazwyczaj obowiązkowe w całej organizacji.
- *Wytyczne* pomagają użytkownikom, personelowi odpowiedzialnemu za systemy i innym osobom w skutecznym zabezpieczaniu systemów. W wytycznych zazwyczaj zakłada się, że systemy są bardzo zróżnicowane, a wprowadzenie standardów nie zawsze jest osiągalne, właściwe i opłacalne. Na przykład wytyczne organizacyjne mogą być wykorzystane jako pomoc w opracowaniu specyficznych dla danego systemu standardowych procedur. Wytyczne są często stosowane, aby zapewnić, że konkretne środki bezpieczeństwa nie zostaną pominięte, mimo że mogą być wdrażane, i to poprawnie, na wiele sposobów.
- *Procedury* opisują sposób wdrażania obowiązujących polityk bezpieczeństwa, standardów i wytycznych. Jest to szczegółowy opis kroków, jakie muszą wykonać użytkownicy, personel operacyjny systemu lub inne osoby, aby zrealizować określone zadanie (np. przygotowanie nowych kont użytkowników i nadanie im odpowiednich uprawnień).

Niektóre organizacje wydają ogólne instrukcje dotyczące bezpieczeństwa informacji, regulaminy, podręczniki lub podobne dokumenty. Mogą one łączyć w sobie politykę, wytyczne, standardy i procedury, ponieważ są ze sobą ściśle powiązane. Podręczniki i regulaminy mogą stanowić ważne narzędzia, jednak często przydatne jest wyraźne rozróżnienie między polityką a jej realizacją. Może to pomóc w zwiększeniu elastyczności i opłacalności poprzez zapewnienie alternatywnych sposobów wdrażania w celu osiągnięcia celów polityki.

5.2 Polityka programowa

Polityka programowa służy do tworzenia programu bezpieczeństwa informacji w organizacji. Polityki programowe wyznaczają strategiczny kierunek dla zabezpieczeń i przydzielają zasoby do ich wdrożenia w organizacji. Personel wyższego szczebla, zazwyczaj SISO, opracowuje politykę programową w celu utworzenia lub restrukturyzacji programu bezpieczeństwa informacji w danej organizacji. Taka ogólna polityka określa cel programu i jego zakres w organizacji, odnosi się do kwestii zgodności i nakłada na organizację odpowiedzialność za bezpośrednie wdrożenie programu bezpieczeństwa informacji, jak również inne powiązane obowiązki.

5.2.1 Podstawowe elementy polityki programowej

Polityka programowa zawiera elementy opisane poniżej.

- *Cel.* Polityka programowa zawiera często oświadczenie opisujące cel i założenia programu. Potrzeby związane z bezpieczeństwem, takie jak: integralność, dostępność i poufność, mogą stanowić podstawę celów organizacji określonych w polityce. Na przykład w organizacji odpowiedzialnej za utrzymanie dużych baz danych o znaczeniu krytycznym, należy położyć szczególny nacisk na ograniczenie liczby błędów, utraty danych, uszkodzeń danych i na ich odzyskiwanie. W organizacji odpowiedzialnej za utrzymanie wrażliwych danych osobowych cele mogą natomiast koncentrować się na silniejszej ochronie przed nieuprawnionym ujawnieniem.
- *Zakres.* W polityce programowej jasno określa się, jakie zasoby (np. obiekty, sprzęt i oprogramowanie, informacje i personel) chroni program bezpieczeństwa informacji. W wielu przypadkach program będzie obejmował wszystkie systemy

i cały personel organizacji, natomiast w innych wskazane może być, aby program bezpieczeństwa informacji miał bardziej ograniczony zakres. Na przykład polityka mająca na celu ochronę informacji przechowywanych w systemie niejawnym lub o wysokim wpływie na atrybuty bezpieczeństwa systemu będzie znacznie bardziej rygorystyczna niż polityka przeznaczona do zabezpieczenia systemu o niskim poziomie wpływu.

- *Obowiązki.* Po ustanowieniu programu bezpieczeństwa informacji zarządzanie nim jest zazwyczaj powierzane nowo utworzonej lub istniejącej komórce organizacyjnej. Należy również ustalić zakres odpowiedzialności personelu i działów w całej organizacji. W tej części oświadczenia polityki rozróżnia się na przykład obowiązki dostawców usług informatycznych i zarządzających aplikacjami wykorzystującymi świadczone usługi. W polityce ustanawia się również operacyjne jednostki bezpieczeństwa dla głównych systemów, szczególnie tych, z którymi jest związane wysokie ryzyko lub które są najważniejsze dla działalności organizacji. Może ona również służyć jako podstawa do ustalenia zakresu odpowiedzialności pracowników. Role i obowiązki zostały omówione w rozdziale 3 niniejszej publikacji.
- *Zgodność (ang. Compliance)* . W polityce programowej zazwyczaj porusza się dwie kwestie dotyczące zgodności.

1. Ogólna zgodność zapewniająca spełnienie wymagań niezbędnych do opracowania programu i przypisanych w nim obowiązków dla różnych komórek organizacyjnych. Często odpowiedzialność za monitorowanie zgodności, w tym za to, jak organizacja wdraża priorytety kierownictwa ujęte w programie, powierza się jednostce nadzorującej.
2. Stosowanie określonych kar i działań dyscyplinarnych. Ponieważ polityka bezpieczeństwa jest dokumentem ogólnym, zwykle nie opisuje się w niej konkretnych kar za różne uchybienia. Zamiast tego, w polityce można autoryzować utworzenie struktur zgodności, które będą obejmować naruszenia i konkretne działania dyscyplinarne.

Ważnym aspektem tworzenia polityki zgodności jest pamiętanie, że jej naruszenie przez pracownika może być nieumyślne. Na przykład, niestosowanie się do niej może być często wynikiem braku wiedzy lub szkolenia. W przypadku kwestii związanych z karami i działaniami dyscyplinarnymi w stosunku do osób fizycznych, niezwykle ważne jest uzyskanie pomocy ze strony odpowiedniego doradcy prawnego. W polityce nie trzeba opisywać kar, które zostały już przewidziane przez prawo, chociaż można je wymienić, jeśli będzie ona również wykorzystywana jako dokument informacyjny lub szkoleniowy.

5.3 Polityka dotycząca konkretnego zagadnienia

W oparciu o wytyczne zawarte w polityce bezpieczeństwa informacji, tworzone są polityki dotyczące konkretnych zagadnień zajmujące się obszarami, które są aktualnie istotne i stanowią problem dla organizacji. Ich celem jest zapewnienie pracownikom w organizacji konkretnych wskazówek i instrukcji dotyczących właściwego użytkowania systemów. Polityka dotycząca konkretnego zagadnienia jest przeznaczona dla każdej technologii, z której korzysta organizacja, i należy ją napisać w taki sposób, aby była zrozumiała dla użytkowników. W przeciwieństwie do polityk programowych, polityki dotyczące konkretnych zagadnień należy regularnie weryfikować ze względu na częste technologiczne zmiany w organizacji.

5.3.1 Przykładowe tematy polityk dotyczących konkretnych zagadnień

Istnieje wiele obszarów, w przypadku których odpowiednie może być opracowanie polityki dotyczącej konkretnego zagadnienia. Wprowadzenie nowych technologii i odkrycie nowych zagrożeń często pociągają za sobą konieczność stworzenia polityki dotyczącej konkretnego zagadnienia. Poniżej opisano przykłady polityk dotyczących konkretnych zagadnień.

- *Dostęp do Internetu.* Połączenie z Internetem niesie ze sobą wiele korzyści, ale również wiele problemów. Przykładowe zagadnienia, jakie można ująć w polityce dostępu do Internetu, to określenie: kto będzie miał ten dostęp, jakie rodzaje systemów mogą być podłączone do sieci, jakie rodzaje informacji mogą być przez nią przesyłane, wymagania dotyczące uwierzytelniania użytkowników systemów podłączonych do Internetu oraz stosowanie zapór sieciowych.

- *Prywatność poczty elektronicznej.* Polityka ta wyjaśnia, jakie informacje są gromadzone i przechowywane oraz w jaki sposób są one wykorzystywane. Kierownictwo może chcieć monitorować pracownika, aby upewnić się, że korzysta on z systemów organizacji wyłącznie w celach służbowych, lub ustalić, czy nie rozpowszechnia wirusów, nie wysyła obraźliwych treści lub nie ujawnia prywatnych informacji biznesowych. Użytkownikom należy zapewnić pewien poziom prywatności dotyczącej poczty elektronicznej. Polityka ta określa, jaki to będzie poziom oraz okoliczności, w jakich poczta elektroniczna może zostać odczytana.
- *Przynieś własne urządzenie (ang. Bring Your Own Device – BYOD).* Umożliwia osobom fizycznym korzystanie z urządzeń osobistych w miejscu pracy. Zezwolenie na BYOD może zwiększyć produktywność i zmniejszyć koszty dla organizacji. Jednak wprowadzenie do sieci organizacji różnych systemów operacyjnych i konfiguracji użytkowników może stwarzać problemy nie tylko dla bezpieczeństwa informacji organizacji, ale także dla prywatności pracowników. Kompleksowa polityka BYOD zawiera konkretne uwarunkowania dotyczące urządzenia i użytkownika, a także zasady zachowania, których należy przestrzegać, aby móc uzyskać dostęp do zasobów organizacji za pośrednictwem urządzeń osobistych.
- *Media społecznościowe.* Nawet jeśli organizacja nie jest obecna w mediach społecznościowych, jest duże prawdopodobieństwo, że należący do niej użytkownicy mają tam swoje konta. Posiadanie polityki dotyczącej mediów społecznościowych jest kluczowe z punktu widzenia ochrony organizacji i jej pracowników. Polityka dotycząca mediów społecznościowych zawiera wytyczne dla użytkowników, które określają oczekiwane zachowanie podczas korzystania z różnych platform mediów społecznościowych. W zależności od organizacji, polityka może być rygorystyczna, uniemożliwiająca korzystanie z mediów społecznościowych przy użyciu zasobów dostarczonych przez organizację lub łagodna, która pozwala na dostęp do mediów społecznościowych w ramach ograniczeń określonych przez organizację.

Inne tematy, które mogą być przedmiotem polityki dotyczącej konkretnego zagadnienia, obejmują między innymi: podejście do zarządzania ryzykiem i planowanie awaryjne, ochronę informacji poufnych/wrażliwych, nieautoryzowane oprogramowanie, nieautoryzowane wykorzystanie sprzętu, naruszenia polityki, wykorzystanie zewnętrznych nośników danych, prawo do prywatności i fizyczne sytuacje kryzysowe.

5.3.2 Podstawowe elementy polityki dotyczącej konkretnego zagadnienia

Politykę dotyczącą konkretnego zagadnienia można podzielić na elementy opisane poniżej.

- *Określenie zagadnienia.* Aby sformułować politykę dotyczącą danej kwestii, właściciel/władający informacją musi najpierw tę kwestię zdefiniować z uwzględnieniem wszelkich istotnych terminów, wyjątków i warunków. Często warto określić cel lub uzasadnienie polityki, aby ułatwić jej przestrzeganie. Na przykład, organizacja może zechcieć opracować specyficzną politykę dotyczącą używania „nieoficjalnego oprogramowania", czyli takiego, które nie zostało zatwierdzone, zakupione, sprawdzone, nie jest zarządzane ani nie jest własnością organizacji. Dodatkowo, w przypadku niektórych rodzajów oprogramowania, np. będącego prywatną własnością pracowników, ale zatwierdzonego do użytku w pracy lub będącego własnością i używanego przez inne firmy na podstawie umowy z organizacją, może zaistnieć potrzeba uwzględnienia odpowiednich rozgraniczeń i warunków.
- *Określenie stanowiska organizacji.* Po określeniu zagadnienia i wyszczególnieniu związanych z nim warunków, w tej części należy jasno przedstawić stanowisko organizacji (tj. decyzję kierownictwa) w danej sprawie. W powyższym przykładzie oznaczałoby to określenie, czy używanie nieoficjalnego oprogramowania zgodnie z definicją jest zabronione we wszystkich lub w niektórych przypadkach, czy istnieją dalsze wytyczne dotyczące jego zatwierdzania i używania, czy w poszczególnych przypadkach mogą być przyznawane wyjątki, przez kogo i na jakiej podstawie.

- *Stosowanie.* Polityka dotycząca konkretnego zagadnienia musi również zawierać informacje o jej stosowaniu. Oznacza to określenie: gdzie, jak, kiedy, do kogo i do czego ma zastosowanie dana polityka. Na przykład hipotetyczna polityka dotycząca nieoficjalnego oprogramowania może dotyczyć tylko własnych zasobów i pracowników organizacji w siedzibie organizacji, a nie kontrahentów wykonujących zadania w innych lokalizacjach. Dodatkowo, może zaistnieć potrzeba wyjaśnienia zakresu stosowania polityki w odniesieniu do pracowników podróżujących pomiędzy różnymi lokalizacjami, pracujących z domu lub tych, którzy wożą dyski ze sobą i używają ich w wielu lokalizacjach.
- *Role i obowiązki.* Polityka dotycząca konkretnego zagadnienia zawiera także zazwyczaj przydział ról i obowiązków. Na przykład, jeśli polityka zezwala pracownikom na używanie w pracy prywatnego, nieoficjalnego oprogramowania po uzyskaniu odpowiednich zezwoleń, to należy określić organ udzielający takiego zezwolenia. Polityka powinna określać, kto, z racji pełnionego stanowiska, ma takie uprawnienia. Należy również wyjaśnić, kto jest odpowiedzialny za zapewnienie, że tylko zatwierdzone oprogramowanie będzie używane w zasobach systemu organizacji i ewentualnie za kontrolowanie użytkowników pod kątem nieoficjalnego oprogramowania.
- *Zgodność.* W przypadku niektórych rodzajów polityki właściwe może być bardziej szczegółowe opisanie niedopuszczalnych uchybień i ich konsekwencji. Kary mogą być wyraźnie określone i zgodne z polityką i praktyką kadrową organizacji. W przypadku ich stosowania można koordynować działania z odpowiednimi osobami, urzędami, a nawet przedstawicielami związków zawodowych. Wskazane może być również powierzenie monitorowania zgodności konkretnej jednostce w organizacji.
- *Punkty kontaktowe i dodatkowe informacje.* W przypadku każdej polityki dotyczącej konkretnego zagadnienia należy wskazać odpowiednie osoby w organizacji, z którymi należy się skontaktować w celu uzyskania dalszych informacji, wskazówek i zapewnienia zgodności. Czasem jako punkty kontaktowe lepiej wskazać nie osoby a stanowiska, ponieważ zmieniają się one rzadziej niż osoby je

zajmujące. Przykładowo, w niektórych kwestiach punktem kontaktowym może być kierownik liniowy, w innych zaś kierownik obiektu, osoba odpowiedzialna za wsparcie techniczne, administrator systemu lub przedstawiciel programu bezpieczeństwa. Posługując się ponownie powyższym przykładem, pracownicy musieliby wiedzieć, czy punktem kontaktowym w przypadku pytań i konieczności uzyskania informacji proceduralnych będzie ich bezpośredni przełożony, administrator systemu, czy też osoba zajmująca się bezpieczeństwem informacji.

5.4 Polityka dotycząca konkretnego systemu

Polityki dotyczące programów i zagadnień są ogólnymi dokumentami obejmującymi swoim zakresem całą organizację, natomiast polityki dotyczące systemów zawierają informacje i wskazówki, jakie działania są dozwolone w danym systemie. Polityki te są podobne do polityk dotyczących konkretnych zagadnień, ponieważ odnoszą się do określonych technologii w całej organizacji. Polityki dotyczące konkretnych systemów narzucają jednak odpowiednie konfiguracje zabezpieczeń personelowi odpowiedzialnemu za wdrożenie wymaganych środków bezpieczeństwa w celu spełnienia potrzeb organizacji w zakresie bezpieczeństwa informacji.

Aby opracować spójny i kompleksowy zestaw polityk bezpieczeństwa, personel może wykorzystać proces zarządzania, w ramach którego zasady bezpieczeństwa wynikają z poszczególnych celów. Pomocne może być rozważenie dwupoziomowego modelu polityki bezpieczeństwa systemu składającego się z warstwy celów bezpieczeństwa i warstwy operacyjnych zasad bezpieczeństwa. Są one ściśle powiązane i często trudne do rozróżnienia – to implementacja polityki w technologii. Podobnie jak w przypadku polityk dotyczących konkretnych zagadnień, zaleca się, aby polityki dotyczące konkretnych systemów były poddawane przeglądowi w konkretnym czasie, zgodnie z wymogami organizacji, w celu zapewnienia zgodności z aktualnymi procedurami bezpieczeństwa.

5.4.1 Cele bezpieczeństwa

Pierwszym krokiem w procesie zarządzania jest określenie celów bezpieczeństwa współmiernych do ryzyka dla konkretnego systemu. Proces ten może rozpocząć się od analizy potrzeby integralności, poufności i dostępności, ale nie można na tym

poprzestać. Cel w zakresie bezpieczeństwa musi być szczegółowy, konkretny, dobrze zdefiniowany i sformułowany w taki sposób, aby był jednoznacznie osiągalny. Wszystkie zainteresowane strony odgrywają ważną rolę w tworzeniu kompleksowej, a zarazem praktycznej polityki. Dlatego należy pamiętać, że polityka nie jest tworzona wyłącznie przez kadrę zarządzającą.

5.4.2 Zasady bezpieczeństwa operacyjnego

Po określeniu przez kadrę zarządzającą celów bezpieczeństwa można ustalić i udokumentować zasady zarządzania systemem i jego eksploatacji. Zasady mogą na przykład definiować uprawnione modyfikacje – określając osoby uprawnione do podejmowania określonych działań w szczególnych warunkach w odniesieniu do określonych klas i rekordów informacji. Stopień szczegółowości konieczny do zapewnienia bezpieczeństwa operacyjnego różni się w zależności od systemu. Im bardziej szczegółowe są zasady, tym łatwiej jest administratorom określić, kiedy nastąpiło ich naruszenie. Szczegółowy opis może również ułatwić automatyzację egzekwowania polityki.

Oprócz decyzji o poziomie szczegółowości, kadra zarządzająca określa stopień formalności w dokumentowaniu polityki dotyczącej konkretnego systemu. Znowu, im bardziej sformalizowana dokumentacja, tym łatwiej jest egzekwować politykę i postępować zgodnie z nią. Na przykład, pomocne może być przygotowanie dokumentu określającego uprawnienia dostępu do systemu oraz przypisującego obowiązki w zakresie bezpieczeństwa. Należy również uwzględnić zasady korzystania z systemu oraz konsekwencje ich nieprzestrzegania. Udokumentowanie polityki kontroli dostępu może znacznie ułatwić jej przestrzeganie i egzekwowanie.

Decyzje dotyczące polityk w innych obszarach bezpieczeństwa informacji, takich jak te opisane w niniejszej publikacji, są często dokumentowane w analizie ryzyka, świadectwach akredytacji lub podręcznikach zawierających procedury. Jednak wszelkie kontrowersyjne, nietypowe lub niespotykane polityki również będą wymagały sformalizowania. Nietypowe polityki mogą dotyczyć obszarów, w których polityka dla danego systemu różni się od polityki organizacyjnej lub od normalnej praktyki

w organizacji. Dokumentacja nietypowej polityki zawiera wyjaśnienie powodu odstępstwa od standardowej polityki organizacji.

5.4.3 Wdrażanie polityki dotyczącej konkretnego systemu

Technologia odgrywa ważną rolę w egzekwowaniu polityk dotyczących konkretnych systemów, ale to nie na niej spoczywa wyłączna odpowiedzialność za spełnienie potrzeb organizacji w zakresie bezpieczeństwa. Jeśli do egzekwowania polityki wykorzystywana jest technologia, ważne jest również rozważenie wdrożenia metod ręcznych. Na przykład środki techniczne oparte na systemie można wykorzystać do ograniczenia drukowania poufnych raportów na określonej drukarce. Należy jednak wprowadzić odpowiednie fizyczne środki bezpieczeństwa w celu ograniczenia dostępu do wydruków, w przeciwnym razie pożądany cel bezpieczeństwa nie zostanie osiągnięty.

Do metod technologicznych często stosowanych do realizacji polityki bezpieczeństwa systemu można zaliczyć stosowanie logicznej kontroli dostępu. Przykładami środków kontroli dostępu mogą być: rozdzielenie obowiązków, które jest środkiem kontroli zaprojektowanym w celu wyeliminowania możliwości nadużywania nadanych uprawnień i pomagającym zmniejszyć ryzyko złośliwych działań bez udziału w zmowie oraz zasada minimalnych uprawnień, która umożliwia użytkownikom lub procesom działającym w imieniu użytkowników tylko taki autoryzowany dostęp, który jest niezbędny do wykonania przydzielonych zadań zgodnie z misją organizacji i funkcjami biznesowymi. Istnieją jednak inne zautomatyzowane środki egzekwowania lub wspierania polityki bezpieczeństwa, które zwykle uzupełniają logiczną kontrolę dostępu. Na przykład oprogramowanie do wykrywania włamań może ostrzegać administratorów systemu o podejrzanej aktywności, a nawet podejmować działania w celu jej powstrzymania.

Egzekwowanie polityki bezpieczeństwa systemu w oparciu o technologię ma zarówno zalety, jak i wady. System, odpowiednio zaprojektowany, zaprogramowany, zainstalowany, skonfigurowany i utrzymywany, zapewnia skuteczną realizację polityki w swoim obrębie, ale żaden system nie może zmusić użytkowników do przestrzegania wszystkich procedur. Środki zarządcze również odgrywają ważną rolę

w egzekwowaniu polityki, więc ich zaniedbanie byłoby szkodliwe dla organizacji. Ponadto odstępstwa od polityki mogą być czasami konieczne i właściwe, ale trudne do wdrożenia przy niektórych środkach technicznych. Sytuacja taka występuje często, gdy realizacja polityki bezpieczeństwa jest zbyt rygorystyczna, co może mieć miejsce, gdy analitycy systemowi nie potrafią przewidzieć pewnych ewentualności i przygotować się na nie.

5.5 Współzależności

Polityka związana jest z wieloma tematami poruszanymi w niniejszej publikacji.

- *Zarządzanie programem.* Polityka jest wykorzystywana do ustanowienia programu bezpieczeństwa informacji w organizacji, dlatego jest ściśle związana z zarządzaniem i administrowaniem programem. Zarówno politykę programową, jak i dotyczącą konkretnego systemu można zaimplementować w każdym z obszarów omówionych w niniejszej publikacji. Na przykład organizacja może dążyć do uzyskania spójnego podejścia do planowania awaryjnego dla wszystkich swoich systemów i w tym celu opracuje odpowiednią politykę programową. W innym przypadku może zdecydować, że jej systemy są na tyle niezależne od siebie, że ich właściciele mogą zajmować się incydentami indywidualnie.
- *Kontrola dostępu.* Polityka dotycząca konkretnego systemu jest często realizowana za pomocą kontroli dostępu. Na przykład, w ramach polityki można zdecydować, że tylko dwie osoby w organizacji są upoważnione do uruchomienia programu drukowania czeków. Środki kontroli dostępu są wykorzystywane przez system do wdrożenia i egzekwowania tej polityki.
- *Powiązania z bardziej ogólnymi politykami organizacji.* Ważne jest, aby zrozumieć, że polityki bezpieczeństwa informacji są często rozszerzeniami innych polityk organizacji. Aby zminimalizować zamieszanie, należy zapewnić wzajemne wsparcie i koordynację realizowania polityki bezpieczeństwa informacji i innych polityk organizacji. Na przykład, polityka organizacji dotycząca poczty elektronicznej może być istotna w kontekście realizowania ogólniejszej polityki prywatności.

5.6 Koszty

Z opracowaniem i wdrożeniem polityki bezpieczeństwa informacji wiąże się szereg potencjalnych kosztów. Najbardziej znaczące koszty wynikają z wdrożenia polityki i radzenia sobie z jej późniejszym wpływem na organizację, jej zasoby i personel. Ustanowienie programu bezpieczeństwa informacji realizującego założenia polityki prawdopodobnie nie będzie tanie.

Do tego mogą jeszcze dojść koszty związane z rozwojem samej polityki. Sporządzanie, przegląd, koordynacja, uzgadnianie, rozpowszechnianie i publikacja polityki mogą wymagać licznych działań administracyjnych i zarządczych. W wielu organizacjach skuteczne wdrożenie polityki może wymagać dodatkowego personelu i szkoleń. Ogólnie rzecz biorąc, koszty poniesione przez organizację w związku z opracowaniem i wdrożeniem polityki bezpieczeństwa informacji będą zależały od tego, jak duże należy wprowadzić zmiany, aby kierownictwo zdecydowało, że osiągnięto akceptowalny poziom ryzyka.

Kosztów zabezpieczenia informacji i systemów nie da się uniknąć. Celem jest zapewnienie, aby środki bezpieczeństwa były współmierne do ryzyka, poprzez osiągnięcie równowagi pomiędzy zabezpieczeniami wymaganymi do spełnienia celów bezpieczeństwa organizacji a kosztem takich zabezpieczeń.

6. ZARZĄDZANIE RYZYKIEM BEZPIECZEŃSTWA INFORMACJI

Ryzyko jest miarą stopnia zagrożenia podmiotu przez potencjalną okoliczność lub zdarzenie i zazwyczaj jest funkcją: (I) niekorzystnych skutków, które powstałyby w przypadku wystąpienia okoliczności lub zdarzenia oraz (II) prawdopodobieństwa ich wystąpienia.

Osoby fizyczne zarządzają ryzykiem każdego dnia, choć mogą nie zdawać sobie z tego sprawy. Rutynowe działania, takie jak zapinanie pasów bezpieczeństwa w samochodzie, noszenie parasola, gdy zapowiadany jest deszcz czy spisywanie listy rzeczy do zrobienia zamiast zaufania swojej pamięci – wszystkie one wchodzą w zakres zarządzania ryzykiem. Osoby fizyczne zdają sobie sprawę z różnych zagrożeń i dla swojego dobra podejmują środki ostrożności, aby się przed nimi uchronić lub zminimalizować ich skutki.

Zarówno administracja publiczna, jak i sektor przemysłowy rutynowo zarządzają niezliczonymi rodzajami ryzyka. Przykładowo, aby zmaksymalizować zwrot z inwestycji, firmy muszą często wybierać między planami inwestycji w rozwój, które są agresywne i obarczone wysokim ryzykiem, a planami, w których rozwój będzie następował wolnej, ale będzie bezpieczniejszy. Takie decyzje wymagają analizy ryzyka w stosunku do potencjalnych korzyści, rozważenia alternatywnych rozwiązań, a w końcu wdrożenia tego, co kierownictwo uzna za najlepszy kierunek działania.

W odniesieniu do bezpieczeństwa informacji, zarządzanie ryzykiem jest procesem minimalizacji ryzyka dla działalności organizacji (np. misji, funkcji, wizerunku i reputacji), jej aktywów, osób, innych organizacji oraz państwa, wynikającego z działania systemu. W publikacji NSC 800-39 określono cztery odrębne etapy zarządzania ryzykiem. Zarządzanie ryzykiem wymaga od organizacji (I) określenia ram ryzyka, (II) oceny ryzyka, (III) reakcji na ryzyko oraz (IV) monitorowania ryzyka.

(I) Określenie ram ryzyka – sposób, w jaki organizacje ustanawiają kontekst ryzyka dla środowiska, w którym podejmowane są decyzje oparte na ryzyku. Celem określania ram ryzyka jest opracowanie strategii zarządzania nim, która opisuje, w jaki sposób organizacja zamierza oceniać ryzyko, reagować na nie i je monitorować – jednocześnie tworząc jasną i przejrzystą percepcję ryzyka, którą

organizacja rutynowo wykorzystuje przy podejmowaniu decyzji inwestycyjnych i operacyjnych.

(II) Ocena ryzyka – sposób, w jaki organizacje analizują ryzyko w kontekście ram ryzyka w organizacji. Celem oceny ryzyka jest określenie: (I) zagrożeń dla działalności i aktywów organizacji, osób fizycznych, innych organizacji oraz państwa; (II) podatności organizacji na zagrożenia wewnętrzne i zewnętrzne; (III) szkód (tj. konsekwencji/skutków) dla organizacji, które mogą wystąpić ze względu na możliwość wykorzystania podatności na zagrożenia; oraz (IV) prawdopodobieństwa wystąpienia szkód.

(III) Reagowanie na ryzyko – sposób, w jaki organizacje reagują na ryzyko po jego stwierdzeniu na podstawie wyników oceny ryzyka. Celem etapu reakcji na ryzyko jest zapewnienie spójnej reakcji na ryzyko w całej organizacji, zgodnie z ramami ryzyka w organizacji, poprzez: (I) opracowywanie alternatywnych kierunków działania w zakresie reagowania na ryzyko; (II) ocenę alternatywnych kierunków działania; (III) określanie odpowiednich kierunków działania zgodnych z tolerancją na ryzyko organizacji; oraz (IV) wdrażanie reakcji na ryzyko w oparciu o wybrane kierunki działania.

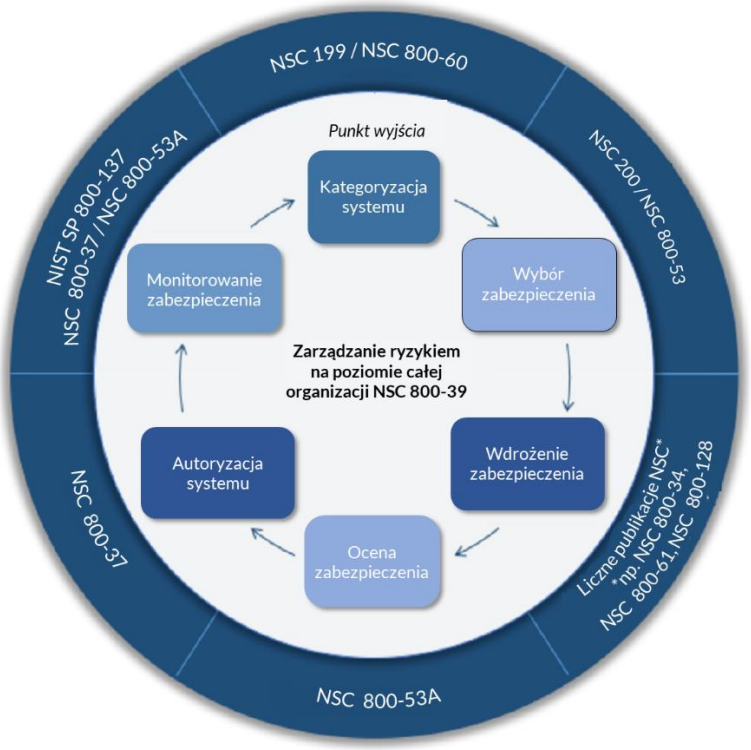
(IV) Monitorowanie ryzyka – sposób, w jaki organizacje monitorują ryzyko na przestrzeni czasu. Celem etapu monitorowania ryzyka jest: (I) sprawdzenie, czy zaplanowane środki reakcji na ryzyko są wdrażane oraz czy spełnione są wymagania dotyczące bezpieczeństwa informacji wynikające/związane z misjami/funkcjami biznesowymi organizacji, ustawodawstwem prawnym, dyrektywami, przepisami, polityką, normami i wytycznymi; (II) określenie przyszłej skuteczności środków reakcji na ryzyko po ich wdrożeniu; oraz (III) identyfikacja zmian mających wpływ na ryzyko w systemach organizacji i środowiskach, w których systemy te działają.

Aby pomóc organizacjom w zarządzaniu ryzykiem bezpieczeństwa informacji na poziomie systemu, NIST opracował ramy zarządzania ryzykiem (*Risk Management Framework – RMF*). W ramach RMF promowane są koncepcje zarządzania ryzykiem w czasie zbliżonym do rzeczywistego oraz ciągłego autoryzowania systemu poprzez

wdrożenie solidnych procesów stałego monitorowania. RMF zawiera również informacje dla liderów wyższego szczebla niezbędne do podejmowania opłacalnych, opartych na ryzyku decyzji w odniesieniu do systemów organizacji wspierających realizację jej głównych misji i funkcji biznesowych, a także włącza bezpieczeństwo informacji do architektury korporacyjnej i cyklu życia systemu (ang. *System Development Life Cycle – SDLC*). Patrz publikacja NIST SP 800-160.

Sześć kroków składających się na RMF to:

1. Kategoryzacja systemu
2. Wybór środków bezpieczeństwa
3. Wdrożenie środków bezpieczeństwa
4. Ocena środków bezpieczeństwa
5. Autoryzacja systemu
6. Monitorowanie środków bezpieczeństwa



Rysunek 1 – Przegląd ram zarządzania ryzykiem (RMF)

6.1 Kategoryzacja

Pierwszy krok RMF koncentruje się na kategoryzacji systemu. W ramach tego kroku organizacje kategoryzują system oraz przetwarzane, przechowywane i przekazywane przez niego informacje w oparciu o analizę wpływu.

Wytyczne dotyczące kategoryzacji bezpieczeństwa dla systemów niebędących systemami bezpieczeństwa narodowego można znaleźć w publikacjach NSC 199 i NSC 800-60.[16].

6.2 Wybór

Drugi etap procesu RMF to wybór wstępnego zestawu podstawowych środków bezpieczeństwa dla systemu w oparciu o kategoryzację bezpieczeństwa, jak również dostosowanie i uzupełnienie tego podstawowego zestawu w zależności od potrzeb w oparciu na ocenie ryzyka i warunków lokalnych w organizacji. Wytyczne dotyczące wyboru środków bezpieczeństwa znajdują się w publikacjach NSC 800-53 i NSC 200.

6.3 Wdrożenie

W trzecim etapie organizacja ma za zadanie wdrożyć środki bezpieczeństwa i opisać, w jaki sposób mają być one stosowane w systemie i jego środowisku działania. Wiele publikacji NIST zawiera informacje na temat wdrażania środków bezpieczeństwa. Są one dostępne do wglądu na stronie internetowej zespołu reagowania na incydenty bezpieczeństwa komputerowego (Computer Security Resource Center)[17].

6.4 Ocena

Czwarty etap umożliwia organizacji ocenę środków bezpieczeństwa przy użyciu odpowiednich procedur oceny oraz określenie zakresu, w jakim są one prawidłowo wdrożone, działają zgodnie z przeznaczeniem i przynoszą pożądane rezultaty w odniesieniu do spełnienia wymagań bezpieczeństwa dla systemu. Publikacja

[16] Krajowa Administracja Archiwów i Rejestrów (*National Archives and Records Administration – NARA*) opracowała rejestr nadzorowanych informacji jawnych (*Controlled Unclassified Information – CUI*). Rejestr CUI jest internetowym repozytorium informacji, wytycznych, polityk i wymogów dotyczących postępowania z CUI, w tym dokumentów wydanych przez organ wykonawczy CUI. Rejestr ten jest dostępny pod adresem https://www.archives.gov/cui/registry/category-list.

[17] Publikacje NIST zostały podane w celach uzupełniających dla osób zainteresowanych.

NSC 800-53A zawiera wytyczne dotyczące opracowania metod i procedur oceny do określania skuteczności środków bezpieczeństwa w systemach publicznych oraz zgłaszania wyników oceny w raporcie oceny bezpieczeństwa.

6.5 Autoryzacja

W piątym etapie osoba autoryzująca oficjalnie autoryzuje system do działania lub dalszego działania w oparciu o wyniki kompleksowej i dokładnej oceny środków bezpieczeństwa. Decyzja ta opiera się na określeniu ryzyka dla działalności i aktywów organizacji, osób fizycznych, innych organizacji i państwa, wynikającego z działania systemu, oraz uznaniu, że ryzyko to jest akceptowalne.

6.6 Monitorowanie

Szóstym etapem RMF jest ciągłe monitorowanie środków bezpieczeństwa w systemie w celu potwierdzenia ich skuteczności na przestrzeni czasu, w miarę jak zachodzą zmiany w systemie i środowisku, w którym system działa. Organizacje na bieżąco monitorują środki bezpieczeństwa w systemie, w tym oceniają ich skuteczność, dokumentują zmiany w systemie lub jego środowisku działania, przeprowadzają analizy wpływu na bezpieczeństwo tych zmian oraz raportują stan bezpieczeństwa systemu do wyznaczonych urzędników organizacji. Szczegółowe wytyczne dotyczące ciągłego monitorowania można znaleźć w publikacji NIST SP 800-137.

7. WIARYGODNOŚĆ

Wiarygodność informacji to stopień pewności, że środki bezpieczeństwa chronią i zabezpieczają informacje i systemy poprzez zapewnienie ich dostępności, integralności, uwierzytelnienia, poufności i niezaprzeczalności. Środki te obejmują zapewnienie możliwości przywrócenia systemów poprzez włączenie zdolności ochrony, wykrywania i reagowania.

Jednak wiarygodność nie daje absolutnej gwarancji, że środki te będą działać zgodnie z założeniami. Zrozumienie tego rozróżnienia jest kluczowe, ponieważ oszacowanie poziomu bezpieczeństwa systemu może być trudne. Niemniej jednak jest to coś, czego jednostki oczekują i co uzyskują, często nie zdając sobie z tego sprawy. Na przykład, ktoś może rutynowo otrzymywać rekomendacje produktów od kolegów, ale może nie uważać takich rekomendacji za w pełni wiarygodne.

W niniejszym rozdziale omówiono planowanie pod kątem wiarygodności oraz przedstawiono dwie kategorie metod i narzędzi zapewniania wiarygodności: projektowanie i późniejsze wdrażanie wiarygodności oraz wiarygodności operacyjnej (podzielonej dalej na audyty i monitorowanie). Podział na te dwie kategorie może być czasem niejednoznaczny, ponieważ w znacznym stopniu się one pokrywają. Takie kwestie jak zarządzanie konfiguracją czy audyty są omawiane w ramach wiarygodności operacyjnej, jednak mogą one być istotne również podczas rozwoju systemu. Podczas procesu projektowania i wdrażania wiarygodności dyskusja zwykle koncentruje się bardziej na kwestiach technicznych i jest połączeniem kwestii dotyczących zarządzania, operacji i kwestii technicznych w ramach wiarygodności operacyjnej.

7.1 Autoryzacja

Autoryzacja to oficjalna decyzja kierownictwa zezwalająca na działanie systemu. Osoba autoryzująca (członek wyższej kadry kierowniczej organizacji) jednoznacznie akceptuje ryzyko eksploatacji systemu dla działalności organizacji (np. misji, funkcji, wizerunku, reputacji), aktywów organizacji, osób fizycznych, innych organizacji i państwa w oparciu o wdrożenie uzgodnionego zestawu środków bezpieczeństwa i prywatności. Osoba autoryzująca i osoba pełniąca funkcję SAOP powinny współpracować. SAOP powinien mieć możliwość przeglądu i zatwierdzania planów

ochrony prywatności przed autoryzacją oraz przegląd pakietów autoryzacyjnych dla systemów zawierających dane osobowe. Dlatego przed podjęciem decyzji o określeniu ryzyka i akceptacji osoba autoryzująca komunikuje się z SAOP w celu rozwiązania wszelkich problemów związanych z ochroną prywatności przed podjęciem ostatecznej decyzji o autoryzacji. Proces autoryzacji wymaga współpracy kierowników i personelu technicznego w celu znalezienia praktycznych, opłacalnych rozwiązań, biorąc przy tym pod uwagę potrzeby związane z bezpieczeństwem, ograniczenia techniczne i operacyjne, wymagania dotyczące innych atrybutów jakości systemu, takich jak prywatność, oraz wymagania dotyczące misji lub działalności.

Aby ułatwić podejmowanie właściwych decyzji w oparciu o ryzyko, opierają się one na wiarygodnych i aktualnych informacjach o wdrożeniu i skuteczności zabezpieczeń – zarówno technicznych, jak i nietechnicznych. Obejmują one:

- funkcje techniczne (czy działają zgodnie z przeznaczeniem?)
- polityki i praktyki operacyjne (czy system jest eksploatowany zgodnie z określonymi politykami i praktykami?)
- ogólne bezpieczeństwo (czy istnieją zagrożenia, przed którymi zabezpieczenia nie chronią?)
- pozostałe ryzyko (czy ryzyko szczątkowe[18] jest na akceptowalnym poziomie?).

Osoba autoryzująca jest odpowiedzialna za autoryzację systemu przed zezwoleniem na jego eksploatację oraz za opracowanie planu stałego monitorowania systemu.

7.1.1 Autoryzacja i wiarygodność

Wiarygodność jest nieodłącznym elementem branym pod uwagę przy podejmowaniu decyzji o dopuszczeniu systemu do eksploatacji. Wiarygodność dotyczy tego, czy środki i procedury techniczne działają zgodnie z zestawem wymogów i specyfikacji bezpieczeństwa oraz z ogólnymi zasadami dotyczącymi jakości.

Osoba autoryzująca podejmuje ostateczną decyzję o tym, jak wiarygodny powinien być dany system i jakiego rodzaju wiarygodność jest wymagana. Aby podjąć właściwą decyzję,

[18] Ryzyko szczątkowe to część ryzyka pozostająca po zastosowaniu środków bezpieczeństwa.

osoba autoryzująca bierze pod uwagę kategoryzację systemu/poziom wpływu i dokonuje przeglądu wyników ocen ryzyka. Osoba autoryzująca analizuje zalety i wady związane z kosztami zapewnienia wiarygodności oraz kosztami środków bezpieczeństwa i ryzyka dla organizacji. Po zakończeniu procesu autoryzacji obowiązkiem osoby autoryzującej jest zaakceptowanie ryzyka szczątkowego dla systemu.

7.1.2 Autoryzacja produktów do działania w podobnych warunkach

Autoryzacja innego produktu lub systemu do działania w podobnych warunkach może być wykorzystana do zapewnienia wiarygodności (np. obustronności). Należy jednak pamiętać, że autoryzacja jest specyficzna dla danego środowiska i systemu. Ponieważ autoryzacja równoważy ryzyko i korzyści, ten sam produkt może zostać uznany za odpowiedni dla jednego środowiska, ale nie dla innego, nawet przez tą samą osobę autoryzującą. Na przykład, osoba autoryzująca może zaaprobować przechowywanie w chmurze danych badawczych, ale nie danych dotyczących zasobów ludzkich, które są obsługiwane przez ten sam system.

7.2 Inżynieria bezpieczeństwa

Rozmiar i złożoność dzisiejszych systemów sprawiają, że budowa godnego zaufania systemu staje się priorytetem. Inżynieria bezpieczeństwa systemów stanowi elementarne podejście do budowania niezawodnych systemów w dzisiejszym złożonym środowisku informatycznym. Więcej informacji na temat inżynierii bezpieczeństwa można znaleźć w publikacji NIST SP 800-160.

7.2.1 Planowanie i wiarygodność

W przypadku systemów nowych lub zmodernizowanych wymagania dotyczące wiarygodności rozpoczynają się w fazie planowania cyklu życia systemu. Planowanie z myślą o wiarygodności stanowi część wymagań dotyczących systemu, ale jest również praktyczne i pomaga personelowi podejmować opłacalne decyzje przy budowie systemu lub przy zakupie komponentów/sprzętu wymaganego do zapewnienia wiarygodności starszego systemu.

7.2.2 Wiarygodność projektu i wdrożenia

Wiarygodność projektu i wdrożenia dotyczy projektu systemu oraz tego, czy cechy systemu, aplikacji lub komponentu spełniają wymagania i specyfikacje bezpieczeństwa. Aby zapewnić wiarygodność projektu i wdrożenia, należy przeanalizować projekt, wdrożenie i instalację systemu. Zwykle jest to związane z fazą rozwoju/nabycia i rozpoczęcia cyklu życia systemu. Można jednak rozważyć zastosowanie tej samej procedury przez cały cykl życia systemu, w miarę jak jest on modyfikowany.

7.2.2.1 Wykorzystanie zaawansowanego lub zaufanego rozwoju

W przypadku rozwoju zarówno standardowych produktów komercyjnych (*ang. Commercial off-the-shelf – COTS*), jak i systemów dostosowanych do potrzeb klienta, wiarygodność może zapewnić zastosowanie zaawansowanych lub zaufanych architektur systemowych, metodologii rozwoju lub technik inżynierii oprogramowania. Przykładami mogą być: weryfikacja projektu i rozwoju bezpieczeństwa, modelowanie formalne, dowody matematyczne, techniki zapewnienia jakości ISO 9000, ISO 15288 (norma dotycząca inżynierii bezpieczeństwa systemów) czy wykorzystanie koncepcji architektury bezpieczeństwa, takich jak zaufana baza przetwarzania (*ang. Trusted Computing Base – TCB*).

Ponieważ nie można w pełni zagwarantować wiarygodności produktów informatycznych, dostępne są uznane procesy oceny pozwalające na określenie poziomu pewności, że ich funkcje bezpieczeństwa oraz zastosowane dla nich środki zapewniające wiarygodność spełniają określone wymagania. Norma ISO 15408 „Wspólne kryteria" (*ang. Common Criteria – CC*) umożliwia uznawanie wyników niezależnych ocen. Norma CC jest przydatna jako poradnik przy opracowywaniu, ocenie i zakupie produktów informatycznych z funkcjami bezpieczeństwa. Więcej informacji na temat normy CC można znaleźć na stronie http://www.commoncriteriaportal.org lub https://buildsecurityin.us-cert.gov/articles/best- practices/requirements-engineering/the-common-criteria.

7.2.2.2 Wykorzystanie niezawodnej architektury

Niektóre architektury systemów są z natury bardziej niezawodne, np. w takich systemach, w których wykorzystano funkcje tolerowania awarii, nadmiarowość,

tworzenie kopii zapasowych (*ang. shadowing*) lub macierze RAID (*ang. Redundant Array of Independent Disks*). Przykłady te związane są przede wszystkim z dostępnością systemu.

7.2.2.3 Osiąganie niezawodnego bezpieczeństwa

Jednym z czynników osiągnięcia niezawodnego bezpieczeństwa jest koncepcja prostego i bezpiecznego użytkowania, która postuluje, że system, który jest łatwiejszy do zabezpieczenia, ma większe szanse bycia rzeczywiście bezpiecznym. Jest bardziej prawdopodobne, że funkcje bezpieczeństwa będą wykorzystywane, jeśli podczas inicjowania systemu domyślnie wybrano opcję „najbardziej bezpieczną". Ponadto, bezpieczeństwo systemu może być uznane za bardziej niezawodne, jeśli nie wykorzystano w nim nowych technologii, które nie zostały jeszcze przetestowane w praktyce (często nazywanych technologiami „bleeding-edge"[19]). Z kolei system, w którym wykorzystuje się starsze, dobrze przetestowane oprogramowanie, może być mniej podatny na błędy.

7.2.2.4 Oceny

Ocena produktu zazwyczaj obejmuje jego testowanie. Oceny mogą być przeprowadzane przez wiele typów organizacji, w tym: krajowe i zagraniczne organizacje rządowe, niezależne podmioty, takie jak organizacje handlowe i branżowe, inni dostawcy lub grupy komercyjne, indywidualni użytkownicy albo konsorcja użytkowników. Recenzje produktów w literaturze branżowej są formą oceny, podobnie jak bardziej formalne przeglądy dokonywane według określonych kryteriów. Ważnymi czynnikami, które należy wziąć pod uwagę przy korzystaniu z ocen, są: stopień niezależności grupy oceniającej, zgodność kryteriów oceny z wymaganymi zabezpieczeniami, rygor testowania, środowisko testowe, termin wykonania oceny, kompetencje organizacji oceniającej oraz ograniczenia nałożone na oceny przez grupę oceniającą (np. założenia dotyczące zagrożenia lub środowiska operacyjnego).

[19] *Bleeding edge* odnosi się do produktu lub usługi, zazwyczaj związanej z technologią, która jest dostępna dla konsumentów, ale jest tak nowa i eksperymentalna, że nie została w pełni przetestowana i w konsekwencji może być zawodna. Pierwsi użytkownicy mogą doświadczyć wad projektowych i błędów, które nie zostały zauważone przez twórców.

7.2.2.5 Dokumentacja wiarygodności

Umiejętność opisania wymagań bezpieczeństwa i sposobu ich spełnienia może odzwierciedlać stopień, w jakim projektant systemu lub produktu rozumie istotne kwestie bezpieczeństwa. Jeśli projektant nie rozumie szeroko pojętych wymagań dotyczących bezpieczeństwa, jest mało prawdopodobne, że będzie w stanie je spełnić.

Dokumentacja wiarygodności może dotyczyć bezpieczeństwa systemu lub jego poszczególnych komponentów. Dokumentacja na poziomie systemu opisuje wymagania bezpieczeństwa systemu i sposób ich spełnienia, w tym powiązania między aplikacjami, systemem operacyjnym lub sieciami. Dokumentacja na poziomie systemu to nie tylko opis systemu operacyjnego, systemu bezpieczeństwa i aplikacji – opisuje ona system w stanie zintegrowanym i wdrożonym w danym środowisku. Dokumentacja komponentów będzie zazwyczaj nabywana wraz z gotowym produktem, natomiast dokumentację systemu będzie zazwyczaj opracowywał projektant lub wdrożeniowiec.

7.2.2.6 Gwarancje, oświadczenia o integralności i zobowiązania

Gwarancje są dodatkowym źródłem wiarygodności. To, że producent, wytwórca, programista systemu lub integrator jest gotów naprawić błędy w określonych ramach czasowych lub do następnego wydania, daje zarządzającemu systemem poczucie zaangażowania w produkt, a także przemawia za jakością produktu. Oświadczenie o integralności jest formalną deklaracją lub certyfikacją produktu. Może ono być uzupełnione o zobowiązanie (a) naprawienia artykułu (tj. gwarancja) lub (b) pokrycia strat (tj. zobowiązanie), jeśli produkt nie będzie zgodny z oświadczeniem o integralności.

7.2.2.7 Opublikowane zapewnienia producenta

Wiarygodność wynikająca z opublikowanych zapewnień lub formalnych deklaracji producenta lub dewelopera jest ograniczona i oparta na reputacji. W przypadku istnienia umowy sama reputacja staje się niewystarczająca, biorąc pod uwagę odpowiedzialność prawną nałożoną na producenta.

7.2.2.8 Wiarygodność dystrybucji

Często ważne jest, aby wiedzieć, że oprogramowanie dotarło niezmodyfikowane, zwłaszcza jeśli jest rozpowszechniane elektronicznie. W takim przypadku pewność, że kod nie został zmodyfikowany, mogą zapewnić bity kontrolne lub podpisy cyfrowe. Do sprawdzenia oprogramowania pochodzącego ze źródeł o nieznanej wiarygodności (np. forum internetowego) można wykorzystać oprogramowanie antywirusowe.

7.3 Wiarygodność operacyjna

Wiarygodność projektu i wdrożenia obejmuje również jakość zabezpieczeń wbudowanych w systemy. Wiarygodność operacyjna odnosi się tego, czy zabezpieczenia są omijane lub podatne na zagrożenia oraz czy są przestrzegane wymagane procedury. Nie dotyczy to zmian w wymaganiach bezpieczeństwa systemu, które mogą być spowodowane zmianami w systemie i jego środowisku operacyjnym lub zagrożeniami (kwestia takich zmian została omówiona w podrozdziale 10.15).

Poziom bezpieczeństwa ma tendencję do obniżania się podczas fazy eksploatacji w cyklu życia systemu. Użytkownicy i operatorzy systemów odkrywają nowe sposoby celowego lub niezamierzonego obchodzenia lub naruszania zabezpieczeń, zwłaszcza jeśli są przeświadczeni, że takie działanie poprawia funkcjonalność lub że nie będzie miało żadnych konsekwencji dla nich lub ich systemów. Ścisłe przestrzeganie procedur jest rzadkością. Polityka staje się nieaktualna, a w administracji systemu nagminnie pojawiają się błędy.

Organizacje stosują trzy podstawowe metody utrzymania wiarygodności operacyjnej opisane poniżej.

- *Ocena systemu.* Pojedyncze działanie lub ciągły proces mający na celu ocenę bezpieczeństwa. Ocena może mieć bardzo różny zakres – może obejmować cały system w celu jego autoryzacji lub zbadanie jednego nietypowego zdarzenia.
- *Audyt systemu.* Niezależny przegląd oraz badanie dokumentacji i działań w celu oceny adekwatności zabezpieczeń systemu oraz zapewnienia zgodności z ustalonymi politykami i procedurami operacyjnymi.

- *Monitorowanie systemu.* Proces utrzymywania stałej świadomości w zakresie bezpieczeństwa informacji, podatności na zagrożenia i zagrożeń w celu ułatwienia podejmowania decyzji dotyczących zarządzania ryzykiem w organizacji.

Ogólnie rzecz ujmując, im bardziej dane działanie jest wykonywane „w czasie rzeczywistym", tym bliżej mu do kategorii monitorowania. To rozróżnienie może powodować niepotrzebne semantyczne nieporozumienia, zwłaszcza w odniesieniu do ścieżek audytu generowanych przez system. Codzienny lub cotygodniowy przegląd ścieżki audytu pod kątem prób nieautoryzowanego dostępu jest na ogół uznawany za proces monitorowania, natomiast przegląd archiwalnej ścieżki z kilku miesięcy (np. śledzenie działań konkretnego użytkownika) jest zazwyczaj traktowany jako audyt. Ogólnie rzecz biorąc, specyficzne określenia stosowane w odniesieniu do działań związanych z zapewnieniem wiarygodności są jednak znacznie mniej ważne niż rzeczywista praca nad utrzymaniem wiarygodności operacyjnej.

7.3.1 Ocena środków bezpieczeństwa i zabezpieczeń prywatności

Oceny mogą dotyczyć jakości systemu w postaci zbudowanej, wdrożonej lub eksploatowanej. Oceny mogą być przeprowadzane w trakcie tworzenia systemu, po jego zainstalowaniu oraz w fazie operacyjnej. Metody oceny obejmują rozmowy, badania i testy. Niektóre z powszechnie stosowanych technik testowania to testy funkcjonalne (sprawdzenie, czy dana funkcja działa zgodnie z wymaganiami) lub testy penetracyjne (sprawdzenie, czy można obejść zabezpieczenia). Zakres takich technik jest szeroki, od kilku przypadków testowych aż do dogłębnych badań z wykorzystaniem metryk, narzędzi automatycznych lub wielu szczegółowych przypadków testowych. Wytyczne dotyczące oceny można znaleźć w publikacji NSC 800-53A.

7.3.2 Metody i narzędzia audytu

Audyt przeprowadzony z myślą o wiarygodności operacyjnej ma na celu zbadanie czy system spełnia wyraźnie określone lub dorozumiane wymagania bezpieczeństwa, a także polityki dotyczące danego systemu i organizacji. W ramach niektórych audytów bada się również, czy wymagania bezpieczeństwa są odpowiednie, choć jest to poza zakresem wiarygodności operacyjnej (patrz podrozdział 10.15). Mniej formalne audyty są często nazywane przeglądami bezpieczeństwa.

Audyty mogą być przeprowadzane samodzielnie lub niezależne, co oznacza, że mogą być zarządzane przez osoby z organizacji lub spoza niej. Oba rodzaje mogą dostarczyć wyczerpujących informacji na temat technicznych, proceduralnych, zarządczych lub innych aspektów bezpieczeństwa. Zasadniczą różnicą pomiędzy audytem samodzielnym a niezależnym jest obiektywizm. Przeglądy przeprowadzane przez personel zarządzający systemem, często nazywane samokontrolami/samoocenami, wiążą się z nieodłącznym konfliktem interesów. Pracownicy zarządzający systemem mogą mieć niewielką motywację do zgłaszania, że system został źle zaprojektowany lub jest niedbale obsługiwany. Z drugiej strony, mogą być motywowani silnym pragnieniem poprawy bezpieczeństwa swojego systemu. Ponadto doskonale znają system i mogą być w stanie znaleźć ukryte problemy.

Niezależny audytor, w przeciwieństwie do nich, nie zajmuje się zawodowo danym systemem. Osoba przeprowadzająca niezależny audyt jest niezwiązana z daną organizacją i wolna od osobistych lub zewnętrznych ograniczeń, które mogłyby wpłynąć na jej niezawisłość. Niezależny audyt może być przeprowadzony przez profesjonalny zespół audytorów zgodnie z ogólnie przyjętymi standardami.

Istnieje wiele metod i narzędzi, które można wykorzystać do audytu, niektóre z nich zostały opisane poniżej.

7.3.2.1 Narzędzia automatyczne

Nawet w przypadku małych systemów z wieloma użytkownikami, ręczne sprawdzanie zabezpieczeń może wymagać znacznych zasobów. Narzędzia automatyczne umożliwiają sprawdzenie nawet dużych systemów pod kątem różnych wad zabezpieczeń i podatności.

Istnieją dwa rodzaje narzędzi automatycznych: (1) narzędzia aktywne, które znajdują podatności na zagrożenia poprzez próbę ich wykorzystania; oraz (2) testy pasywne, które jedynie badają system i wnioskują o istnieniu problemów na podstawie jego stanu.

Narzędzia automatyczne mogą być wykorzystywane do wyszukiwania różnych zagrożeń i podatności na zagrożenia, takich jak: niewłaściwa kontrola dostępu lub konfiguracje kontroli dostępu, słabe hasła, brak integralności oprogramowania systemowego lub niezainstalowanie wszystkich istotnych aktualizacji i poprawek oprogramowania. Narzędzia te są często bardzo skuteczne w znajdowaniu podatności

na zagrożenia i bywają wykorzystywane przez hackerów do włamywania się do systemów. Wykorzystanie tych narzędzi zapewnia administratorom systemu spore korzyści. Wiele z tych narzędzi jest prostych w użyciu. Jednak niektóre programy (np. narzędzia do audytu kontroli dostępu w dużych systemach mainframe) wymagają specjalistycznych umiejętności do obsługi i interpretacji.

7.3.2.2 Audyt istniejących środków bezpieczeństwa

Audytor może dokonać przeglądu istniejących zabezpieczeń i ustalić, czy są one skuteczne. Będzie on często analizował zarówno środki systemowe, jak i pozasystemowe. Stosowane techniki obejmują badanie, obserwację i testowanie zarówno danych, jak i samych środków bezpieczeństwa. W ramach audytu można również wykryć działania niezgodne z prawem, błędy, nieprawidłowości lub brak zgodności z przepisami. Można również wykorzystać plany bezpieczeństwa systemu oraz testy penetracyjne omówione poniżej.

7.3.2.3 Wykorzystanie planu bezpieczeństwa systemu (SSP)

Plan bezpieczeństwa systemu (*ang. System Security Plan – SSP*) zawiera szczegóły wdrożenia, na podstawie których można przeprowadzić audyt. Plan ten, omówiony w podrozdziale 10.12, zawiera najważniejsze zagadnienia związane z bezpieczeństwem systemu, w tym kwestie zarządcze, operacyjne i techniczne. Jedną z zalet stosowania planu bezpieczeństwa systemu jest to, że odzwierciedla on unikalne środowisko bezpieczeństwa systemu, nie jest to jedynie ogólna lista zabezpieczeń. Można opracować zestawy środków bezpieczeństwa, w tym krajowe lub organizacyjne polityki i praktyki (często określane jako zabezpieczenia bazowe). SSP jest również używany do celów archiwalnych oraz w przypadkach, w których istnieją połączenia międzysystemowe i może być konieczne udostępnienie go innym organizacjom.

Zabezpieczenia bazowe są punktem wyjścia w procesie wyboru środków bezpieczeństwa dla systemu. Aby zapewnić wstępny zestaw zabezpieczeń dla określonego poziomu wpływu, określono trzy grupy zabezpieczeń bazowych, odpowiadające systemom o niskim, umiarkowanym i wysokim poziomie wpływu, wykorzystując do tego celu koncepcję

najwyższej wartości[20] opisaną w publikacji NSC 200. Po wybraniu zestawu podstawowych zabezpieczeń organizacje korzystają z wytycznych dotyczących dostosowywania zawartych w publikacji NSC 800-53 w celu usunięcia niektórych z nich (z uzasadnieniem opartym na ryzyku) lub dodania zabezpieczeń kompensacyjnych lub uzupełniających w celu zwiększenia poziomu bezpieczeństwa konkretnego systemu.

Należy zadbać o to, aby odstępstwa od bazowego zestawu zabezpieczeń były oparte na ocenie związanego z tym ryzyka, ponieważ zmiany te mogą być odpowiednie dla danego środowiska systemu lub ograniczeń technicznych.

7.3.2.4 Testowanie penetracyjne

W ramach testowania penetracyjnego można próbować włamać się do systemu na różne sposoby. Oprócz korzystania z aktywnych narzędzi automatycznych, jak to opisano powyżej, testowanie penetracyjne można wykonywać również „ręcznie". Najbardziej użyteczny rodzaj testów penetracyjnych polega na wykorzystaniu metod, które mogłyby zostać użyte przeciwko systemowi. W przypadku hostów w Internecie z pewnością będą to narzędzia automatyczne. W przypadku wielu systemów niedbałe procedury lub brak wewnętrznych środków bezpieczeństwa aplikacji są powszechnymi podatnościami na zagrożenia, na które mogą być ukierunkowane testy penetracyjne. Inną metodą jest inżynieria społeczna, która polega na oszukiwaniu użytkowników lub administratorów w celu ujawnienia informacji o systemach, w tym ich haseł.

7.3.2.5 Metody i narzędzia służące do monitorowania

Monitorowanie bezpieczeństwa jest działaniem ciągłym polegającym na wyszukiwaniu podatności na zagrożenia i problemów związanych z bezpieczeństwem. Wiele stosowanych metod jest podobnych do tych wykorzystywanych podczas audytów, ale używa się ich bardziej regularnie lub w przypadku niektórych zautomatyzowanych narzędzi, w czasie rzeczywistym.

[20] Koncepcja najwyższej wartości — w przypadku systemu, potencjalne wartości wpływu przypisane do stosownych atrybutów bezpieczeństwa (poufności, integralności, dostępności) są to najwyższe wartości pośród tych atrybutów, które zostały określone dla poszczególnych rodzajów informacji przetwarzanych w danym systemie (zaczerpnięto z publikacji NSC 199).

7.3.2.6 Przegląd dzienników systemu

Okresowy przegląd lub wykorzystanie automatycznych narzędzi do analizy dzienników generowanych przez system może umożliwić wykrycie problemów z bezpieczeństwem, w tym prób przekroczenia uprawnień dostępu lub uzyskania dostępu do systemu w nietypowych godzinach (patrz podrozdział 10.15).

7.3.2.7 Narzędzia automatyczne

System można monitorować pod kątem problemów z bezpieczeństwem za pomocą kilku rodzajów automatycznych narzędzi. Poniżej kilka przykładów.

- Programy do wykrywania złośliwych kodów są popularnym sposobem kontroli pod kątem infekcji tego typu. Wykrywają one obecność złośliwego kodu w plikach wykonywalnych programów.
- Funkcje sumy kontrolnej generują wartość matematyczną używaną do wykrywania zmian w danych na podstawie zawartości pliku. Podczas weryfikowania integralności pliku suma kontrolna wygenerowana dla bieżącego pliku jest porównywana z wartością wygenerowaną wcześniej. Jeśli obie wartości są równe, potwierdza to integralność pliku. Użycie funkcji sumy kontrolnej dla programu umożliwia wykrycie złośliwego kodu, przypadkowych zmian w plikach oraz innych zmian w plikach. Mogą jednak zostać potajemnie podmienione w systemie przez intruza. Podpis cyfrowy nie tylko chroni przed przypadkowymi zmianami w plikach. Jest zdecydowanie lepszym rozwiązaniem niż suma kontrolna. Można go użyć również do weryfikacji integralności pliku.
- Programy sprawdzające siłę hasła umożliwiają przetestowanie haseł w oparciu o słowniki („zwykły” słownik, wyspecjalizowany słownik z łatwymi do odgadnięcia hasłami, albo oba), a także sprawdzenie czy hasła nie są typowymi permutacjami identyfikatora użytkownika. Przykładem haseł w słowniku specjalnym mogą być nazwy regionalnych drużyn sportowych i nazwiska gwiazd. Typową permutacją może być identyfikator użytkownika pisany wspak albo dodawanie liczb lub znaków specjalnych po często występujących hasłach.

- Programy do weryfikowania integralności mogą być wykorzystywane przez aplikacje do poszukiwania dowodów na manipulowanie danymi, błędy i pominięcia. Wykorzystywane techniki obejmują kontrole spójności i zasadności oraz walidację podczas wprowadzania i przetwarzania danych. Techniki te mogą służyć do sprawdzania elementów danych – podczas wprowadzania lub przetwarzania – pod kątem oczekiwanych wartości lub zakresów wartości, do analizowania transakcji pod kątem właściwego przebiegu, kolejności i autoryzacji lub do badania elementów danych pod kątem oczekiwanych zależności. Programy do weryfikowania integralności obejmują podstawowy zestaw procesów mających na celu zapewnienie osób fizycznych, że niewłaściwe działania, zarówno przypadkowe, jak i celowe, zostaną wychwycone. Działanie wielu programów do weryfikowania integralności polega na rejestrowaniu działań użytkowników indywidualnych.
- Systemy wykrywania włamań oparte na hostach analizują ścieżkę audytu systemu pod kątem aktywności, która mogłaby stanowić nieautoryzowane działanie, w szczególności logowania, połączenia, wywołania systemów operacyjnych i różne parametry poleceń. Wykrywanie włamań omówiono w podrozdziałach 10.1 i 10.3.
- Programy do monitorowania wydajności systemu analizują dzienniki wydajności systemu w czasie rzeczywistym w poszukiwaniu problemów z dostępnością, w tym aktywnych ataków, spowolnień systemu i sieci oraz awarii.

7.3.2.8 Zarządzanie konfiguracją

Zarządzanie konfiguracją daje pewność, że działający system został skonfigurowany zgodnie z potrzebami i standardami organizacji, że wszelkie zmiany, które mają być wprowadzone, zostały sprawdzone pod kątem wpływu na bezpieczeństwo oraz że zmiany te zostały zatwierdzone przez kierownictwo przed wdrożeniem. Zarządzanie konfiguracją może być wykorzystane do zapewnienia, że zmiany zachodzą w identyfikowalnym i kontrolowanym środowisku oraz że nie naruszają one w sposób niezamierzony żadnej z właściwości systemu, w tym jego bezpieczeństwa. Niektóre organizacje, szczególnie te posiadające bardzo duże systemy (np. administracja

rządowa), powierzają zarządzanie konfiguracją zespołowi ds. kontroli konfiguracji. Jeśli taki zespół istnieje, bardzo ważne jest, aby w jego pracach uczestniczył ekspert ds. bezpieczeństwa informacji.

Zmiany w systemie mogą mieć wpływ na bezpieczeństwo. Takie zmiany mogą wprowadzać lub ograniczać podatności na zagrożenia oraz mogą wymagać uaktualniania planu awaryjnego, analizy ryzyka lub autoryzacji. Więcej szczegółowych informacji na temat zarządzania konfiguracją można znaleźć w podrozdziale 10.5.

7.3.2.9 Literatura branżowa / publikacje / wiadomości elektroniczne

Oprócz monitorowania systemu użyteczne może być również monitorowanie zewnętrznych źródeł informacji. Źródła takie jak literatura branżowa, zarówno w formie drukowanej, jak i elektronicznej, zawierają informacje o podatnościach zabezpieczeń na zagrożenia, poprawkach i innych kwestiach mających wpływ na bezpieczeństwo. Na stronie Forum of Incident Response Teams (FIRST)znajduje się elektroniczna lista dyskusyjna, na którą trafiają informacje o zagrożeniach, podatnościach na zagrożenia i poprawkach. Krajowa baza danych dotyczących podatności na zagrożenia (*National Vulnerability Database – NVD*) jest repozytorium opartych na standardach danych dotyczących zarządzania podatnościami na zagrożenia, reprezentowanych za pomocą automatycznego protokołu zabezpieczeń zawartości (*Security Content Automation Protocol – SCAP*). Dane te umożliwiają automatyzację zarządzania podatnościami na zagrożenia, pomiaru poziomu bezpieczeństwa i zgodności z przepisami. NVD zawiera bazy danych list kontrolnych bezpieczeństwa, błędów w oprogramowaniu związanych z bezpieczeństwem, błędnych konfiguracji, nazw produktów i metryk wpływu. Zespół reagowania na incydenty komputerowe w USA (*United States Computer Emergency Readiness Team – US-CERT*), reaguje na poważne incydenty, analizuje zagrożenia i wymienia najważniejsze informacje dotyczące cyberbezpieczeństwa z zaufanymi partnerami z całego świata. Ponadto Centra Wymiany Informacji i Analiz (*Information Sharing and Analysis Center – ISAC*) udostępniają krytyczne dla danego sektora informacje o zagrożeniach fizycznych i w cyberprzestrzeni oraz o sposobach ich łagodzenia w celu zapewnienia świadomości zagrożeń w całym sektorze.

7.4 Współzależności

Wiarygodność jest problemem dla każdego środka ochrony i zabezpieczenia omawianego w tej publikacji. Ważnym faktem, który należy tutaj podkreślić, jest to, że wiarygodność dotyczy nie tylko środków technicznych, lecz także operacyjnych. W tym rozdziale skupiono się na wiarygodności systemów, jednak uzyskanie pewności, że środki zarządcze działają prawidłowo, również jest bardzo ważne. Czy identyfikatory użytkowników i uprawnienia dostępu są aktualizowane? Czy plan awaryjny był testowany? Czy istnieje możliwość ingerencji w ścieżkę audytu? Czy program bezpieczeństwa jest skuteczny? Czy polityki są zrozumiałe i przestrzegane? Jak zauważono we wstępie do tego rozdziału, potrzeba wiarygodności jest bardziej powszechna niż się to często wydaje.

Wiarygodność jest ściśle związana z planowaniem dotyczącym bezpieczeństwa w cyklu życia systemu. Systemy mogą być zaprojektowane tak, aby ułatwić przeprowadzenie różnego rodzaju testów pod kątem określonych wymagań bezpieczeństwa. Planując takie testy na wczesnym etapie projektowania, można ograniczyć koszty. Niektórych rodzajów wiarygodności nie da się uzyskać bez odpowiedniego planowania.

7.5 Koszty

Istnieje wiele metod uzyskania potwierdzenia, że zabezpieczenia działają zgodnie z oczekiwaniami. Ponieważ metody potwierdzania mają raczej charakter jakościowy niż ilościowy, konieczna jest ich ocena. Potwierdzenie może być również dość kosztowne, zwłaszcza jeśli przeprowadzane są obszerne testy. Warto ocenić poziom otrzymanego potwierdzenia w stosunku do kosztów, aby podjąć jak najlepszą decyzję. Ogólnie rzecz biorąc, koszty personelu podnoszą koszty wiarygodności. Zastosowanie narzędzi automatycznych jest na ogół ograniczone do rozwiązywania konkretnych problemów, ale są one zazwyczaj mniej kosztowne.

8. BEZPIECZEŃSTWO PODCZAS OBSŁUGI, WSPARCIA I EKSPLOATACJI SYSTEMU

Obsługa, wsparcie i eksploatacja systemu to wszystkie aspekty związane z funkcjonowaniem systemu. Są to zarówno administrowanie systemem, jak i zadania zewnętrzne względem systemu, które wspierają jego działanie (np. prowadzenie dokumentacji). Obsługa i eksploatacja nie obejmują planowania ani projektowania systemu. Obsługa i eksploatacja każdego systemu, od trzyosobowej sieci lokalnej po ogólnoświatową aplikację obsługującą tysiące użytkowników, ma kluczowe znaczenie dla utrzymania jego bezpieczeństwa. Obsługa, wsparcie i eksploatacja to rutynowe działania, które umożliwiają prawidłowe funkcjonowanie systemów. W ich zakres wchodzi rozwiązywanie problemów z oprogramowaniem lub sprzętem, instalowanie i utrzymanie oprogramowania oraz pomoc użytkownikom w rozwiązywaniu problemów.

Nieuznawanie bezpieczeństwa za element obsługi, wsparcia i eksploatacji systemów może być szkodliwe dla organizacji. W literaturze dotyczącej systemów bezpieczeństwa informacji można znaleźć przykłady, w jaki sposób organizacje osłabiały działanie swoich często kosztownych zabezpieczeń: źle przygotowana dokumentacja, stare konta użytkowników, oprogramowanie powodujące konflikty czy słaba kontrolę kont serwisowych. Polityki i procedury organizacji często nie uwzględniają wielu z tych istotnych kwestii. Najważniejsze z nich to:

- wsparcie użytkowników,
- obsługa oprogramowania,
- zarządzanie konfiguracją,
- tworzenie kopii zapasowych,
- zabezpieczanie nośników,
- dokumentacja,
- utrzymanie systemu.

Cele obsługi i eksploatacji systemu oraz bezpieczeństwa informacji są ze sobą ściśle powiązane, jednak istnieją między nimi różnice. Podstawowym celem obsługi, wsparcia i eksploatacji systemu jest nieprzerwane i poprawne działanie systemu, natomiast cele bezpieczeństwa informacji w systemie to poufność, dostępność i integralność.

Niniejszy rozdział dotyczy działań związanych z obsługą, wsparciem i eksploatacją bezpośrednio związanych z bezpieczeństwem. Każdy środek bezpieczeństwa omówiony w tej publikacji opiera się, w taki czy inny sposób, na obsłudze, wsparciu i eksploatacji systemu. W tym rozdziale skupiono się jednak na obszarach, które nie zostały omówione w innych rozdziałach. Na przykład pracownicy odpowiedzialni za eksploatację zwykle tworzą konta użytkowników w systemie. Temat ten został omówiony w podrozdziale 10.7. Podobnie, wkład personelu odpowiedzialnego za obsługę, wsparcie i eksploatację w program i szkolenia w zakresie bezpieczeństwa został omówiony w podrozdziale 10.2.

8.1 Wsparcie użytkowników

W wielu organizacjach wsparcie użytkowników należy do obowiązków biura obsługi. Biuro obsługi może wspierać całą organizację, jednostkę, konkretny system lub ich kombinację. W przypadku mniejszych systemów bezpośrednie wsparcie dla użytkowników zapewnia zwykle administrator systemu. W przypadku większości systemów doświadczeni użytkownicy zapewniają nieformalne wsparcie dla innych użytkowników. Nierzadko wsparcie dla użytkowników jest ściśle powiązane ze zdolnością organizacji do reagowania na incydenty.

Z punktu widzenia bezpieczeństwa ważne jest, aby pracownicy wsparcia technicznego potrafili rozpoznać, które problemy (zgłaszane im przez użytkowników) są związane z bezpieczeństwem. Na przykład niemożność zalogowania się użytkownika do systemu może wynikać z zablokowania jego konta z powodu zbyt wielu nieudanych prób dostępu. Może to świadczyć o obecności złośliwych użytkowników, którzy próbowali odgadnąć hasło użytkownika.

Ogólnie rzecz biorąc, pracownicy odpowiedzialni za wsparcie, obsługę i eksploatację systemu muszą być w stanie zidentyfikować problemy związane z bezpieczeństwem, odpowiednio na nie zareagować i poinformować odpowiednie osoby. Istnieje szeroki

zakres możliwych problemów z bezpieczeństwem – niektóre z nich to problemy wewnętrzne z aplikacjami niestandardowymi, inne dotyczą produktów standardowych. Dodatkowo problemy mogą mieć charakter programowy lub sprzętowy.

Im bardziej zaangażowany i kompetentny jest personel odpowiedzialny za wsparcie, obsługę i eksploatację systemu, tym mniejszy będzie zakres nieformalnego wsparcia dla użytkowników. Wsparcie zapewniane przez innych użytkowników może być cenne, ale mogą oni nie być świadomi wszystkich problemów w całej organizacji lub tego, jak są one powiązane.

8.2 Obsługa oprogramowania

Oprogramowanie jest podstawą działania systemu organizacji, niezależnie od wielkości i złożoności tego systemu. Dlatego tak ważne jest, aby oprogramowanie funkcjonowało prawidłowo i było chronione przed uszkodzeniem. Istnieje wiele elementów obsługi oprogramowania.

Pierwszym elementem jest kontrolowanie, jakie oprogramowanie jest używane w systemie. Jeśli użytkownicy lub personel obsługujący system może zainstalować i uruchomić w systemie dowolne oprogramowanie, jest on bardziej podatny na wirusy, nieoczekiwane interakcje oprogramowania i programy, które mogą obejść lub ominąć zabezpieczenia. Jedną z metod kontroli oprogramowania jest jego inspekcja lub testowanie przed zainstalowaniem (np. określenie zgodności z niestandardowymi aplikacjami, zidentyfikowanie innych niespodziewanych interakcji). Może to dotyczyć nowych pakietów oprogramowania, aktualizacji, produktów standardowych lub oprogramowania niestandardowego, w zależności od potrzeb. Oprócz kontroli instalowania i uruchamiania nowych programów, organizacje nadzorują również konfigurację i wykorzystanie zaawansowanych narzędzi systemowych. Za pomocą narzędzi systemowych można naruszyć integralność systemów operacyjnych i logicznych kontroli dostępu.

Innym elementem obsługi oprogramowania może być zapewnienie, że oprogramowanie nie zostało zmodyfikowane bez odpowiednich uprawnień. Wymaga to ochrony oprogramowania i kopii zapasowych i może być realizowane za pomocą kombinacji logicznych i fizycznych środków kontroli dostępu.

Wiele organizacji wprowadza również program mający na celu zapewnienie, że oprogramowanie jest odpowiednio licencjonowane, zgodnie z wymogami. Na przykład, organizacja może audytować systemy pod kątem nielegalnych kopii oprogramowania chronionego prawem autorskim. Problem ten dotyczy przede wszystkim systemów (lub urządzeń) użytkowników, ale może wystąpić w każdym rodzaju systemu.

8.3 Zarządzanie konfiguracją

Procesem ściśle związanym ze wsparciem oprogramowania jest zarządzanie konfiguracją – śledzenie i zatwierdzanie zmian w systemie. Zarządzanie konfiguracją może być formalne lub nieformalne i zwykle dotyczy zmian w sprzęcie, oprogramowaniu, sieci i innych elementach. Podstawowym celem zarządzania konfiguracją w zakresie bezpieczeństwa jest zapewnienie, że zmiany w systemie nie zmniejszą w sposób niezamierzony lub nieświadomy poziomu bezpieczeństwa. Można do tego wykorzystać niektóre z metod omówionych w punkcie dotyczącym wsparcia oprogramowania (np. inspekcje i testowanie zmian w oprogramowaniu). Inne metody zostały omówione w rozdziale 7.

Należy zauważyć, że celem bezpieczeństwa jest wiedza o tym, jakie zmiany występują, a nie zapobieganie zmianom w bezpieczeństwie. Mogą zaistnieć okoliczności, w których zmniejszenie poziomu bezpieczeństwa zostanie uznane za dopuszczalne ryzyko ze względu na konieczność realizacji misji. W takich przypadkach zmniejszenie poziomu bezpieczeństwa opiera się na decyzji osoby autoryzującej, która rozważyła wszystkie odpowiednie czynniki. Ponadto wynikający z tego wzrost ryzyka powinien być na bieżąco monitorowany.

Drugim celem zarządzania konfiguracją w zakresie bezpieczeństwa jest zapewnienie, że zmiany w systemie znajdują odzwierciedlenie w innej dokumentacji, takiej jak plan awaryjny. Jeśli zmiana jest duża, może być konieczne ponowne przeanalizowanie niektórych lub wszystkich zabezpieczeń systemu. Problem ten omówiono w podrozdziale 10.15.

8.4 Tworzenie kopii zapasowych

Pracownicy odpowiedzialni za wsparcie techniczne i obsługę systemu, a niekiedy także użytkownicy, tworzą kopie zapasowe oprogramowania, konfiguracji i danych. Funkcja

ta ma kluczowe znaczenie dla planowania awaryjnego. Częstotliwość tworzenia kopii zapasowych zależy od tego, jak często zmieniają się dane i jak ważne są te zmiany. Aby ustalić, jaki harmonogram tworzenia kopii zapasowych jest odpowiedni, należy skonsultować się z administratorami systemu. Ważne jest również sprawdzenie czy kopie zapasowe rzeczywiście nadają się do użytku. Ponadto kopie zapasowe należy przechowywać w bezpieczny sposób (zagadnienie to omówiono poniżej).

8.5 Zabezpieczanie nośników

Zabezpieczenia nośników to różne środki zapewniające fizyczną i środowiskową ochronę oraz rozliczalność cyfrowych i niecyfrowych nośników danych. Przykłady nośników cyfrowych to dyskietki, taśmy magnetyczne, zewnętrzne/wymienne dyski twarde, dyski flash, płyty CD i DVD. Przykładami nośników innych niż cyfrowe są papier i mikrofilm. Z punktu widzenia bezpieczeństwa, zabezpieczenia nośników mają na celu zapobieganie utracie poufności, integralności lub dostępności informacji, w tym danych lub oprogramowania, podczas przechowywania lub rozpowszechniania poza systemem. Może to obejmować przechowywanie informacji przed ich wprowadzeniem do systemu i po ich eksportowaniu.

Zakres stosowania zabezpieczeń nośników zależy od wielu czynników, w tym od rodzaju danych, ilości nośników i charakteru środowiska użytkownika. Ochrona fizyczna i środowiskowa służy do uniemożliwienia dostępu do nośnika osobom nieupoważnionym i chroni przed takimi czynnikami, jak wysoka i niska temperatura czy szkodliwe pola magnetyczne. Jeśli to konieczne w celu uzyskania pełnej rozliczalności, można rejestrować użycie poszczególnych nośników (np. kaset z taśmami), tak aby organizacje mogły pociągnąć upoważnione osoby do odpowiedzialności za ich działania. Więcej informacji na temat ochrony nośników można znaleźć w podrozdziale 10.10.

8.6 Dokumentacja

Dokumentacja wszystkich aspektów wsparcia, obsługi i eksploatacji systemu jest ważna dla zapewnienia ciągłości i spójności. Sformalizowanie praktyk i procedur operacyjnych na odpowiednim poziomie szczegółowości pomaga wyeliminować luki i niedopatrzenia w zakresie bezpieczeństwa, zapewnia nowym pracownikom wystarczająco szczegółowe instrukcje oraz funkcję zapewnienia jakości, która

umożliwia prawidłowe i skuteczne wykonywanie wszystkich operacji. Należy dokumentować również szczegółowe dane dotyczące implementacji zabezpieczeń w systemie. Jest to wiele rodzajów dokumentacji, takich jak plany bezpieczeństwa, plany awaryjne, analizy ryzyka oraz polityki i procedury bezpieczeństwa. Większość zgromadzonych w ten sposób informacji, w szczególności analizy ryzyka i zagrożeń, należy chronić przed nieuprawnionym ujawnieniem. Dokumentacja bezpieczeństwa musi być również aktualna i dostępna. W ramach dostępności należy uwzględnić wyjątkowe czynniki, takie jak konieczność szybkiego dostępu do planu awaryjnego podczas sytuacji awaryjnej.

Niektóre dokumenty bezpieczeństwa mogą wymagać zaprojektowania w celu zaspokojenia potrzeb różnych ról w systemie. Dlatego wiele organizacji dzieli dokumentację na politykę i procedury. Można opracować podręcznik procedur bezpieczeństwa, aby pomóc użytkownikom systemu bezpiecznie wykonywać swoją pracę. W przypadku pracowników odpowiedzialnych za obsługę, eksploatację i wsparcie systemów, podręcznik procedur bezpieczeństwa może w sposób bardzo szczegółowy odnosić się do szerokiej gamy zagadnień technicznych i operacyjnych.

8.7 Utrzymanie systemu

Utrzymanie systemu wymaga fizycznego lub logicznego dostępu do niego. System może być utrzymywany przez personel odpowiedzialny za wsparcie techniczne i eksploatację, dostawców sprzętu lub oprogramowania albo zewnętrznych usługodawców. Niezbędne działania można wykonywać na miejscu lub zdalnie, za pośrednictwem połączeń komunikacyjnych. Może być również konieczne przeniesienie sprzętu do miejsca naprawy w celu przeprowadzenia konserwacji. Jeśli ktoś, kto zazwyczaj nie ma dostępu do systemu, przeprowadza jego konserwację, pojawia się podatność na zagrożenia.

W pewnych okolicznościach konieczne może być podjęcie dodatkowych środków ostrożności (np. badanie przeszłości pracowników serwisu), aby zapobiec niektórym problemom, takim jak „węszenie” w obszarze fizycznym. Jednak, gdy ktoś ma już dostęp do systemu, bardzo trudno jest zapobiec szkodom wyrządzonym w procesie konserwacji.

W wielu systemach dostępne są konta serwisowe. Te specjalne konta logowania są zwykle skonfigurowane fabrycznie, a ustawione hasła są powszechnie znane. Zmiana tych haseł lub inne ograniczenie dostępu do tych kont ma kluczowe znaczenie. Należy opracować procedury zapewniające, że dostęp do wstępnie skonfigurowanych kont będą mieli tylko upoważnieni pracownicy obsługi technicznej. Jeśli konto ma być używane zdalnie, uwierzytelnienie dostawcy usług serwisowych można przeprowadzać z wykorzystaniem połączenia zwrotnego. Umożliwia to upewnienie się, że zdalne działania diagnostyczne rzeczywiście są prowadzone z ustalonego numeru telefonu w siedzibie dostawcy. Inne pomocne techniki to między innymi szyfrowanie i deszyfrowanie komunikacji diagnostycznej, zaawansowane techniki identyfikacji i uwierzytelniania, takie jak tokeny, oraz zdalną weryfikację rozłączenia.

Producenci większych systemów i dostawcy zewnętrzni mogą oferować więcej usług diagnostycznych i pomocniczych, a większe systemy mogą być wyposażone w porty diagnostyczne. Kluczowe jest zapewnienie, aby te porty były używane tylko przez upoważniony personel. Nie mogą być dostępne dla złośliwych użytkowników i powinny być aktywne tylko w razie potrzeby.

8.8 Współzależności

Większość środków bezpieczeństwa omawianych w niniejszej publikacji jest związana z elementami wsparcia, obsługi i eksploatacji systemu, takimi jak:

- *Personel*. Większość pracowników odpowiedzialnych za wsparcie, obsługę i eksploatację ma specjalny dostęp do systemu. Niektóre organizacje przeprowadzają kontrolę przeszłości osób na takich stanowiskach (patrz podrozdział 10.13).
- *Obsługa incydentów*. Personel odpowiedzialny za wsparcie, obsługę i eksploatację systemu może obejmować również pracowników organizacji zajmujących się obsługą incydentów. Nawet jeśli pochodzą oni z odrębnych organizacji, muszą współpracować w celu identyfikacji incydentów i reagowania na nie (patrz podrozdział 10.8).

- *Planowanie awaryjne.* Personel odpowiedzialny za wsparcie, obsługę i eksploatację systemu zwykle wnosi swój techniczny wkład w planowanie awaryjne i wykonuje czynności związane z tworzeniem kopii zapasowych, uaktualnianiem dokumentacji i ćwiczeniem reagowania na sytuacje awaryjne (patrz podrozdział 10.6).
- *Świadomość, szkolenia i edukacja w zakresie bezpieczeństwa.* Personel odpowiedzialny za wsparcie, obsługę i eksploatację systemu jest przeszkolony w zakresie procedur bezpieczeństwa i świadomy znaczenia bezpieczeństwa. Ponadto może przekazywać wiedzę techniczną potrzebną do nauczenia użytkowników, jak zabezpieczać swoje systemy (patrz podrozdział 10.2).
- *Środki fizyczne i środowiskowe.* Personel odpowiedzialny za wsparcie, obsługę i eksploatację systemu często kontroluje bezpośredni obszar fizyczny wokół niego (patrz podrozdział 10.11).
- *Zabezpieczenia techniczne.* Zabezpieczenia techniczne są instalowane, utrzymywane i używane przez personel odpowiedzialny za wsparcie, obsługę i eksploatację systemu. Tworzy on konta użytkowników, dodaje użytkowników do list kontroli dostępu (*ang. access control lists - ACL*), przegląda dzienniki audytu pod kątem nietypowej aktywności, kontroluje masowe szyfrowanie na łączach telekomunikacyjnych i wykonuje niezliczone zadania operacyjne potrzebne do skutecznego stosowania zabezpieczeń technicznych. Ponadto personel odpowiedzialny za wsparcie, obsługę i eksploatację systemu zapewnia niezbędne wsparcie podczas wyboru zabezpieczeń, wykorzystując swoją wiedzę o możliwościach systemu i ograniczeniach operacyjnych (patrz rozdział 10).
- *Wiarygodność.* Personel odpowiedzialny za wsparcie, obsługę i eksploatację systemu dba o to, aby zmiany w systemie nie powodowały powstawania podatności na zagrożenia, stosując metody zapewniające wiarygodność do oceny lub testowania zmian i ich wpływu na system. Wiarygodność operacyjna jest zwykle zapewniana przez personel odpowiedzialny za wsparcie, obsługę i eksploatację systemu (patrz rozdział 7).

8.9 Koszty

Koszt zapewnienia odpowiedniego poziomu bezpieczeństwa w ramach bieżącego wsparcia i eksploatacji systemu zależy w dużej mierze od wielkości i charakterystyki środowiska operacyjnego oraz charakteru prowadzonego przetwarzania. Zatrudnienie dodatkowych specjalistów ds. bezpieczeństwa wsparcia, obsługi i eksploatacji systemu może nie być konieczne. Jeżeli dostępny jest już wystarczający personel wsparcia i obsługi, ważne jest, aby został on przeszkolony w zakresie aspektów dotyczących bezpieczeństwa przydzielonych mu zadań. Wstępne i bieżące szkolenia są kosztem udanego włączenia środków bezpieczeństwa do działań z zakresu wsparcia, obsługi i eksploatacji systemu.

Kolejne koszty są związane z tworzeniem i aktualizacją dokumentacji w celu zapewnienia, że kwestie bezpieczeństwa są odpowiednio odzwierciedlone w polityce wsparcia, obsługi i eksploatacji, procedurach i obowiązkach.

9. KRYPTOGRAFIA

Kryptografia to dziedzina matematyki zajmująca się przekształcaniem danych. Jest to ważne narzędzie do ochrony informacji, wykorzystywane w wielu obszarach bezpieczeństwa informacji. Kryptografia może na przykład pomóc w zapewnieniu poufności i integralności danych. Te atrybuty bezpieczeństwa można uzyskać, stosując różne algorytmy kryptograficzne, takie jak podpisy elektroniczne oraz zaawansowane uwierzytelnianie użytkowników. Chociaż współczesna kryptografia opiera się na zaawansowanej matematyce, użytkownicy mogą czerpać z niej korzyści bez zrozumienia jej naukowych podstaw.

Informacyjnie dla zainteresowanych - NIST opublikował szereg publikacji specjalnych (*Special Publication – SP*) i federalnych standardów przetwarzania informacji (*Federal Information Processing Standard – FIPS*), które można wykorzystać w przypadku stosowania kryptografii w organizacjach. Lista takich publikacji SP i FIPS znajduje się w załączniku A do publikacji NIST SP 800-175B, *Guideline for Using Crypto Standards: Cryptographic Mechanisms*. Podstawę dla publikacji SP i FIPS opracowywanych przez NIST stanowią przepisy prawa, rozporządzenia i dyrektywy wykonawcze oraz inne wytyczne organizacji. Uprawnienia ustawodawcze, polityki i dyrektywy odnoszące się do kryptografii zostały przedstawione w publikacji NIST SP 800-175A, *Guideline for Using Crypto Standards: Directives, Mandates, and Policies*.

Sama kryptografia nie zaspokoi potrzeb z zakresu wiarygodności informacji żadnej organizacji. Natomiast w połączeniu z innymi środkami bezpieczeństwa kryptografia jest przydatnym narzędziem do zaspokojenia szerokiego spektrum potrzeb i wymagań w zakresie bezpieczeństwa informacji. W tym rozdziale opisano podstawowe aspekty głównych technologii kryptograficznych oraz niektóre konkretne sposoby zastosowania kryptografii w celu poprawy poziomu bezpieczeństwa. Omówiono również wybrane istotne kwestie, które należy rozważyć przy wdrażaniu kryptografii do systemów.

9.1 Wykorzystanie kryptografii

Kryptografia służy do ochrony danych zarówno wewnątrz systemu, jak i poza jego granicami. Dane w systemie mogą być wystarczająco chronione za pomocą logicznych i fizycznych środków kontroli dostępu (które można uzupełnić kryptografią). Jednak poza systemem kryptografia jest czasem jedynym sposobem ochrony danych. Dane nie mogą być na przykład chronione przez logiczne lub fizyczne środki kontroli dostępu stosowane przez ich twórcę, gdy są przesyłane przez linie komunikacyjne lub znajdują się w innym systemie. Kryptografia zapewnia rozwiązanie, które chroni dane nawet wtedy, gdy nie są one już pod kontrolą ich twórcy.

9.1.1 Szyfrowanie danych

Jednym z najlepszych sposobów na zapewnienie poufności danych bez ponoszenia dużych kosztów jest zastosowanie szyfrowania. Podczas szyfrowania następuje przekształcenie zrozumiałych danych, zwanych tekstem jawnym, w niezrozumiałą formę, zwaną szyfrogramem. Odwrócenie tego procesu jest możliwe dzięki deszyfrowaniu. Jednym ze sposobów ochrony danych elektronicznych jest zastosowanie zaawansowanego standardu szyfrowania (*ang. Advanced Encryption Standard – AES*). Algorytm AES jest algorytmem kryptograficznym, który można wykorzystać do szyfrowania i deszyfrowania informacji. Po zaszyfrowaniu danych szyfrogram nie musi być chroniony przed ujawnieniem. Jeśli jednak szyfrogram zostanie zmodyfikowany, nie będzie można go poprawnie odszyfrować. Bardziej wyczerpujący opis algorytmu AES można znaleźć w publikacji FIPS 197, *Advanced Encryption Standard (AES).*

Do szyfrowania danych można wykorzystać zarówno kryptografię z kluczem prywatnym, jak i publicznym, chociaż nie wszystkie algorytmy z kluczem publicznym zapewniają szyfrowanie danych. W przypadku stosowania algorytmu z kluczem prywatnym, dane są szyfrowane przy użyciu określonego klucza. Ten sam klucz musi być użyty do odszyfrowania danych. Kiedy do szyfrowania używana jest kryptografia z kluczem publicznym, każda strona może użyć klucza publicznego dowolnej innej strony do zaszyfrowania wiadomości. Jednak tylko strona posiadająca odpowiedni klucz prywatny może odszyfrować, a tym samym odczytać, wiadomość. Istnieje kilka

czynników przemawiających za wyborem jednego lub drugiego rodzaju kryptografii. Na przykład, organizacja może wybrać kryptografię z kluczem publicznym, ponieważ jest ona bardziej bezpieczna i wygodna w użyciu, jako że nie trzeba nikomu przekazywać kluczy prywatnych. Aby kryptografia z kluczem prywatnym mogła zadziałać, musi dojść do przekazania klucza, ponieważ ten sam klucz jest używany do szyfrowania i deszyfrowania konkretnych danych. Bardziej szczegółowe wytyczne dotyczące infrastruktury klucza publicznego (*ang. Public Key Infrastructure – PKI*) znajdują się w publikacji NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, NIST SP 800-57 Part 3, *Recommendation for Key Management: Part 3 - Application Specific Key Management Guidance* oraz NIST SP 800-152, *A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS).*

9.1.2 Integralność

Integralność to właściwość danych polegająca na tym, że nie zostały one zmienione w sposób nieuprawniony od momentu ich utworzenia, przesłania lub przechowywania. W systemach nie zawsze istnieje możliwość skanowania informacji przez człowieka w celu ustalenia czy dane zostały usunięte, dodane lub zmodyfikowane. Nawet jeśli skanowanie jest możliwe, dana osoba może nie wiedzieć, jakie powinny być prawidłowe dane. Na przykład, „tak” może zostać zmienione na „nie” lub 1000 USD na 10 000 USD. Dlatego wskazane jest posiadanie zautomatyzowanego sposobu wykrywania zarówno celowych, jak i niezamierzonych modyfikacji danych.

Kody do wykrywania błędów (np. bity parzystości) są od dawna stosowane w protokołach komunikacyjnych, aby wykryć niezamierzone modyfikacje danych, jednak osoba dokonująca ataku, przechwytująca i modyfikująca wiadomość może zastąpić również ten kod. Za pomocą kryptografii można skutecznie wykryć zarówno celowe, jak i niezamierzone modyfikacje.

9.1.3 Podpisy elektroniczne

Współczesne systemy przechowują i przetwarzają dokumenty w formie elektronicznej. Dysponowanie dokumentami w formie elektronicznej pozwala na ich szybkie przetwarzanie i przesyłanie oraz poprawia ogólną efektywność. Zatwierdzenie papierowego dokumentu tradycyjnie odbywało się poprzez złożenie odręcznego

podpisu. Potrzebny jest zatem elektroniczny odpowiednik podpisu ręcznego, który ma taki sam status prawny. Oprócz omówionych powyżej zabezpieczeń integralności, kryptografia może zapewnić sposób powiązania dokumentu z konkretną osobą, jak ma to miejsce w przypadku podpisu ręcznego. Podpisy elektroniczne mogą bazować na algorytmie szyfrowania z kluczem prywatnym lub publicznym. Metody z kluczem publicznym są jednak na ogół łatwiejsze w użyciu.

Samo wykonanie cyfrowego zdjęcia podpisu ręcznego nie zapewnia odpowiedniego poziomu bezpieczeństwa. Taki zdigitalizowany podpis ręczny mógłby być łatwo skopiowany z jednego dokumentu elektronicznego do innego bez możliwości ustalenia, czy odbyło się to legalnie. Natomiast podpis elektroniczny może zostać jednoznacznie zweryfikowany dla jednej wiadomości i tylko dla tej wiadomości. Na przykład, funkcja kryptograficznego skrótu[21], taka jak SHA-3, może być użyta do zwiększenia bezpieczeństwa i skuteczności podpisu cyfrowego, zapewniając, że oryginalna wiadomość nie mogła zostać zmieniona na inną wiadomość z tą samą wartością skrótu, a co za tym idzie, tym samym podpisem. Więcej informacji na temat funkcji skrótu kryptograficznego, w szczególności SHA-3, można znaleźć w publikacji FIPS 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*.

9.1.3.1 Podpisy elektroniczne z kluczem prywatnym

Podpis elektroniczny może zostać złożony przy użyciu kodu uwierzytelniania wiadomości (*ang. Message Authentication Code – MAC*) z kluczem prywatnym. Na przykład, jeśli dwie strony mają wspólny klucz prywatny, a jedna strona otrzymuje dane z kodem MAC, które zostaną poprawnie zweryfikowane przy użyciu wspólnego klucza, strona ta może założyć, że druga strona podpisała dane. W tej metodzie zakłada się, że obie strony mają do siebie zaufanie. Dzięki zastosowaniu kodu MAC uzyskuje się integralność danych i formę podpisu elektronicznego. Przy zastosowaniu dodatkowych środków bezpieczeństwa, takich jak

[21] Funkcja skrótu kryptograficznego (hash) to funkcja skrótu, która została zaprojektowana w celu zapewnienia specjalnych właściwości, w tym odporności na kolizję.

„notarialne”[22] uwierzytelnienie klucza[23] i atrybuty klucza[24], złożenie podpisu elektronicznego jest możliwe nawet wtedy, gdy obie strony sobie nie ufają.

9.1.3.2 Podpisy elektroniczne z kluczem publicznym

Inny rodzaj podpisu elektronicznego nosi nazwę podpisu cyfrowego i jest realizowany z wykorzystaniem algorytmu kryptograficznego z kluczem publicznym. Dane są podpisywane elektronicznie poprzez zastosowanie do nich klucza prywatnego twórcy (dokładny matematyczny proces, na którym jest oparta ta metoda, nie jest istotny w kontekście niniejszego omówienia). Aby przyspieszyć proces, klucz prywatny jest stosowany do krótszej formy danych, zwanej „skrótem” (*ang. „hash”)* lub „skrótem wiadomości” (*ang. message digest”*), a nie do całego zestawu danych. Powstały w ten sposób podpis cyfrowy może być przechowywany lub przesyłany wraz z danymi. Podpis może być zweryfikowany przez dowolną stronę przy użyciu klucza publicznego osoby podpisującej. Funkcja ta jest bardzo przydatna np. przy dystrybucji podpisanych kopii oprogramowania wolnego od wirusów. Każdy odbiorca może sprawdzić, czy program jest nadal pozbawiony wirusów. Jeśli podpis zostanie pomyślnie zweryfikowany, osoba weryfikująca ma pewność, że dane nie zostały zmodyfikowane po podpisaniu i że właściciel klucza publicznego był osobą podpisującą.

NIST wydał standardy podpisu cyfrowego i bezpiecznego skrótu do użytku przez instytucje publiczne w ramach publikacji FIPS 186-4, *Digital Signature Standard* oraz FIPS 180-4, *Secure Hash Standard.*

9.1.4 Uwierzytelnianie użytkowników

Uwierzytelnianie jest procesem, który zapewnia podmiotowi odbierającemu informacje pewność co do źródła informacji. Kryptografia może być wykorzystana do zwiększenia bezpieczeństwa technik uwierzytelniania użytkowników. Jak to omówiono

[22] "Notariusz" to rodzaj placówki, w której odbywa się uwierzytelnienie pochodzenia dzielonego sekretu, czyli miejsce, gdzie potwierdza się, że przesyłający sekret jest rzeczywiście tym za kogo się podaje.

[23] Notarialne uwierzytelnienie klucza – metoda, stosowana w połączeniu z systemami kryptograficznymi (zwanymi systemami notarialnego uwierzytelniania klucza), która zapewnia dodatkowe bezpieczeństwo kluczy poprzez identyfikację nadawcy i odbiorcy, dając tym samym pewność co do autentyczności wymienianych kluczy.

[24] Atrybuty klucza – odrębny identyfikator podmiotu.

w podrozdziale 10.7, kryptografia jest podstawą kilku zaawansowanych metod uwierzytelniania. Zamiast przekazywania haseł przez otwartą sieć, uwierzytelnianie może odbywać się poprzez wykazanie znajomości klucza kryptograficznego. Korzystając z tych metod, można stosować hasło jednorazowe, które nie jest podatne na podsłuch. Uwierzytelnianie użytkowników może bazować na algorytmie szyfrowania z kluczem prywatnym lub publicznym.

9.2 Zagadnienia dotyczące wdrażania

W tym podrozdziale omówiono kilka ważnych zagadnień, które należy rozważyć w przypadku stosowania (np. projektowania, implementacji, integracji) kryptografii w systemie. NIST opracował kilka dokumentów FIPS i SP, które dotyczą wdrażania kryptografii w informacjach i systemach rządowych. Lista tych dokumentów FIPS i SP znajduje się w załączniku A do publikacji NIST SP 800-175B.

9.2.1 Wybór standardów projektowania i wdrażania

NIST i inne organizacje opracowały liczne standardy dotyczące projektowania, wdrażania i stosowania kryptografii oraz włączania jej do systemów zautomatyzowanych. Stosując te standardy, organizacje mogą zmniejszyć koszty i chronić swoje inwestycje w technologię. Zapewniają one rozwiązania, które zostały zaakceptowane przez szeroką społeczność i zweryfikowane przez ekspertów w odpowiednich dziedzinach. Standardy pomagają zapewnić interoperacyjność sprzętu różnych producentów, umożliwiając organizacji wybór spośród różnych produktów w celu znalezienia rozwiązań efektywnych kosztowo.

Menadżerowie i użytkownicy systemów wybierają odpowiedni standard kryptograficzny na podstawie analizy kosztów i skuteczności, trendów w zakresie przyjmowania standardu oraz wymagań dotyczących interoperacyjności. Ponadto każdy standard jest dokładnie analizowany w celu określenia, czy jest on możliwy do zaadoptowania przez organizację w ramach pożądanego zastosowania.

9.2.2 Wybór między wdrożeniem w ramach oprogramowania, sprzętu lub oprogramowania układowego

Kadra kierownicza decydująca o zakupie różnych produktów zabezpieczających, które spełniają dany standard, musi przeanalizować pewne kompromisy pomiędzy bezpieczeństwem, kosztami, prostotą, wydajnością i łatwością wdrożenia. Rozwiązania kryptograficzne można wdrażać w ramach oprogramowania, sprzętu lub oprogramowania układowego. Każda z tych opcji wiąże się z określonymi kosztami i korzyściami.

Ogólnie rzecz biorąc, oprogramowanie jest tańsze i działa wolniej niż sprzęt, chociaż w przypadku zastosowań na dużą skalę sprzęt może być tańszy. Ponadto, oprogramowanie może być mniej bezpieczne, ponieważ jest łatwiejsze do modyfikacji lub obejścia niż równoważne produkty sprzętowe. Odporność na manipulacje sprzętu jest zwykle uważana za bardziej niezawodną.

W wielu przypadkach metody kryptograficzne są wdrażane w ramach urządzenia sprzętowego (np. układu elektronicznego, procesora z pamięcią ROM), ale są kontrolowane przez oprogramowanie. Oprogramowanie to wymaga ochrony integralności, aby mieć pewność, że do urządzenia sprzętowego dostarczane są prawidłowe informacje (np. zabezpieczenia, dane) i nie są one omijane. Z tego względu na ogół rozwiązanie ma charakter hybrydowy, nawet jeśli podstawowa metoda kryptograficzna została wdrożona w ramach sprzętu. Skuteczna ochrona wymaga prawidłowego zarządzania całym rozwiązaniem hybrydowym.

Oprogramowanie układowe można znaleźć w niemal każdym współczesnym urządzeniu technologicznym, w tym w telefonach komórkowych, inteligentnych telewizorach, a nawet w klawiaturach USB. Dlatego ochrona wdrożonego oprogramowania układowego ma kluczowe znaczenie.

Jednym ze sposobów ochrony systemu jest zakup sprzętu z wbudowanymi zabezpieczeniami, które zapobiegają złośliwym modyfikacjom oprogramowania układowego. Więcej informacji na temat zabezpieczania oprogramowania układowego można znaleźć w publikacjach NIST SP 800-147, *BIOS Protection Guidelines* oraz NIST SP 800-155 , *BIOS Integrity Measurement Guidelines*.

9.2.3 Zarządzanie kluczami

Bezpieczeństwo informacji zabezpieczonych za pomocą kryptografii zależy bezpośrednio od ochrony zapewnionej kluczom. Wszystkie klucze muszą być chronione przed modyfikacją, a klucze tajne i prywatne wymagają ochrony przed nieuprawnionym ujawnieniem. Zarządzanie kluczami to procedury i protokoły, zarówno ręczne, jak i zautomatyzowane, stosowane w całym cyklu życia kluczy. Obejmuje on generowanie, dystrybucję, przechowywanie, wprowadzanie, używanie, niszczenie i archiwizację kluczy kryptograficznych.

W małej społeczności użytkowników klucze publiczne i ich „właściciele" mogą być silnie związani poprzez ich zwykłą wymianę (np. umieszczenie ich na płytach CD-ROM lub innych nośnikach). Jednakże prowadzenie elektronicznego biznesu na większą skalę, potencjalnie obejmującego użytkowników rozproszonych po świecie i w ramach organizacji, wymaga środków umożliwiających uzyskiwanie kluczy publicznych drogą elektroniczną z wysokim stopniem pewności co do ich integralności i powiązania z danymi osobami. Obsługa powiązania między kluczem a jego właścicielem jest ogólnie określana mianem infrastruktury klucza publicznego.

Użytkownicy muszą również mieć możliwość dostępu do społeczności posiadaczy kluczy, generowania kluczy (lub zlecania ich generowania w swoim imieniu), udostępniania kluczy publicznych, unieważniania kluczy (np. w przypadku ujawnienia klucza prywatnego) oraz zmiany kluczy. Ponadto może być konieczne stosowanie znaczników czasu/daty oraz archiwizowanie kluczy w celu weryfikacji starych podpisów.

Więcej informacji na temat zarządzania kluczami można znaleźć w publikacjach NIST SP 800-57 Part 1, *Recommendation for Key Management, part 1: General*, NIST SP 800-57 Part 2, *Recommendation for Key Management*, Part 2: *Best Practices for Key Management Organization* oraz NIST SP 800-57 Part 3.

9.2.4 Bezpieczeństwo modułów kryptograficznych

Metody kryptograficzne są zazwyczaj wdrażane w modułach oprogramowania, oprogramowania układowego, sprzętu lub ich kombinacji. Moduł ten zawiera algorytmy kryptograficzne, określone parametry zabezpieczeń oraz tymczasowe miejsca przechowywania kluczy używanych przez te algorytmy. Prawidłowe działanie

kryptografii wymaga bezpiecznego projektu, wdrożenia i wykorzystania modułu kryptograficznego. Obejmuje to ochronę modułu przed manipulacją.

Zgodność ze standardami może być ważna z wielu powodów, w tym ze względu na interoperacyjność lub poziom zapewnionego bezpieczeństwa. NIST opracował program walidacji modułów kryptograficznych (*ang. Cryptographic Module Validation Program – CMVP*) , który umożliwia walidację modułów kryptograficznych pod kątem zgodności ze standardem FIPS 140-2, *Security Requirements for Cryptographic Modules.* Celem CMVP jest promowanie stosowania zatwierdzonych modułów kryptograficznych i zapewnienie instytucjom rządowym wskaźników zabezpieczeń do wykorzystania przy zamawianiu sprzętu zawierającego zatwierdzone moduły kryptograficzne. Lista modułów, które zostały zatwierdzone przez NIST, jest dostępna na stronie centrum zasobów bezpieczeństwa komputerowego (*Computer Security Resource Center – CSRC*).

Standard FIPS 140-2 określa wymagania bezpieczeństwa, które muszą być spełnione przez moduł kryptograficzny wykorzystywany w systemie bezpieczeństwa chroniącym informacje wrażliwe, ale nieobjęte klauzulą tajności. W standardzie tym zdefiniowano cztery poziomy bezpieczeństwa dla modułów kryptograficznych, a każdy kolejny poziom zapewnia znaczne zwiększenie ochrony w stosunku do poprzedniego. Wyróżnienie czterech poziomów umożliwia dobranie opłacalnych rozwiązań, które będą odpowiednie dla różnych stopni wrażliwości danych i różnych środowisk aplikacji. Użytkownik może wybrać najlepszy moduł dla danej aplikacji lub systemu, unikając kosztów niepotrzebnych zabezpieczeń.

9.2.5 Stosowanie kryptografii w sieciach

Wykorzystanie kryptografii w ramach zastosowań sieciowych często wymaga wzięcia pod uwagę specjalnych czynników. W takich zastosowaniach użyteczność modułu kryptograficznego może zależeć od jego zdolności do spełnienia specjalnych wymogów wynikających z lokalnie podłączonego sprzętu komunikacyjnego lub protokołów sieciowych i oprogramowania.

Zaszyfrowane informacje, kody MAC lub podpisy cyfrowe mogą wymagać przejrzystych protokołów komunikacyjnych lub sprzętu, aby uniknąć błędnego

zinterpretowania ich przez sprzęt lub oprogramowanie komunikacyjne jako informacji kontrolnych. Konieczne może być sformatowanie zaszyfrowanych informacji, kodu MAC lub podpisu cyfrowego, aby zapewnić, że nie będą one wprowadzać w błąd sprzętu lub oprogramowania komunikacyjnego. Istotne jest, aby kryptografia spełniała wymagania wynikające z zastosowania urządzeń komunikacyjnych i nie zakłócała prawidłowego i efektywnego działania sieci.

Dane są szyfrowane w sieci przy użyciu metody szyfrowania linii/szyfrowania grupowego (*ang. link encryption/bulk encryption*) lub szyfrowania typu „punkt-punkt" (*ang. end-to-end encryption*). Na ogół szyfrowanie linii jest stosowane przez dostawców usług, takich jak transmisja danych. Umożliwia ono szyfrowanie wszystkich danych na całej ścieżce komunikacyjnej (np. łącza satelitarnego, obwodu telefonicznego, linii telekomunikacyjnego). Ponieważ szyfrowanie grupowe szyfruje również dane routingu, węzły komunikacyjne muszą je odszyfrować, aby kontynuować routing.

W przypadku szyfrowania „punkt-punkt" dane są szyfrowane podczas przechodzenia przez sieć, ale informacje o routingu pozostają niezaszyfrowane. Szyfrowanie to jest zazwyczaj stosowane przez organizację będącą użytkownikiem końcowym. Przykładami współczesnych zastosowań szyfrowania „punkt-punkt" są narzędzia Pretty Good Privacy (PGP) oraz Secure/Multipurpose Internet Mail Extensions (S/MIME) do obsługi poczty elektronicznej. Możliwe jest łączenie obu rodzajów szyfrowania.

9.2.6 Zgodność z przepisami dotyczącymi eksportu

Rząd każdego kraju kontroluje eksport implementacji algorytmów kryptograficznych. Zasady regulujące eksport mogą być dość złożone, ponieważ uwzględniają wiele czynników. Ponadto kryptografia jest dynamicznie rozwijającą się dziedziną, więc zasady te mogą się zmieniać co jakiś czas. Pytania dotyczące eksportu implementacji algorytmów kryptograficznych należy kierować do odpowiedniego organu państwowego odpowiedzialnego za zabezpieczenia kryptograficzne.

9.3 Współzależności

Istnieje wiele współzależności pomiędzy kryptografią i innymi środkami bezpieczeństwa omówionymi w niniejszej publikacji. Metody kryptograficzne zależą od innych zabezpieczeń, ale też pomagają w ich zapewnieniu. Na przykład:

- *Bezpieczeństwo fizyczne.* Fizyczne zabezpieczenie modułu kryptograficznego jest konieczne, aby zapobiec lub przynajmniej wykryć fizyczną wymianę lub modyfikację systemu kryptograficznego i znajdujących się w nim kluczy. W wielu środowiskach (np. otwarte biura, laptopy) sam moduł kryptograficzny musi spełniać określone poziomy bezpieczeństwa fizycznego. W innych środowiskach (np. zamknięte obiekty komunikacyjne, wpłatomaty/bankomaty) moduł kryptograficzny będzie bezpieczny w zabezpieczonym obiekcie.
- *Uwierzytelnianie użytkowników.* Kryptografia może być stosowana zarówno do ochrony haseł przechowywanych w systemach, jak i tych przekazywanych między systemami. Ponadto techniki uwierzytelniania oparte na kryptografii mogą być stosowane w połączeniu z technikami opartymi na hasłach lub zamiast nich, aby zapewnić silniejsze uwierzytelnianie użytkowników.
- *Logiczna kontrola dostępu.* W wielu przypadkach oprogramowanie kryptograficzne może być wbudowane w system hosta, a zapewnienie zaawansowanej ochrony fizycznej danego systemu może nie być wykonalne. W takich przypadkach logiczna kontrola dostępu może być sposobem na odizolowanie oprogramowania kryptograficznego od innych części systemu hosta, ochronę oprogramowania kryptograficznego przed manipulacją oraz zabezpieczenie kluczy przed wymianą lub ujawnieniem. Środki takie stanowią odpowiednik ochrony fizycznej.
- *Ścieżki audytu.* Kryptografia może odgrywać użyteczną rolę w przypadku ścieżek audytu, które są wykorzystywane do wspierania podpisów elektronicznych. Zapisy audytu mogą zawierać podpisy elektroniczne dla zapewnienia integralności, a kryptografia może być potrzebna do ochrony zapisów audytu przechowywanych w systemach przed ujawnieniem lub modyfikacją.

- *Wiarygodność.* Zapewnienie, że moduł kryptograficzny jest prawidłowo i bezpiecznie wdrożony, jest niezbędne do efektywnego wykorzystania kryptografii. NIST prowadzi programy walidacji pod kątem kilku własnych standardów kryptograficznych (patrz podrozdział 9.2.4). Dostawcy mogą poddać swoje produkty walidacji pod kątem zgodności ze standardem przeprowadzając szereg rygorystycznych testów. Testy takie dają większą gwarancję, że moduł spełnia określone standardy, a projektanci systemów, integratorzy i użytkownicy mogą mieć dzięki nim pewność, że produkty poddane walidacji są zgodne z przyjętymi standardami.

Systemy kryptograficzne są monitorowane i okresowo kontrolowane, aby zapewnić, że nadal spełniają swoje cele z zakresu bezpieczeństwa. Weryfikacji podlegają wszystkie parametry związane z prawidłowym działaniem systemu kryptograficznego. Działanie samego systemu jest okresowo testowane, a wyniki podlegają audytowi. Niektóre informacje, takie jak klucze tajne lub klucze prywatne w systemach z kluczem publicznym, nie podlegają audytowi. Natomiast klucze nietajne lub nieprywatne mogą być wykorzystane w symulowanej procedurze audytu.

9.4 Koszty

Wykorzystanie kryptografii do ochrony informacji wiąże się z kosztami zarówno bezpośrednimi, jak i pośrednimi, które są częściowo uwarunkowane dostępnością produktów. Istnieje wiele różnych produktów umożliwiających implementację kryptografii w układach scalonych, płytach rozszerzeń, adapterach oraz samodzielnych jednostkach.

9.4.1 Koszty bezpośrednie

Poniżej opisano źródła bezpośrednich kosztów związanych z kryptografią.

- Zakup lub implementacja modułu kryptograficznego i jego integracja z systemem. Nośnik (tj. sprzęt, oprogramowanie, oprogramowanie układowe lub ich kombinacja) oraz różne inne kwestie, takie jak poziom bezpieczeństwa, konfiguracja logiczna i fizyczna oraz specjalne wymagania dotyczące przetwarzania mające wpływ na koszt.

- Zarządzanie kryptografią oraz generowaniem, dystrybucją, archiwizacją i usuwaniem kluczy kryptograficznych, a także środkami bezpieczeństwa służącymi do ich ochrony.

9.4.2 Koszty pośrednie

Poniżej opisano źródła pośrednich kosztów związanych z kryptografią.

- Spadek wydajności systemu lub sieci, wynikający z dodatkowego obciążenia po zastosowaniu ochrony kryptograficznej do przechowywanych lub przekazywanych danych.
- Zmiany w sposobie interakcji użytkowników z systemem, wynikające z bardziej rygorystycznego egzekwowania środków bezpieczeństwa. Kryptografia może jednak stać się niemal nieodczuwalna dla użytkowników, dzięki czemu jej wpływ jest minimalny.

10. KATEGORIE ŚRODKÓW BEZPIECZEŃSTWA

Standard NSC 200 określa minimalne wymagania bezpieczeństwa w wielu związanych z nim obszarach, mając na celu ochronę poufności, integralności i dostępności. Przedstawione poniżej obszary składają się na szeroko zakrojony, zrównoważony program bezpieczeństwa informacji, który uwzględnia zarządcze, operacyjne i techniczne aspekty ochrony informacji i systemów rządowych.

Ten podrozdział zawiera krótki opis każdej kategorii środków bezpieczeństwa. Dla każdej grupy przygotowano listę środków, które umożliwiają osiągnięcie poszczególnych celów związanych z bezpieczeństwem. Pełny katalog środków bezpieczeństwa, wraz z opisem każdego z nich, można znaleźć w publikacji NSC 800-53.

10.1 Kontrola dostępu (*Access Control – AC*)

Wymagania dotyczące wykorzystywania i zakazy używania różnych zasobów systemowych różnią się znacznie w zależności od systemu. Na przykład niektóre informacje muszą być dostępne dla wszystkich użytkowników, niektóre mogą być potrzebne kilku grupom lub działom, a do niektórych może mieć dostęp tylko kilka osób. Użytkownicy muszą mieć dostęp do określonych informacji potrzebnych im do wykonywania pracy, jednak konieczne może być odmówienie dostępu do danych niezwiązanych z pracą. Ważne może być również kontrolowanie rodzaju dozwolonego dostępu (np. możliwość wykonywania, ale nie zmieniania programów systemowych przez zwykłego użytkownika). Tego typu ograniczenia dostępu ułatwiają egzekwowanie polityki i pomagają uniemożliwić podejmowanie nieuprawnionych działań.

Dostęp to możliwość skorzystania z dowolnego zasobu systemu. Kontrola dostępu to proces spełniania lub odrzucania określonych żądań dotyczących: 1) uzyskania i wykorzystania informacji oraz związanych z nimi usług przetwarzania informacji; oraz 2) wejścia do określonych obiektów fizycznych (np. budynków rządowych, obiektów wojskowych, wejść na przejścia graniczne). Środki kontroli dostępu w systemie nazywane są logicznymi środkami kontroli dostępu. Mogą one decydować nie tylko o tym, kto lub co (w przypadku procesu) ma mieć dostęp do określonego zasobu

systemowego, ale także o dopuszczalnym typie dostępu. Środki te mogą być wbudowane w system operacyjny, włączone do programów użytkowych lub głównych narzędzi (np. systemów zarządzania bazami danych, systemów komunikacyjnych) albo wdrożone w ramach dodatkowych pakietów bezpieczeństwa. Logiczne środki kontroli dostępu mogą być wdrożone wewnętrznie w chronionym systemie lub w urządzeniach zewnętrznych.

Przykładami środków bezpieczeństwa kontroli dostępu są: zarządzanie kontami, rozdzielenie obowiązków, zasada minimalnych uprawnień, blokada sesji, wymuszanie przepływu informacji oraz zakończenie sesji.

Organizacja wprowadza ograniczenia dotyczące: (I) dostępu do systemu dla uprawnionych użytkowników; (II) procesów działających w imieniu uprawnionych użytkowników; (III) urządzeń, w tym innych systemów; oraz (IV) rodzajów transakcji i funkcji, które uprawnieni użytkownicy mogą wykonywać.

10.2 Uświadamianie i szkolenia (*Awareness and Training – AT*)

Często to właśnie społeczność użytkowników jest uznawana za najsłabsze ogniwo w zabezpieczeniach systemu. Wynika to z tego, że użytkownicy nie są świadomi, jak ich działania mogą wpłynąć na bezpieczeństwo systemu. Uświadomienie użytkownikom systemu ich odpowiedzialności za bezpieczeństwo i nauczenie ich prawidłowych praktyk sprzyja zmianie ich zachowań. Wspiera również indywidualną rozliczalność, która jest jednym z najważniejszych sposobów poprawy poziomu bezpieczeństwa informacji. Bez znajomości niezbędnych środków bezpieczeństwa oraz sposobu ich stosowania, użytkownicy nie mogą być naprawdę odpowiedzialni za swoje działania. Znaczenie szkolenia w tym zakresie zostało podkreślone w rozporządzeniu KRI[25], które nakłada obowiązek szkolenia osób zajmujących się zarządzaniem, użytkowaniem i obsługą systemów publicznych[26].

Celem uświadamiania, szkolenia i edukacji w zakresie bezpieczeństwa informacji jest zwiększenie poziomu bezpieczeństwa poprzez: (I) podnoszenie poziomu świadomości

[25] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
[26] § 20 ust. 2 pkt. 6 rozporządzenia KRI

o potrzebie ochrony zasobów systemowych; (II) rozwijanie umiejętności i wiedzy, aby użytkownicy systemu mogli bezpieczniej wykonywać swoje zadania; oraz (III) budowanie pogłębionej wiedzy w zakresie potrzebnym do projektowania, wdrażania i obsługi programów bezpieczeństwa dla organizacji i systemów. Organizacja jest odpowiedzialna za dopilnowanie, aby kierownicy i użytkownicy byli świadomi zagrożeń dla bezpieczeństwa związanych z ich działaniami oraz aby personel organizacji był odpowiednio przeszkolony do wykonywania swoich zadań i obowiązków związanych z bezpieczeństwem informacji.

Przykłady środków bezpieczeństwa w zakresie świadomości i szkoleń: szkolenia uświadamiające w zakresie bezpieczeństwa, szkolenia w zakresie bezpieczeństwa dostosowane do realizowanych ról oraz rejestry szkoleń w zakresie bezpieczeństwa.

Organizacje: (I) zapewniają, że kadra zarządzająca i użytkownicy systemów organizacji są świadomi zagrożeń związanych z ich działaniami oraz z obowiązującymi przepisami, zarządzeniami, dyrektywami, politykami, standardami, instrukcjami, regulacjami, a także z procedurami związanymi z bezpieczeństwem systemów organizacji; oraz (II) zapewniają, że personel organizacji jest odpowiednio przeszkolony do wykonywania przydzielonych mu obowiązków i zadań związanych z bezpieczeństwem informacji.

10.3 *Audyt i rozliczalność (Audit and Accountability – AU)*

Audyt to niezależny przegląd oraz badanie dokumentacji i działań w celu oceny adekwatności zabezpieczeń systemu oraz zapewnienia zgodności z ustalonymi politykami i procedurami operacyjnymi. Ścieżka audytu to zapis dotyczący osób, które uzyskały dostęp do systemu, oraz operacji, które użytkownik wykonał w danym okresie. W ramach ścieżek audytu prowadzony jest zapis aktywności systemu – zarówno procesów systemowych i aplikacji, jak i aktywności użytkowników systemów i aplikacji. W połączeniu z odpowiednimi narzędziami i procedurami, ścieżki audytu mogą ułatwiać wykrywanie naruszeń bezpieczeństwa, problemów z wydajnością i wad aplikacji.

Mogą być również wykorzystywane jako wsparcie dla regularnych operacji systemowych, rodzaj polisy ubezpieczeniowej lub oba te elementy. Jako zabezpieczenie, ścieżki audytu są utrzymywane, ale nie są używane, jeśli nie zajdzie taka potrzeba (np. po awarii systemu). Jako wsparcie dla operacji, ścieżki audytu są wykorzystywane, aby ułatwić

administratorom systemu zapewnienie, że system lub zasoby nie zostały uszkodzone przez hackerów, osoby z organizacji lub przez problemy techniczne.

Przykłady środków bezpieczeństwa związanych z audytem i rozliczalnością: zdarzenia związane z audytem, znaczniki czasu, niezaprzeczalność, ochrona informacji o audycie, przechowywanie zapisów audytu oraz audyt sesji.

Organizacje: (I) tworzą, chronią i przechowują zapisy audytu systemu w zakresie niezbędnym do umożliwienia monitorowania, analizowania, badania i zgłaszania bezprawnych, nieautoryzowanych lub niewłaściwych działań w systemie; oraz (II) zapewniają, że działania poszczególnych użytkowników systemu mogą być do nich jednoznacznie przypisane, tak aby można było pociągnąć ich do odpowiedzialności.

10.4 Szacowanie, autoryzacja i monitorowanie (*Control Assessment – CA*)

Oszacowanie środków bezpieczeństwa to testowanie i/lub ocena zarządczych, operacyjnych i technicznych środków bezpieczeństwa w systemie w celu określenia zakresu, w jakim są one prawidłowo wdrożone, działają zgodnie z przeznaczeniem i przynoszą pożądane rezultaty w odniesieniu do spełnienia wymagań bezpieczeństwa systemu. Szacowanie pomaga również określić, czy wdrożone środki są najbardziej skutecznym i opłacalnym rozwiązaniem dla funkcji, którą mają pełnić.

Oszacowanie środków bezpieczeństwa jest przeprowadzana w sposób ciągły, aby ułatwiać analizę aktualnego stanu bezpieczeństwa organizacji w czasie zbliżonym do rzeczywistego.

Po przeprowadzeniu pełnego i dokładnego oszacowania środków bezpieczeństwa osoba autoryzująca podejmuje decyzję o dopuszczeniu systemu do eksploatacji (w przypadku nowego systemu) lub do dalszego użytkowania.

Przykłady oszacowania bezpieczeństwa i autoryzacji zabezpieczeń obejmują: bezpieczeństwo, połączenia między systemami, plany działania i kamienie milowe oraz ciągłość monitorowania.

Organizacje: (I) okresowo oceniają środki bezpieczeństwa w swoich systemach w celu ustalenia, czy są one skuteczne w danym zastosowaniu; (II) opracowują i wdrażają plany działania mające na celu uzupełnienie braków i ograniczenie lub wyeliminowanie

podatności na zagrożenia w swoich systemach; (III) autoryzują eksploatację systemów organizacji i wszelkich powiązanych połączeń systemowych; oraz (IV) na bieżąco monitorują środki bezpieczeństwa w celu zapewnienia ich nieprzerwanej skuteczności.

10.5 Zarządzanie konfiguracją (*Configuration Management – CM*)

Zarządzanie konfiguracją jest zbiorem działań skoncentrowanych na zapewnieniu i utrzymaniu integralności produktów i systemów informacyjnych poprzez kontrolę procesów inicjalizacji, zmiany i monitorowania konfiguracji tych produktów i systemów w ciągu całego SDLC. Zarządzanie konfiguracją polega na określeniu i udokumentowaniu odpowiednich ustawień specyficznych dla systemu, przeprowadzeniu analiz wpływu na bezpieczeństwo oraz zarządzaniu zmianami w ramach grupy ds. kontroli zmian. Umożliwia przegląd całego systemu, co ułatwia zapewnienie, że zmiana wprowadzona w jednym systemie nie będzie miała negatywnych skutków dla innego systemu. Więcej informacji na temat zarządzania konfiguracją można znaleźć w publikacji NIST SP 800-128.

Powszechne bezpieczne konfiguracje (znane również jako listy kontrolne bezpiecznych konfiguracji[27]) stanowią uznane, znormalizowane i ustalone wzorce, które określają bezpieczne ustawienia konfiguracyjne dla platform i produktów informatycznych. Po wdrożeniu listy kontrolne mogą być wykorzystywane do sprawdzenia czy zmiany w systemie zostały zweryfikowane pod kątem bezpieczeństwa.

W ramach typowego audytu bada się konfigurację systemu, aby sprawdzić, czy nie zaszły istotne zmiany (takie jak podłączenie do Internetu), które nie zostały jeszcze przeanalizowane. Przykładowo, Repozytorium list kontrolnych NIST, prowadzone w ramach krajowej bazy danych dotyczących podatności na zagrożenia (*National Vulnerability Database – NVD*), zawiera listy kontrolne, które można wykorzystać do sprawdzenia zgodności z bezpieczną konfiguracją określoną w planie bezpieczeństwa systemu.

Przykłady środków bezpieczeństwa związanych z zarządzaniem konfiguracją: konfiguracja bazowa, kontrola zmian w konfiguracji, analiza wpływu na

[27] Potoczna nazwa: „czeklisty”.

bezpieczeństwo, minimalna funkcjonalność oraz ograniczenia w użytkowaniu oprogramowania.

Organizacje: (I) ustanawiają i utrzymują konfiguracje bazowe i inwentaryzacje swoich systemów, w tym sprzętu, oprogramowania, oprogramowania układowego i dokumentacji w ciągu całego SDLC; oraz (II) określają i egzekwują ustawienia konfiguracji bezpieczeństwa dla produktów informatycznych używanych w systemach.

10.6 Planowanie awaryjne/Ciągłość działania (*Contingency Planning – CP*)

Zagrożenie bezpieczeństwa informacji to zdarzenie, które potencjalnie może zakłócić działanie systemu, a tym samym realizację podstawowej misji i funkcji biznesowych. Takim zdarzeniem może być przerwa w dostawie prądu, awaria sprzętu, pożar lub wyładowania atmosferyczne. Szczególnie niszczycielskie zdarzenia są często określane mianem „katastrof". Aby zapobiec potencjalnym nieprzewidzianym sytuacjom i katastrofom lub zminimalizować spowodowane przez nie szkody, organizacje mogą podjąć kroki wyprzedzające i kontrolować wynik zdarzenia. Ogólnie czynności te nazywane są planowaniem awaryjnym.

Plan awaryjny to polityka i procedura zarządzania, stosowana w celu kierowania reakcją organizacji na odczuwalną utratę zdolności do realizacji misji. Plan awaryjny systemu (*ang. System Contingency Plan – SCP*) jest wykorzystywany przez osoby odpowiedzialne za zarządzanie ryzykiem do określenia, co się stało, dlaczego i co należy zrobić. W przypadku poważnych zakłóceń działania SCP może wskazać na konieczność realizacji planu kontynuacji operacji (*ang. Continuity of Operations Plan – COOP*) lub planu odtworzenia po katastrofie (*ang. Disaster Recovery Plan – DRP*). Planowanie awaryjne to coś więcej niż tylko przygotowanie do przeniesienia się poza siedzibę organizacji po zniszczeniu centrum danych przez katastrofę. Obejmuje ono również sposoby utrzymania operacyjności krytycznych funkcji organizacji w przypadku zakłóceń, zarówno dużych, jak i małych. To szersze spojrzenie na planowanie awaryjne opiera się na dystrybucji wsparcia systemu w całej organizacji. Więcej informacji na temat planowania awaryjnego można znaleźć w publikacji NSC 800-34.

Przykłady środków bezpieczeństwa związanych z planowaniem awaryjnym: plan awaryjny, szkolenie z zakresu planowania awaryjnego, testowanie planu awaryjnego, tworzenie kopii zapasowych systemu oraz odzyskiwanie i odtwarzanie systemu.

Organizacje: (I) opracowują, utrzymują i skutecznie wdrażają plany reagowania na sytuacje kryzysowe, (II) tworzą kopie zapasowe operacji oraz (III) nadzorują odtwarzanie systemów organizacji po katastrofie, aby zapewnić dostępność krytycznych zasobów informatycznych i ciągłość operacji w sytuacjach kryzysowych.

10.7 Identyfikacja i uwierzytelnianie (*Identification and Authentication – IA*)

W przypadku większości systemów identyfikacja i uwierzytelnianie są często pierwszą linią obrony. Identyfikacja to sposób weryfikowania tożsamości użytkownika, procesu lub urządzenia, zazwyczaj będący warunkiem wstępnym przyznania dostępu do zasobów w systemie. Identyfikacja i uwierzytelnianie to środek techniczny, który uniemożliwia nieupoważnionym osobom lub procesom wejście do systemu.

Identyfikacja i uwierzytelnianie to również krytyczny element bezpieczeństwa informacji, ponieważ jest podstawą większości rodzajów kontroli dostępu i ustalania odpowiedzialności użytkowników. Kontrola dostępu wymaga najczęściej, aby system był w stanie zidentyfikować i rozróżnić użytkowników. Na przykład kontrola dostępu jest często oparta na zasadzie minimalnych uprawnień, zgodnie z którą użytkownikom przyznaje się tylko taki dostęp, jaki jest niezbędny do wykonywania ich obowiązków. Rozliczalność użytkowników wymaga powiązania działań w systemie z konkretnymi osobami, a zatem wymaga, aby system identyfikował użytkowników.

Systemy rozpoznają osoby na podstawie otrzymanych danych uwierzytelniających. Uwierzytelnianie wiąże się z kilkoma wyzwaniami – koniecznością gromadzenia danych uwierzytelniających, bezpiecznego przekazywania tych danych oraz sprawdzania, czy osoba, która została pierwotnie uwierzytelniona, jest nadal osobą korzystającą z systemu. Na przykład, użytkownik może odejść od terminala nie wylogowując się, a inna osoba może zacząć go używać.

Istnieją cztery sposoby potwierdzania tożsamości użytkownika, które mogą być stosowane pojedynczo lub w połączeniu. Tożsamość użytkownika może być uwierzytelniona na podstawie:

- informacji, którą dana osoba zna – np. hasła lub osobistego numeru identyfikacyjnego (*ang. Personal Identification Number – PIN*);
- czegoś, co dana osoba posiada (tokena) – np. karty bankomatowej lub karty inteligentnej;
- czegoś, czym dana osoba jest (biometria statyczna) – np. odcisk palca, siatkówka oka, twarz;
- czegoś, co dana osoba robi (biometria dynamiczna) – np. wzorzec głosu, pismo odręczne, rytm pisania na klawiaturze.

Choć może się wydawać, że każda z tych pojedynczych metod może umożliwiać skuteczne uwierzytelnianie, z każdą z nich wiążą się pewne problemy. Jeśli dana osoba chce podszyć się pod kogoś innego w systemie, może odgadnąć lub poznać hasło tego użytkownika albo ukraść lub sfabrykować jego tokeny. Każda z metod ma również wady dla uprawnionych użytkowników i administratorów systemu – użytkownicy zapominają haseł i gubią tokeny, a administratorzy są obciążeni koniecznością ewidencjonowania danych identyfikacyjnych i autoryzacyjnych oraz tokenów. Również z systemami biometrycznymi wiążą się istotne problemy techniczne, dotyczące akceptacji przez użytkowników oraz kosztów.

Przykłady środków bezpieczeństwa związanych z identyfikacją i uwierzytelnianiem: identyfikacja i uwierzytelnianie urządzenia, zarządzanie identyfikatorami, zarządzanie tokenami uwierzytelniającymi, informacje zwrotne dotyczące tokenów uwierzytelniających oraz ponowne uwierzytelnianie.

Organizacje: (I) identyfikują użytkowników systemu, procesy działające w imieniu użytkowników lub urządzenia oraz (II) uwierzytelniają lub weryfikują tożsamość tych użytkowników, procesów lub urządzeń, jako warunek wstępny umożliwienia dostępu do systemów organizacji.

10.8 Indywidualne uczestnictwo (*Individual Participation – IP*)

Zaangażowanie osób, których informacje są przetwarzane przez system, jest ważnym aspektem ochrony prywatności i opracowywania godnych zaufania systemów. Działanie systemu może mieć istotny wpływ na jakość życia ludzi i ich zdolność do bycia

autonomicznymi jednostkami. Ich skuteczne zaangażowanie może pomóc złagodzić to ryzyko i zapobiec wielu problemom. Na przykład osoby fizyczne mogą czuć się nadzorowane przez system, co może wywołać efekt zniechęcenia do ich zwykłych zachowań lub sprawić, że zmienią swoje interakcje z systemem w nieoczekiwany sposób. Mogą mieć poczucie, że informacje zostały przywłaszczone albo wykorzystane dla zysku lub korzyści organizacji bez ich zgody lub wystarczającej korzyści finansowej dla nich. Wykluczenie z dostępu do informacji może wpłynąć na jakość danych, co może prowadzić do podejmowania niekorzystnych decyzji dotyczących użytkowników, w tym niewłaściwych ograniczeń w dostępie do produktów, usług lub innych rodzajów dyskryminacji.

Środki bezpieczeństwa związane z indywidualnym uczestnictwem dotyczą interakcji użytkownika z systemem i mają umożliwić mu przyjęcie wiarygodnych założeń na temat tego, w jaki sposób system przetwarza informacje o nim. Ponadto środki te tworzą punkty kontaktowe, dzięki którym użytkownicy mogą lepiej poznać system i zaangażować się w zarządzanie swoimi informacjami. Użytkownicy, którzy mają możliwość uczestniczenia w podejmowaniu decyzji dotyczących przetwarzania informacji o nich, mogą mieć większe zaufanie do systemu i angażować się w jego obsługę w konstruktywny sposób. Ponadto umożliwienie użytkownikom poprawiania niedokładnych informacji może poprawić funkcjonowanie systemu i uchronić ich od problemów wynikających z działań systemu opartych na przetwarzaniu niedokładnych informacji. Dzięki środkom bezpieczeństwa związanym z indywidualnym uczestnictwem organizacje powiadamiają osoby fizyczne o przetwarzaniu ich danych osobowych na bieżąco. W stosownych przypadkach, dzięki opcjom dostępu do informacji i wyrażenia zgody, środki te angażują również osoby fizyczne jako aktywnych uczestników procesu decyzyjnego dotyczącego ich danych osobowych oraz zapewniają im możliwość poprawienia lub zmiany tych danych za pomocą odpowiednich mechanizmów dochodzenia roszczeń.

Przykłady środków bezpieczeństwa związanych z indywidualnym uczestnictwem: wyrażanie zgody, dochodzenie roszczeń, zawiadomienie o prywatności, oświadczenia dotyczące ustawy o ochronie danych osobowych oraz indywidualny dostęp.

Organizacje: (I) proszą o zgodę na przetwarzanie danych osobowych; (II) zapewniają dostęp do danych osobowych i możliwości dla osób fizycznych dochodzenia roszczeń mających na celu zmianę lub poprawienie danych osobowych; oraz (III) informują osoby fizyczne o przetwarzaniu danych osobowych.

10.9 Reagowanie na incydenty (*Incident Response – IR*)

Systemy są narażone na szeroki zakres zdarzeń powodujących zagrożenia, od uszkodzenia plików danych, poprzez wirusy, aż po klęski żywiołowe. Podatność na niektóre z nich można zmniejszyć poprzez wprowadzenie odpowiednich standardowych procedur operacyjnych, które będą stosowane w przypadku wystąpienia incydentu. Na przykład skutki często występujących zdarzeń, takich jak omyłkowe usunięcie pliku, można zazwyczaj naprawić poprzez przywrócenie pliku z kopii zapasowej. Poważniejsze zdarzenia powodujące zagrożenia, takie jak awarie spowodowane klęskami żywiołowymi, są zwykle uwzględniane w planie awaryjnym organizacji.

Mogą one być również wynikiem działania wirusa, innego złośliwego kodu lub intruza w systemie (zarówno z organizacji, jak i spoza niej). Bardziej ogólnie mogą się odnosić do tych zdarzeń, które bez reakcji wyszkolonego personelu mogłyby spowodować poważne szkody. Przykładem zdarzenia powodującego zagrożenie i wymagającego natychmiastowej reakcji wyspecjalizowanego personelu może być atak na organizację metodą DoS. Taki rodzaj ataku wymaga szybkich działań ze strony zespołu reagowania na incydenty w celu zmniejszenia wpływu, jaki będzie on miał na organizację. Definicja zdarzenia powodującego zagrożenie jest dość elastyczna i może się różnić w zależności od organizacji i środowiska obliczeniowego.

Zagrożenia dla systemów i sieci ze strony hackerów i złośliwych kodów są dobrze znane, jednak ich występowanie pozostaje nieprzewidywalne. Incydenty związane z bezpieczeństwem w większych sieciach (np. w Internecie), takie jak włamania i zakłócenia usług, zaszkodziły możliwościom obliczeniowym wielu organizacji. Przy pierwszych konfrontacjach z takimi incydentami większość organizacji reaguje w sposób doraźny. Jednak powtarzanie się podobnych zdarzeń może sprawić, że opracowanie standardowej zdolności do szybkiego wykrywania i reagowania na nie

będzie znacznie bardziej opłacalne. Jest to szczególnie ważne, ponieważ incydenty często „rozprzestrzeniają się", jeśli zostaną pozostawione bez reakcji, powiększając skalę szkód i negatywnie wpływając na organizację.

Obsługa incydentów jest ściśle związana z planowaniem awaryjnym. Zdolność do obsługi incydentów może być postrzegana jako element planowania awaryjnego, ponieważ pozwala na szybkie i skuteczne reagowanie na zakłócenia w normalnym działaniu. Ogólnie rzecz biorąc, planowanie awaryjne dotyczy zdarzeń, które mogą potencjalnie zakłócić działanie systemu. Obsługa incydentów może być uważana za tę część planowania awaryjnego, która dotyczy wyłącznie reagowania na złośliwe zagrożenia techniczne. Więcej informacji na temat obsługi incydentów można znaleźć w publikacji NSC 800-61.

Przykłady środków bezpieczeństwa związanych z reagowaniem na incydenty: szkolenie w zakresie reagowania na incydenty, testowanie reakcji na incydenty, obsługa incydentów, monitorowanie incydentów i raportowanie o incydentach.

Organizacje: (I) tworzą w swoich systemach operacyjną zdolność do obsługi incydentów, która obejmuje odpowiednie przygotowanie, wykrywanie, analizę, ograniczanie, odzyskiwanie oraz działania związane z reagowaniem na potrzeby użytkowników; oraz (II) monitorują, dokumentują i zgłaszają incydenty odpowiednim Zespołom Reagowania na Incydenty Bezpieczeństwa Komputerowego (*ang. Computer Security Incident Response Team - CSIRT*)[28].

10.10 Utrzymanie i wsparcie (*Maintenance – MA*)

Aby utrzymać systemy w dobrym stanie technicznym oraz zminimalizować ryzyko związane z awariami sprzętu i oprogramowania, konieczne jest, aby organizacje opracowały procedury utrzymania i wsparcia swoich systemów. Istnieje wiele różnych sposobów, w jaki organizacja może spełnić wymagania dotyczące utrzymania i wsparcia.

[28] Ustawa o krajowym systemie cyberbezpieczeństwa ustanowiła trzy Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego: CSIRT NASK, CSIRT GOV oraz CSIRT MON. Każdy z CSIRT odpowiedzialny jest za koordynację incydentów zgłaszanych przez przyporządkowane zgodnie z ustawą podmioty.

Kontrolowane utrzymanie systemu to takie utrzymanie, które jest zaplanowane i przeprowadzane zgodnie ze specyfikacjami producenta. Utrzymanie przeprowadzane poza harmonogramem, zwane utrzymaniem korekcyjnym, ma miejsce, gdy system ulegnie awarii lub wygeneruje błąd, który musi zostać usunięty, aby przywrócić go do stanu używalności. Utrzymanie może być przeprowadzane lokalnie lub zdalnie. Utrzymanie zdalne to każda konserwacja lub diagnostyka wykonywana przez osoby komunikujące się za pośrednictwem sieci wewnętrznej lub zewnętrznej (np. przez Internet).

Przykłady środków bezpieczeństwa związanych z utrzymaniem: kontrolowane utrzymanie, narzędzia do utrzymania, utrzymanie zdalne, personel techniczny i planowane wsparcie.

Organizacje: (I) przeprowadzają okresowe i terminowe działania związane z utrzymaniem swoich systemów; oraz (II) zapewniają skuteczne środki bezpieczeństwa dotyczące narzędzi, technik, mechanizmów i personelu wykorzystywanego do utrzymania systemu.

10.11 Ochrona nośników danych (*Media Protection – MP*)

Ochrona nośników danych to środek bezpieczeństwa służący do ochrony nośników systemowych, które można podzielić na cyfrowe i niecyfrowe. Przykłady nośników cyfrowych: dyskietki, taśmy magnetyczne, zewnętrzne/wymienne dyski twarde, dyski flash, płyty CD i DVD. Przykładami nośników innych niż cyfrowe są papier i mikrofilm.

Ochrona nośników może ograniczać dostęp i udostępniać nośniki tylko upoważnionemu personelowi, stosować etykiety bezpieczeństwa do informacji wrażliwych i zapewniać instrukcje dotyczące sposobu usuwania informacji z nośników, tak aby nie można było ich odzyskać lub odtworzyć. Ochrona nośników obejmuje również fizyczną kontrolę nośników systemowych i zapewnienie rozliczalności, jak również zakaz wnoszenia do obszarów o ograniczonym dostępie lub wynoszenia z nich urządzeń mobilnych zdolnych do przechowywania i przenoszenia informacji.

Przykłady środków bezpieczeństwa związanych z ochroną nośników: dostęp do nośników, oznaczanie nośników, przechowywanie nośników, transport nośników i sanityzacja nośników.

Organizacje: (I) chronią nośniki danych, zarówno papierowe, jak i cyfrowe; (II) ograniczają dostęp do informacji na nośnikach systemowych do uprawnionych użytkowników; oraz (III) poddają sanityzacji lub niszczą nośniki danych przed utylizacją lub dopuszczeniem do ponownego użycia.

10.12 Autoryzacja prywatności (*Privacy Authorization – PA*)

Aby lepiej chronić prywatność osób fizycznych i ograniczyć problemy wynikające z przetwarzania przez system ich informacji, organizacje powinny mieć jasne uzasadnienie dla gromadzenia, wykorzystywania, utrzymywania i udostępniania danych osobowych (*ang. Personally Identifiable Information – PII*). Gromadzenie i utrzymywanie zbyt dużych ilości informacji może stwarzać potencjalne podatności na zagrożenia albo umożliwiać wewnętrzne nadużycia lub rozszerzone zastosowania, które przekraczają granice prywatności. Osoby fizyczne mogłyby zostać napiętnowane w wyniku ujawnienia informacji o nich lub ucierpieć z powodu kradzieży tożsamości. Podmioty zewnętrzne, którym udostępniane są informacje, mogą nie brać pod uwagę celu lub kontekstu, w jakim były one gromadzone, i wykorzystywać je w sposób sprzeczny z interesami dotyczącymi prywatności osób fizycznych. W rezultacie osoby fizyczne mogą stracić zaufanie do danych systemów, co może doprowadzić do rezygnacji lub zagrożenia przyjęcia nowych technologii, nawet tych mających na celu poprawę dostępu do usług publicznych.

Organizacje mogą być zmuszone do przestrzegania przepisów ustawowych lub wykonawczych, a także wewnętrznych polityk dotyczących przetwarzania danych osobowych. Środki bezpieczeństwa związane z ochroną prywatności umożliwiają organizacji zapewnienie, że przetwarza ona dane osobowe tylko w sposób, do którego jest uprawniona, i tylko wtedy, gdy ma jasno określone cele. Zapewnienie to ułatwia organizacji spełnienie obowiązku przestrzegania odpowiednich polityk oraz minimalizuje potencjalne koszty niezgodności z nimi i ryzyko utraty reputacji. Dokumentowanie tych informacji pomaga również osobom fizycznym zrozumieć, w jaki sposób system przetwarza ich dane osobowe (PII).

Przykłady zabezpieczeń związanych z ochroną prywatności: upoważnienie do gromadzenia danych, określenie celu oraz udostępnianie informacji podmiotom zewnętrznym.

Organizacje: (I) określają podstawy prawne, które upoważniają je do gromadzenia, wykorzystywania, utrzymywania i udostępniania określonych danych osobowych; (II) określają w swoich powiadomieniach cele gromadzenia danych osobowych; oraz (III) zarządzają udostępnianiem danych osobowych podmiotom zewnętrznym.

10.13 Ochrona fizyczna i środowiskowa (*Physical and Environmental Protection – PE*)

Termin bezpieczeństwo fizyczne i środowiskowe odnosi się do środków podejmowanych w celu ochrony systemów, budynków i związanej z nimi infrastruktury towarzyszącej przed zagrożeniami związanymi z ich środowiskiem fizycznym. Środki fizyczne i środowiskowe dotyczą trzech szeroko rozumianych obszarów:

1. Obiekt fizyczny to zazwyczaj budynek, inna struktura lub pojazd, w którym znajdują się elementy systemu i sieci. Systemy można podzielić na podstawie miejsca ich działania na stacjonarne, mobilne lub przenośne. Systemy stacjonarne są montowane w konstrukcjach w stałych miejscach lokalizacji. Systemy mobilne są instalowane w pojazdach, które pełnią funkcję konstrukcji, ale nie znajdują się w stałej lokalizacji. Systemy przenośne mogą być eksploatowane w wielu różnych miejscach, w tym w budynkach, pojazdach lub na otwartej przestrzeni. Fizyczne cechy tych struktur i pojazdów determinują poziom zagrożenia ze strony czynników fizycznych, takich jak pożar, przeciekający dach czy nieautoryzowany dostęp.
2. Ogólna geograficzna lokalizacja operacyjna obiektu determinuje charakterystykę zagrożeń naturalnych, do których zaliczają się trzęsienia ziemi i powodzie; zagrożeń spowodowanych przez człowieka, takich jak: włamania, rozruchy społeczne lub przechwytywanie transmisji i emisji ujawniającej; oraz szkodliwych działań w pobliżu, w tym wycieków toksycznych substancji chemicznych, eksplozji, pożarów i zakłóceń elektromagnetycznych pochodzących z emiterów (np. radarów).

3. Infrastruktura pomocnicza to usługi (wykonywane zarówno przez urządzenia lub oprogramowanie, jak i przez ludzi), które podtrzymują działanie systemu. Działanie systemu zależy zazwyczaj od infrastruktury wspomagającej, np. od energii elektrycznej, ogrzewania i klimatyzacji oraz telekomunikacji. Awaria lub niewłaściwe działanie takiej infrastruktury może przerwać działanie systemu i spowodować fizyczne uszkodzenie sprzętu lub przechowywanych danych.

Przykłady fizycznych i środowiskowych środków bezpieczeństwa: upoważnienia do dostępu fizycznego, kontrola dostępu fizycznego, monitorowanie dostępu fizycznego, wyłączanie awaryjne, zasilanie awaryjne, oświetlenie awaryjne, alternatywne miejsce pracy, wyciek informacji oraz monitorowanie i śledzenie aktywów.

Organizacje: (I) ograniczają fizyczny dostęp do systemów, urządzeń i właściwych środowisk operacyjnych do uprawnionych osób; (II) chronią fizyczny obiekt i infrastrukturę wspierającą systemy; (III) dostarczają narzędzia pomocnicze dla systemów; (IV) chronią systemy przed zagrożeniami środowiskowymi; oraz (V) zapewniają odpowiednie środowiskowe środki bezpieczeństwa w obiektach zawierających systemy.

10.14 Planowanie (*Planning – PL*)

Systemy coraz częściej pełnią strategiczną rolę w organizacji. Wspierają organizację w prowadzeniu codziennej działalności i ułatwiają podejmowanie decyzji. Dzięki odpowiedniemu planowaniu systemy mogą zapewnić poziom bezpieczeństwa współmierny do ryzyka związanego z ich działaniem, poprawić produktywność i wydajność oraz udostępnić nowe sposoby zarządzania i organizowania. Planowanie dotyczące systemów jest kluczowe w tworzeniu i realizacji celów organizacji w zakresie bezpieczeństwa informacji.

Plan bezpieczeństwa systemu (*ang. System Security Plan – SSP*)[29] jest opracowywany w celu przedstawienia przeglądu wymagań bezpieczeństwa systemu oraz sposobu, w jaki środki bezpieczeństwa i zabezpieczenia rozszerzone spełniają te wymagania. Samo wdrożenie

[29] Więcej informacji na temat opracowania planu bezpieczeństwa systemu można znaleźć w publikacji NSC 800-18.

środków bezpieczeństwa nie gwarantuje ogólnej ochrony systemu. Organizacje muszą również opracować, udokumentować i upowszechnić sposób wdrażania tych środków, zasady opisujące odpowiedzialność użytkowników oraz sposób eksploatacji systemu przez organizację w kontekście bezpieczeństwa informacji.

Przykłady środków bezpieczeństwa związanych z planowaniem: plan bezpieczeństwa systemu, zasady postępowania, koncepcja bezpieczeństwa operacji, architektura bezpieczeństwa informacji oraz centralne zarządzanie.

Organizacje: opracowują, dokumentują, okresowo aktualizują i wdrażają plany bezpieczeństwa dla swoich systemów, które opisują istniejące lub planowane środki bezpieczeństwa dla systemu, a także zasady zachowania osób mających dostęp do systemów.

10.15 Programy zarządzania (*Program Management – PM*)

Systemy i przetwarzane przez nie informacje mają kluczowe znaczenie dla zdolności wielu organizacji do realizacji ich misji i funkcji biznesowych. Nie bez przyczyny kadra kierownicza traktuje bezpieczeństwo systemu jako zagadnienie związane z zarządzaniem i stara się chronić zasoby informatyczne swojej organizacji tak, jak każdy inny cenny składnik majątku. Aby robić to skutecznie, konieczne jest opracowanie kompleksowego podejścia do zarządzania.

Wiele programów bezpieczeństwa, rozproszonych po całej organizacji, zawiera różne elementy pełniące różne funkcje. Takie podejście ma swoje zalety, jednak dystrybucja funkcji bezpieczeństwa dotyczących systemu w wielu organizacjach jest przypadkowa, zwykle oparta na ich historii (tj. zależy od tego, kto w danej organizacji był dostępny do wykonania danego zadania, kiedy pojawiła się taka potrzeba). W idealnej sytuacji podział funkcji bezpieczeństwa dotyczących systemu jest wynikiem planowej i zintegrowanej filozofii zarządzania.

Zarządzanie bezpieczeństwem systemu na wielu poziomach ma swoje zalety. Każdy poziom wnosi wkład w realizację ogólnego programu bezpieczeństwa systemu, dysponując różnymi rodzajami wiedzy, uprawnień i zasobów. Ogólnie rzecz biorąc, personel wyższego szczebla (np. na poziomie siedziby głównej czy jednostek w danej organizacji) lepiej rozumieją organizację jako całość i mają większe uprawnienia.

Z drugiej strony, personel niższego szczebla (np. na poziomie obiektu systemowego i poziomach użytkowych) są lepiej zaznajomieni z konkretnymi wymaganiami technicznymi i proceduralnymi oraz problemami systemów i użytkowników. Poziomy zarządzania programem bezpieczeństwa systemu wzajemnie się uzupełniają i dzięki temu poprawiają swoją skuteczność.

Przykłady środków bezpieczeństwa związanych z programem zarządzania: plan programu bezpieczeństwa informacji, zasoby bezpieczeństwa informacji, plan działania i proces realizacji kamieni milowych, inwentaryzacja systemu, architektura korporacyjna, strategia zarządzania ryzykiem, program dotyczący zagrożeń wewnętrznych oraz program zwiększania świadomości zagrożeń.

10.16 Bezpieczeństwo osobowe (*Personnel Security – PS*)

Użytkownicy odgrywają istotną rolę w ochronie systemu, gdyż wiele ważnych zagadnień z zakresu bezpieczeństwa informacji dotyczy użytkowników, projektantów, wdrożeniowców i menadżerów. Sposób, w jaki osoby te wchodzą w interakcje z systemem oraz poziom dostępu, jaki jest im potrzebny do wykonywania pracy, również może wpływać na stan bezpieczeństwa systemu. Niemal żaden system nie może być zabezpieczony bez właściwego uwzględnienia aspektów bezpieczeństwa osób.

Bezpieczeństwo osobowe ma na celu zminimalizowanie ryzyka, jakie stwarza personel (stały, tymczasowy lub wykonawcy/podwykonawcy) dla aktywów organizacji poprzez złośliwe wykorzystanie lub nadużycie legalnego dostępu do zasobów organizacji. Działania takich pracowników mogą mieć negatywny wpływ na status i reputację organizacji. Pracownicy mogą mieć dostęp do niezwykle wrażliwych, poufnych lub zastrzeżonych informacji, których ujawnienie może zniszczyć reputację organizacji lub doprowadzić do ogromnych strat finansowych. Dlatego organizacje muszą zachować czujność podczas rekrutacji i zatrudniania nowych pracowników, a także w przypadku, gdy pracownik przenosi się do innej organizacji lub zostaje zwolniony. Newralgiczny charakter i wartość majątku organizacji wymaga zastosowania gruntownych środków bezpieczeństwa osób.

Przykłady środków bezpieczeństwa osobowego: weryfikacja personelu, zwalnianie personelu, przenoszenie personelu, umowy dostępu i sankcje.

Organizacje: (I) zapewniają, że osoby zajmujące odpowiedzialne stanowiska w organizacjach (w tym zewnętrzni dostawcy usług) są godne zaufania i spełniają ustalone kryteria bezpieczeństwa dla tych stanowisk; (II) zapewniają, że informacje i systemy organizacyjne są chronione podczas i po działaniach dotyczących personelu, takich jak zwolnienia i przeniesienia; oraz (III) stosują formalne sankcje wobec pracowników, którzy nie przestrzegają zasad i polityk bezpieczeństwa organizacji.

10.17 Szacowanie ryzyka (*Risk Assessment – RA*)

Organizacje polegają na technologii informacyjnej i związanych z nią systemach, aby skutecznie realizować swoje misje. Rosnąca liczba produktów informatycznych wykorzystywanych w różnych organizacjach i branżach może przynieść wiele korzyści, jednak w niektórych przypadkach mogą one również wprowadzać poważne zagrożenia i negatywnie wpływać na systemy organizacji poprzez wykorzystanie zarówno znanych, jak i nieznanych podatności na zagrożenia. Wykorzystanie podatności na zagrożenia w systemach organizacji może zagrozić poufności, integralności lub dostępności informacji przetwarzanych, przechowywanych lub przesyłanych przez te systemy.

Szacowanie ryzyka jest jednym z czterech komponentów zarządzania ryzykiem opisanych w publikacji NSC 800-39. W ramach szacowania ryzyka określa się zagrożenia dla działalności organizacji, jej aktywów, osób, innych organizacji i państwa, które mogą wynikać z działania systemu, oraz nadaje się im priorytety. Szacowanie ryzyka, które może być przeprowadzone na wszystkich trzech poziomach w hierarchii zarządzania ryzykiem, zapewnia decydentom informacje i wspiera reakcje na ryzyko poprzez identyfikację: (I) istotnych zagrożeń dla organizacji lub zagrożeń kierowanych za pośrednictwem organizacji przeciwko innym organizacjom; (II) podatności organizacji na zagrożenia wewnętrzne i zewnętrzne; (III) wpływu (tj. szkody) dla organizacji, który może wystąpić ze względu na wykorzystanie podatności na zagrożenia; oraz (IV) prawdopodobieństwa wystąpienia szkody. Więcej informacji na temat szacowania ryzyka można znaleźć w publikacji NSC 800-30.

Przykłady środków bezpieczeństwa związanych z szacowaniem ryzyka: kategoryzacja bezpieczeństwa, szacowanie ryzyka, skanowanie podatności, przegląd technicznych zabezpieczeń do ochrony przed podglądem i podsłuchem.

Organizacje: okresowo oceniają ryzyko swojej działalności (np. misji, funkcji, wizerunku, reputacji), aktywów organizacyjnych i osób, które może wynikać z działania ich systemów i związanego z tym przetwarzania, przechowywania lub przekazywania informacji organizacji.

10.18 Pozyskiwanie systemów i usług (*System and Services Acquisition – SA*)

Podobnie jak w przypadku innych elementów systemów do przetwarzania informacji, ich zabezpieczenia są najbardziej efektywne i skuteczne, jeśli są zaplanowane i zarządzane w całym cyklu życia systemu, od wstępnego planowania, poprzez projektowanie, wdrażanie, eksploatację i usuwanie. Wiele zdarzeń i analiz istotnych dla bezpieczeństwa ma miejsce podczas eksploatacji systemu, która rozpoczyna się wraz z nabyciem przez organizację niezbędnych narzędzi i usług. Skuteczna integracja wymagań bezpieczeństwa z architekturą korporacyjną pomaga również zapewnić, aby ważne kwestie związane z bezpieczeństwem były uwzględniane na wczesnym etapie SDLC oraz zagwarantować ich bezpośrednie powiązanie z misją organizacji lub procesami biznesowymi.

SSP można opracować na dowolnym etapie cyklu życia systemu. Jednak, aby zminimalizować koszty i zapobiec zakłóceniom w bieżącej działalności, zalecanym podejściem jest wprowadzenie planu na początku cyklu życia systemu. Dodawanie zabezpieczeń do systemu jest znacznie droższym rozwiązaniem niż uwzględnienie ich na samym początku. Ważne jest, aby wymagania dotyczące bezpieczeństwa nadążały za zmianami w środowisku informatycznym, technologii i personelu.

Przykłady środków bezpieczeństwa związanych z nabywaniem systemów i usług: alokacja zasobów, proces nabywania, dokumentacja systemu, ochrona łańcucha dostaw, wiarygodność, analiza krytyczności, szkolenia prowadzone przez deweloperów, autentyczność komponentów oraz kontrola deweloperów.

Organizacje: (I) przeznaczają wystarczające zasoby, aby odpowiednio chronić swoje systemy; (II) stosują procesy SDLC, które uwzględniają kwestie bezpieczeństwa informacji; (III) wprowadzają ograniczenia dotyczące użytkowania i instalacji oprogramowania; oraz (IV) dbają o to, aby dostawcy zewnętrzni stosowali odpowiednie środki bezpieczeństwa w celu ochrony informacji, aplikacji lub usług zlecanych innym podmiotom.

10.19 Ochrona systemów i sieci telekomunikacyjnych (*System and Communications Protection – SC*)

Środki ochrony systemu i komunikacji zapewniają szereg zabezpieczeń dla systemu. Niektóre środki bezpieczeństwa z tej grupy dotyczą poufności i integralności informacji w trakcie przechowywania i tranzytu. Mogą one zapewnić ochronę poufności i integralności metodami fizycznymi lub logicznymi. Na przykład organizacja może zapewnić ochronę fizyczną, wydzielając pewne funkcje na oddzielne serwery, z których każdy ma własny zestaw adresów IP.

Organizacje mogą lepiej zabezpieczyć swoje informacje poprzez oddzielenie funkcji dla użytkowników od funkcji zarządzania systemem. Tego typu ochrona uniemożliwia dostęp do funkcji zarządzania systemem przez interfejs dla nieuprzywilejowanych użytkowników. Ochrona systemu i sieci telekomunikacyjnych wyznacza również granice, które ograniczają dostęp do publicznie dostępnych informacji w ramach systemu. Wykorzystując zabezpieczenia brzegowe, organizacja może monitorować i kontrolować komunikację na granicach zewnętrznych oraz na kluczowych granicach wewnętrznych systemu.

Przykłady środków bezpieczeństwa związanych z ochroną systemu i sieci telekomunikacyjnych: partycjonowanie aplikacji, ochrona przed atakami DoS, ochrona brzegu systemu, zaufana ścieżka, kod mobilny, autentyczność sesji, cienkie węzły (*ang. thin nodes*), „honeypoty", poufność i integralność transmisji, bezpieczeństwo operacji, ochrona informacji w trakcie przechowywania i tranzytu oraz ograniczenia użytkowania.

Organizacje: (I) monitorują, kontrolują i chronią komunikację w organizacji (tj. informacje przesyłane lub odbierane przez ich systemy) na granicach zewnętrznych

i kluczowych granicach wewnętrznych systemów; oraz (II) stosują projekty architektoniczne, techniki rozwoju oprogramowania i zasady inżynierii systemów, które sprzyjają skutecznemu zabezpieczeniu informacji w ramach ich systemów.

10.20 Integralność systemu i informacji (*System and Information Integrity – SI*)

Integralność jest definiowana jako zabezpieczenie przed niewłaściwą modyfikacją lub zniszczeniem informacji oraz zapewnienie jej niezaprzeczalności i autentyczności. Jest to zapewnienie, że dane mogą być dostępne lub modyfikowane tylko przez upoważniony personel. Integralność systemu i informacji daje pewność, że informacje, do których istnieje dostęp, nie zostały naruszone lub uszkodzone przez błąd w systemie.

Przykłady środków bezpieczeństwa związanych z integralnością systemu i informacji: usuwanie usterek, ochrona przed złośliwymi kodami, weryfikacja funkcji bezpieczeństwa, sprawdzanie poprawności danych wejściowych, obsługa błędów, nietrwałość danych[30] i ochrona pamięci.

Organizacje: (I) identyfikują, zgłaszają i korygują wady informacji i systemów w odpowiednim czasie; (II) zapewniają ochronę przed złośliwymi kodami w odpowiednich lokalizacjach w swoich systemach; oraz (III) monitorują alerty i porady dotyczące bezpieczeństwa systemu i odpowiednio na nie reagują.

[30] Dane, które nie są dostępne po całkowitym zamknięciu aplikacji. Możemy powiedzieć, że dane non - persistence oznaczają dane zmienne, które są dostępne podczas wykonywania aplikacji.

ZAŁĄCZNIK A - REFERENCJE

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[31]	
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 800-18	Przewodnik do opracowywania planów bezpieczeństwa systemów informacyjnych w podmiotach publicznych – na podstawie NIST SP 800-18
NSC 800-30	Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne – na podstawie NIST SP 800-30
NSC 800-34	Poradnik planowania awaryjnego – na podstawie NIST SP 800-34
NSC 800-37	Ramy zarządzania ryzykiem w organizacjach i systemach 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

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

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[31]	
NSC 800-53B	Zabezpieczenia bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B
NSC 800-53 MAP	Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 Patrz: SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)
NSC 800-60	Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informacyjnego – na podstawie NIST SP 800-60
NSC 800-61	Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego – na podstawie NIST SP 800-61
NSC 800-82	Przewodnik w zakresie bezpieczeństwa systemów sterowania przemysłowego– na podstawie NIST SP 800-82

PUBLIKACJE ANGLOJĘZYCZNE[32]	
[E-Gov Act]	E-Government Act of 2002, Public Law 107-347, 116 Stat 2899. http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf
[Clinger-Cohen Act]	Clinger-Cohen Act, Public Law 107-217, 116 Stat 1234. https://www.gsa.gov/graphics/staffoffices/Clinger.htm
[FISMA$_{2002}$]	Federal Information Security Management Act of 2002, Pub. L. 107-347 (Title III), 116 Stat. 2946. https://www.gpo.gov/fdsys/pkg/CHRG-107hhrg86343/pdf/CHRG-107hhrg86343.pdf
[FISMA$_{2014}$]	Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073. http://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf
[OMB Circular A-130]	Office of Management and Budget (OMB), *Managing Information as a Strategic Resource*, OMB Memorandum Circular A-130, Revised July 28, 2016. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf
[FIPS140-2]	U.S. Department of Commerce. *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards (FIPS) Publication 140-2, May 25, 2001 (with Change Notices through December 3, 2002), 69pp. https://doi.org/10.6028/NIST.FIPS.140-2
[FIPS180-4]	U.S. Department of Commerce. *Secure Hash Standard (SHS)*, Federal Information Processing Standards (FIPS) Publication 180-4, August 2015, 36pp. https://doi.org/10.6028/NIST.FIPS.180-4

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

PUBLIKACJE ANGLOJĘZYCZNE[32]	
[FIPS186-4]	U.S. Department of Commerce. *Digital Signature Standard (DSS)*, Federal Information Processing Standards (FIPS) Publication 186-4, July 2013, 130pp. https://doi.org/10.6028/NIST.FIPS.186-4
[FIPS 197]	U.S. Department of Commerce. *Advanced Encryption Standard*, Federal Information Processing Standards (FIPS) Publication 197, November 2001, 51pp. https://doi.org/10.6028/NIST.FIPS.197
[FIPS199]	U.S. Department of Commerce. *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards (FIPS) Publication 199, February 2004, 13pp. https://doi.org/10.6028/NIST.FIPS.199
[FIPS200]	U.S. Department of Commerce. *Minimum Security Requirements for Federal Information and Information Systems*, Federal Information Processing Standards (FIPS) Publication 200, March 2006, 17pp. https://doi.org/10.6028/NIST.FIPS.200
[FIPS 202]	U.S. Department of Commerce. *SHA-3: Permutation-Based Hash and Extendable-Output Functions*, Federal Information Processing Standards (FIPS) Publication 202, August 2015, 37pp. https://doi.org/10.6028/NIST.FIPS.202
[NISTIR 7298]	Kissel, R., *Glossary of Key Information Security Terms*, NISTIR 7298 Revision 2, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2013, 222pp. https://doi.org/10.6028/NIST.IR.7298r2

PUBLIKACJE ANGLOJĘZYCZNE[32]	
[NISTIR 8062]	Brooks, S., Garcia, M., Lefkovitz, N., Lightman, S., Nadeau, E., *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, NISTIR 8062, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2017, 49pp. https://doi.org/10.6028/NIST.IR.8062
[SP800-18]	NIST Special Publication (SP) 800-18 Revision 1, *Guide for Developing Security Plans for Systems*, National Institute of Standards and Technology, Gaithersburg, Maryland, February 2006, 48pp. https://doi.org/10.6028/NIST.SP.800-18r1
[SP800-30]	NIST Special Publication (SP) 800-30 Revision 1, *Guide for Conducting Risk Assessments*, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2012, 95pp. https://doi.org/10.6028/NIST.SP.800-30r1
[SP800-32]	NIST Special Publication (SP) 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, National Institute of Standards and Technology, Gaithersburg, Maryland, February 2001, 54pp. https://doi.org/10.6028/NIST.SP.800-32
[SP800-34]	NIST Special Publication (SP) 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2010 (updated November 2010), 149pp. https://doi.org/10.6028/NIST.SP.800-34r1
[SP800-37]	NIST Special Publication (SP) 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Systems: A Security Life Cycle Approach*, National Institute of Standards and Technology, Gaithersburg, Maryland, February 2010 (updated June 2014), 102pp. https://doi.org/10.6028/NIST.SP.800-37r1

PUBLIKACJE ANGLOJĘZYCZNE[32]	
[SP800-39]	NIST Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, National Institute of Standards and Technology, Gaithersburg, Maryland, March 2011, 88pp. https://doi.org/10.6028/NIST.SP.800-39
[SP800-53]	NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Systems and Organizations*, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2013 (updated January 2015), 462pp. https://doi.org/10.6028/NIST.SP.800-53r4
[SP800-53A]	NIST Special Publication (SP) 800-53A Revision 4, *Assessing Security and Privacy Controls in Systems and Organizations*, National Institute of Standards and Technology, Gaithersburg, Maryland, December 2014, 487pp. https://doi.org/10.6028/NIST.SP.800-53Ar4
[SP800-57 PART 1]	NIST Special Publication (SP) 800-57 part 1 Revision 4, *Recommendation for Key Management, Part 1: General*, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2016, 160pp. https://doi.org/10.6028/NIST.SP.800-57pt1r4
[SP800-57 PART 2]	NIST Special Publication (SP) 800-57 part 2, *Recommendation for Key Management, Part 2: Best Practices for Key Management Organizations*, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2005, 79pp. https://doi.org/10.6028/NIST.SP.800-57p2

PUBLIKACJE ANGLOJĘZYCZNE[32]	
[SP800-57 PART 3]	NIST Special Publication (SP) 800-57 part 3 Revision 1, *Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance*, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2015, 102pp. https://doi.org/10.6028/NIST.SP.800-57Pt3r1
[SP800-60]	NIST Special Publication (SP) 800-60 volume 1 Revision 1, *Guide for Mapping Types of Information Systems to Security Categories*, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2008, 53pp. https://doi.org/10.6028/NIST.SP.800-60v1r1
[SP800-61]	NIST Special Publication (SP) 800-61 Revision 2, *Computer Security Incident Handling Guide*, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2012, 79pp. https://doi.org/10.6028/NIST.SP.800-61r2
[SP800-82]	NIST Special Publication (SP) 800-82 Revision 2, *Guide to Industrial Control Systems (ICS) Security*, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2015, 247pp. https://doi.org/10.6028/NIST.SP.800-82r2
[SP800-95]	NIST Special Publication (SP) 800-95, *Guide to Secure Web Services*, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2007, 128pp. https://doi.org/10.6028/NIST.SP.800-95
[SP800-122]	NIST Special Publication (SP) 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2010, 59pp. https://doi.org/10.6028/NIST.SP.800-122

PUBLIKACJE ANGLOJĘZYCZNE[32]	
[SP800-128]	NIST Special Publication (SP) 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2011, 88pp. https://doi.org/10.6028/NIST.SP.800-128
[SP800-137]	NIST Special Publication (SP) 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2011, 80pp. https://doi.org/10.6028/NIST.SP.800-137
[SP800-147]	NIST Special Publication (SP) 800-147, *BIOS Protection Guidelines*, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2011, 26pp. https://doi.org/10.6028/NIST.SP.800-147
[SP800-152]	NIST Special Publication (SP) 800-152, *A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)*, National Institute of Standards and Technology, Gaithersburg, Maryland, October 2015, 147pp. https://doi.org/10.6028/NIST.SP.800-152
[SP800-155]	NIST Special Publication (SP) 800-155 (DRAFT), *BIOS Integrity Measurement Guidelines*, National Institute of Standards and Technology, Gaithersburg, Maryland, December 2011, 47pp. http://csrc.nist.gov/publications/drafts/800-155/draft-SP800-155_Dec2011.pdf
[SP800-160]	NIST Special Publication (SP) 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2016, 307pp. https://doi.org/10.6028/NIST.SP.800-160

PUBLIKACJE ANGLOJĘZYCZNE[32]	
[SP800-161]	NIST Special Publication (SP) 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2015, 282pp. https://doi.org/10.6028/NIST.SP.800-161
[SP800-162]	NIST Special Publication (SP) 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2014, 46pp. https://doi.org/10.6028/NIST.SP.800-162
[SP800-175A]	NIST Special Publication (SP) 800-175A, *Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies*, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2016, 44pp. https://doi.org/10.6028/NIST.SP.800-175A
[SP800-175B]	NIST Special Publication (SP) 800-175B, *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*, National Institute of Standards and Technology, Gaithersburg, Maryland, March 2016, 81pp. https://doi.org/10.6028/NIST.SP.800-175B

ZAŁĄCZNIK B - SŁOWNIK

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

Wybrane definicje pojęć[33] stosowanych w niniejszej publikacji zostały rozwinięte poniżej. [34]

Terminologia	Opis
Atak (*Attack*)	Każdy rodzaj złośliwej aktywności, która ma na celu gromadzenie, zakłócanie, uniemożliwianie dostępu, degradację lub niszczenie zasobów systemu informacyjnego lub samych informacji. Źródło: CNSSI-4009
Audyt (*Audit*)	Niezależny przegląd oraz badanie dokumentacji i działań w celu oceny adekwatności zabezpieczeń systemu oraz zapewnienia zgodności z ustalonymi politykami i procedurami operacyjnymi. Źródło: CNSSI-4009
Autoryzacja (*Authorization*)	Oficjalna decyzja kierownictwa wydana przez wyższego szczebla pracownika, zezwalająca na działanie systemu lub dziedziczonych zabezpieczeń wspólnych przez wyznaczone systemy organizacji i jednoznacznie akceptująca ryzyko dla działalności organizacji (w tym misji, funkcji, wizerunku i reputacji), aktywów organizacji, osób, innych organizacji i państwa w oparciu o wdrożenie uzgodnionego zestawu zabezpieczeń i środków ochrony prywatności. Nazywana również *upoważnieniem do działania*. Źródło: Okólnik OMB A-130

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

Terminologia	Opis
Bezpieczeństwo (*Security*)	Stan, który wynika z wprowadzenia i utrzymania środków ochronnych umożliwiających organizacji wykonywanie jego misji lub funkcji krytycznych pomimo ryzyka wynikającego z zagrożeń związanych z wykorzystaniem systemów informacyjnych. Środki ochronne mogą obejmować kombinację środków do odstraszania, unikania, zapobiegania, wykrywania, odzyskiwania i korygowania, które powinny stanowić część podejścia organizacji do zarządzania ryzykiem. Źródło: CNSSI-4009
Bezpieczeństwo informacji (*Information Security*)	Ochrona informacji i systemów informacyjnych przed nieuprawnionym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem działania, modyfikacją lub zniszczeniem w celu zapewnienia poufności, integralności i dostępności. Źródło: 44 U.S.C., pkt 3542
Bit (*Bit*)	Cyfra binarna mająca wartość 0 lub 1. Źródło: FIPS 180-4
Bomba logiczna (*Logic Bomb*)	Fragment kodu celowo umieszczony w systemie oprogramowania, który uruchamia złośliwą funkcję, gdy spełnione są określone warunki. Źródło: CNSSI-4009
Brama (*Gateway*)	System pośredni (interfejs, przekaźnik), który podłącza się do dwóch (lub większej liczby) sieci komputerowych pełniących podobne funkcje, ale różne implementacje, i który umożliwia jedno- lub dwukierunkową komunikację między sieciami. Źródło: IETF RFC 4949 wer. 2

Terminologia	Opis
Dane biometryczne (*Biometrics*)	Wymierna cecha fizyczna lub osobista cecha zachowania wykorzystywana do rozpoznania tożsamości lub weryfikacji podanej tożsamości osoby zgłaszającej. Przykładami danych biometrycznych są obrazy twarzy, odciski palców i wzory skanu tęczówki. Źródło: FIPS 201
Dostosowywanie (*Tailoring*)	Proces, w którym zestaw bazowych środków bezpieczeństwa jest modyfikowany na podstawie: (I) zastosowania wytycznych dotyczących zakresu zastosowania; (II) specyfikacji kompensacyjnych środków bezpieczeństwa, jeśli są konieczne; oraz (III) specyfikacji parametrów zdefiniowanych przez organizację w środkach bezpieczeństwa poprzez wyraźne deklaracje przypisania i wyboru. Źródło: NIST SP 800-37
Etykieta zabezpieczająca (*Security Label*)	Środki stosowane do powiązania zestawu atrybutów bezpieczeństwa z określonym obiektem informacyjnym jako część struktury danych dla tego obiektu. Źródło: NIST SP 800-53
Godna zaufania baza przetwarzania (*Trusted Computing Base*)	Całość mechanizmów ochrony w systemie komputerowym, w tym sprzęt, oprogramowanie i oprogramowanie układowe – kombinacja odpowiedzialna za egzekwowanie polityki bezpieczeństwa. Źródło: CNSSI-4009
Hacker (*Hacker*)	Użytkownik, który próbuje uzyskać lub uzyskuje dostęp do systemu informacyjnego w nieuprawniony sposób. Źródło: CNSSI-4009

Terminologia	Opis
Hasło (*Password*)	Ciąg znaków (liter, cyfr i innych symboli) używany do uwierzytelnienia tożsamości lub weryfikacji uprawnień dostępu. Źródło: FIPS 140-2
Incydent (*Incident*)	Zdarzenie, które faktycznie lub potencjalnie zagraża poufności, integralności lub dostępności systemu informacyjnego lub informacji przetwarzanych, przechowywanych lub przesyłanych przez system, albo które stanowi naruszenie lub bezpośrednie zagrożenie naruszenia polityki bezpieczeństwa, procedur bezpieczeństwa lub polityki dopuszczalnego użytkowania. Źródło: FIPS 200
Informacje (*Information*)	1. Fakty lub idee, które mogą być wyrażone (zakodowane) w postaci różnych form danych. 2. Wiedza (np. dane, instrukcje) na dowolnym nośniku lub w dowolnej formie, która może być przekazywana między jednostkami systemu. Źródło: IETF RFC 4949 wer. 2
Infrastruktura klucza publicznego (PKI) (*Public Key Infrastructure [PKI]*)	Struktura służąca do wydawania, utrzymywania i unieważniania certyfikatów klucza publicznego. Źródło: FIPS 186-4
Integralność (*Integrity*)	Zabezpieczenie przed niewłaściwą modyfikacją lub zniszczeniem informacji oraz zapewnienie jej niezaprzeczalności i autentyczności. Źródło: 44 U.S.C., pkt 3542
Integralność systemu (*System Integrity*)	Właściwość systemu, który wykonuje swoją zamierzoną funkcję w sposób niezakłócony, bez możliwości nieautoryzowanej manipulacji, zarówno celowej, jak i przypadkowej. Źródło: NIST SP 800-27

Terminologia	Opis
Inżynieria bezpieczeństwa (*Security Engineering*)	Interdyscyplinarne podejście i środki umożliwiające tworzenie bezpiecznych systemów. Koncentruje się na określeniu potrzeb klienta, wymagań dotyczących ochrony bezpieczeństwa oraz wymaganych funkcji we wczesnym etapie cyklu życia systemu, dokumentowaniu wymagań, a następnie przystąpieniu do projektowania, syntezy i walidacji systemu z uwzględnieniem całości problemu. Źródło: CNSSI-4009
Klucz (*Key*)	Parametr używany w połączeniu z algorytmem kryptograficznym, który określa jego działanie. Przykłady mające zastosowanie do niniejszego standardu obejmują: obliczanie podpisu cyfrowego na podstawie danych oraz weryfikację podpisu cyfrowego. Źródło: FIPS 186-4
Klucz prywatny (*Private Key*)	Klucz kryptograficzny, używany w algorytmie kryptograficznym z kluczem publicznym, który jest jednoznacznie powiązany z podmiotem i nie jest upubliczniany. Źródło: FIPS 140-2
Klucz publiczny (*Public Key*)	Klucz kryptograficzny, używany w algorytmie kryptograficznym z kluczem publicznym, który jest jednoznacznie powiązany z podmiotem i może być upubliczniany. Źródło: FIPS 140-2
Klucz tajny (Sekret) (*Secret Key*)	Klucz kryptograficzny, używany w algorytmie kryptograficznym z kluczem tajnym, który jest jednoznacznie powiązany z jednym lub większą liczbą podmiotów i nie powinien być upubliczniany. Źródło: FIPS 140-2

Terminologia	Opis
Kod złośliwy (*Malicious Code*)	Oprogramowanie lub oprogramowanie układowe służące do wykonania nieautoryzowanego procesu, który będzie miał negatywny wpływ na poufność, integralność lub dostępność systemu. Wirus, robak, koń trojański lub inna jednostka oparta na kodzie, która infekuje host. Oprogramowanie szpiegujące i niektóre formy programów typu adware również są przykładami złośliwych kodów. Źródło: NIST SP 800-53
Kontrola dostępu (*Access Control*)	Proces spełniania lub odrzucania określonych żądań dotyczących: 1) uzyskania i wykorzystania informacji oraz związanych z nimi usług przetwarzania informacji; oraz 2) wejścia do określonych obiektów fizycznych (np. budynków rządowych, obiektów wojskowych, wejść na przejścia graniczne). Źródło: FIPS 201-2
Koń trojański (*Trojan Horse*)	Program komputerowy, który wydaje się mieć użyteczną funkcję, ale ma również ukryte i potencjalnie złośliwe działanie, które polega na omijaniu mechanizmów bezpieczeństwa, czasami poprzez wykorzystanie legalnych uprawnień jednostki systemu, która wywołuje program. Źródło: CNSSI-4009
Kryptografia z kluczem publicznym (*Public Key Cryptography*)	System szyfrowania, w którym wykorzystuje się parę kluczy, publiczny i prywatny, do szyfrowania i/lub podpisu cyfrowego. Źródło: CNSSI-4009
Monitorowanie klawiatury (*Keystroke Monitoring*)	Proces używany do przeglądania lub rejestrowania zarówno naciskania klawiszy przez użytkownika komputera, jak i reakcji komputera podczas sesji interaktywnej. Monitorowanie klawiatury jest zwykle uważane za specjalny rodzaj ścieżek audytu.

Terminologia	Opis
Odmowa świadczenia usługi (*Denial of Service*)	Uniemożliwienie autoryzowanego dostępu do zasobów lub opóźnienie operacji, w których czas jest elementem krytycznym. (Czas na wykonanie operacji może wynosić milisekundy lub nawet godziny, w zależności od świadczonej usługi). Źródło: CNSSI-4009
Oprogramowanie szpiegujące (*Spyware*)	Oprogramowanie, które jest potajemnie instalowane w systemie w celu zbierania informacji o osobach lub organizacjach bez ich wiedzy; rodzaj złośliwego kodu. Źródło: NIST SP 800-53
Oprogramowanie złośliwe (*Malware*)	Patrz *Kod złośliwy*. Źródło: NIST SP 800-53
Osoba autoryzująca (AO) (*Authorizing Official [AO]*)	Wyższy szczebla osoba posiadająca uprawnienia do formalnego przyjęcia odpowiedzialności za eksploatację systemu przy akceptowalnym poziomie ryzyka dla działalności (w tym misji, funkcji, wizerunku lub reputacji) i aktywów organizacji, osób fizycznych, innych organizacji i państwa. Źródło: NIST SP 800-37 wer. 1
Plan bezpieczeństwa systemu (*System Security Plan*)	Formalny dokument, który zawiera przegląd wymagań bezpieczeństwa dla systemu i opisuje istniejące lub planowane środki bezpieczeństwa mające na celu spełnienie tych wymagań. Źródło: NIST SP 800-18
Podatność (*Vulnerability*)	Słaby punkt w systemie informacyjnym, procedurach bezpieczeństwa systemu, wewnętrznych środkach bezpieczeństwa lub wdrożeniu, który może zostać wykorzystany przez źródło zagrożenia. Źródło: NIST SP 800-30 wer. 1

Terminologia	Opis
Podpis cyfrowy (*Digital Signature*)	Wynik procesu kryptograficznej transformacji danych. Jeśli jest prawidłowo zrealizowany, zapewnia: 1. uwierzytelnienie pochodzenia, 2. integralność danych oraz 3. niezaprzeczalność podpisującego. Źródło: FIPS 140-2
Polityka bezpieczeństwa informacji (*Information Security Policy*)	Zbiór dyrektyw, przepisów, reguł i praktyk, które określają, w jaki sposób organizacja zarządza informacjami, chroni je i rozpowszechnia. Źródło: CNSSI-4009
Protokół uwierzytelniania typu wezwanie-odpowiedź (*Challenge-Response Protocol*)	Protokół uwierzytelniania, w którym weryfikator wysyła wnioskodawcy wezwanie (zwykle wartość losową lub identyfikator jednorazowy), które wnioskodawca łączy z sekretem (często poprzez utworzenie wspólnego hasha i udostępnionego sekretu lub poprzez zastosowanie do wezwania operacji klucza prywatnego) w celu wygenerowania odpowiedzi, która jest wysyłana do weryfikatora. Weryfikator może niezależnie zweryfikować odpowiedź wygenerowaną przez wezwanego (np. poprzez odwrócenie tworzenia skrótu hasha i udostępnionego sekretu i porównanie z odpowiedzią lub użycie do odpowiedzi klucza publicznego) i ustalić, że wezwany posiada i kontroluje sekret. Źródło: NIST SP 800-63-2
Przywilej (*Privilege*)	Uprawnienie przyznane osobie, programowi lub procesowi. Źródło: CNSSI-4009
Ramy zarządzania ryzykiem (RMF) (*Risk Management Framework [RMF]*)	Ustrukturyzowane podejście stosowane do nadzorowania ryzyka i zarządzania nim przez organizacje. Źródło: CNSSI-4009

Terminologia	Opis
Relacje wzajemne (*Reciprocity*)	Wspólne porozumienie między uczestniczącymi podmiotami dotyczące wzajemnego akceptowania swoich ocen bezpieczeństwa w celu ponownego wykorzystania zasobów systemu informacyjnego i/lub ocen poziomu bezpieczeństwa w celu wymiany informacji. Źródło: NIST SP 800-37
Robak (*Worm*)	Program powielający się, rozpowszechniający się i działający samoczynnie, który do rozprzestrzeniania się wykorzystuje mechanizmy sieciowe. Patrz *Kod złośliwy*. Źródło: CNSSI-4009
Rola (*Role*)	Pełniona funkcja lub stanowisko pracy, do którego w systemie mogą być przypisane osoby lub inne podmioty. Źródło: IETF RFC 4949 wer. 2
Rozliczalność (*Accountability*)	Cel bezpieczeństwa; wymaganie, aby działania podmiotu mogły być do niego jednoznacznie przypisane. Wspiera to osiągnięcie niezaprzeczalności, odstraszanie (teoria odstraszania zakłada, że zachowanie jednostki może być zmienione poprzez zastosowanie postrzeganej kary), izolację błędów, wykrywanie włamań i zapobieganie im oraz odzyskiwanie danych i działania prawne po zakończeniu danego działania. Źródło: NIST SP 800-27 wer. A

Terminologia	Opis
Ryzyko (*Risk*)	Miara stopnia zagrożenia podmiotu przez potencjalną okoliczność lub zdarzenie. Zazwyczaj jest funkcją: (I) niekorzystnych skutków, które powstałyby w przypadku wystąpienia okoliczności lub zdarzenia oraz (II) prawdopodobieństwa ich wystąpienia. [Uwaga: Ryzyko związane z bezpieczeństwem systemu to ryzyko wynikające z utraty poufności, integralności lub dostępności informacji lub systemów i odzwierciedlające potencjalny niekorzystny wpływ na działalność organizacji (w tym misję, funkcje, wizerunek lub reputację), aktywa organizacji, osoby fizyczne, inne organizacje i państwo. Niekorzystne skutki dla państwa to na przykład narażenie na szwank systemów, które obsługują infrastrukturę krytyczną lub mają zasadnicze znaczenie dla ciągłości operacji rządowych]. Źródło: NIST SP 800-37
Ryzyko bezpieczeństwa informacji (*Information Security Risk*)	Ryzyko dla działalności organizacji (w tym misji, funkcji, wizerunku, reputacji), jej aktywów, osób fizycznych, innych organizacji i państwa wynikające z możliwości nieuprawnionego dostępu, wykorzystania, ujawnienia, zakłócenia, modyfikacji lub zniszczenia informacji i/lub systemu. Źródło: NIST SP 800-30 wer. 1
Spam (*Spam*)	Niechciane elektroniczne wiadomości lub nadużycie elektronicznych systemów przesyłania wiadomości w celu masowego wysyłania niepożądanych wiadomości zbiorczych. Źródło: CNSSI-4009

Terminologia	Opis
Suma kontrolna (*Checksum*)	Wartość, która: a) jest obliczana przez funkcję zależną od zawartości obiektu danych i b) jest przechowywana lub przekazywana razem z obiektem, w celu wykrywania zmian w danych. Źródło: IETF RFC 4949 wer. 2
Sygnatura (*Signature*)	Rozpoznawalny, wyróżniający się wzorzec związany z atakiem, taki jak ciąg binarny w wirusie lub określony zestaw naciśnięć klawiszy wykorzystywany do uzyskania nieautoryzowanego dostępu do systemu. Źródło: NIST SP 800-61
System (*System*)	Każdy zorganizowany zespół zasobów i procedur połączonych i regulowanych przez interakcję lub współzależność w celu uzyskania zestawu określonych funkcji. Uwaga Do systemów zalicza się również systemy specjalistyczne, takie jak systemy przemysłowe/sterowania procesami, centrale telefoniczne i prywatne centrale telefoniczne (Private Branch Exchange – PBX) oraz systemy kontroli środowiska. Źródło: NIST SP 800-53
System informacyjny (*Information System*)	Odrębny zbiór zasobów informacyjnych zorganizowanych w celu gromadzenia, przetwarzania, utrzymywania, wykorzystywania, udostępniania, rozpowszechniania informacji lub dysponowania nimi. [Uwaga: Do systemów informacyjnych zalicza się również systemy specjalistyczne, takie jak systemy przemysłowe/sterowania procesami, centrale telefoniczne i prywatne centrale telefoniczne (*Private Branch Exchange – PBX*) oraz systemy kontroli środowiska]. Źródło: 44 U.S.C., pkt 3502

Terminologia	Opis
System wykrywania włamań (IDS) (*Intrusion Detection System [IDS]*)	Oprogramowanie, które automatyzuje proces wykrywania włamań. Źródło: NIST SP 800-94
Szacowanie ryzyka (*Risk Assessment*)	Proces identyfikacji zagrożeń dla działalności organizacji (w tym misji, funkcji, wizerunku, reputacji), aktywów organizacji, osób fizycznych, innych organizacji i państwa, wynikających z działania systemu. Część zarządzania ryzykiem, obejmuje analizy zagrożeń i podatności na zagrożenia oraz uwzględnia środki zaradcze w postaci planowanych lub wprowadzonych zabezpieczeń. Synonim analizy ryzyka. Źródło: NIST SP 800-39
Szacowanie środków bezpieczeństwa (*Security Control Assessment*)	Testowanie i/lub ocena zarządczych, operacyjnych i technicznych środków bezpieczeństwa w systemie w celu określenia zakresu, w jakim są one prawidłowo wdrożone, działają zgodnie z przeznaczeniem i przynoszą pożądane rezultaty w odniesieniu do spełnienia wymagań bezpieczeństwa systemu. Źródło: NIST SP 800-37
Szyfrogram (*Ciphertext*)	Dane w postaci zaszyfrowanej. Źródło: NIST SP 800-57 część 1, wer. 4
Szyfrowanie (*Encryption*)	Kryptograficzna transformacja danych umożliwiająca uzyskanie szyfrogramu. Źródło: ISO 7498-2
Szyfrowanie „punkt-punkt” (*End-to-End Encryption*)	Szyfrowanie komunikacji, w ramach której dane są szyfrowane podczas przechodzenia przez sieć, ale informacje o routingu pozostają widoczne.

Terminologia	Opis
Szyfrowanie linii (szyfrowanie grupowe) (*Link Encryption*)	Szyfrowanie informacji pomiędzy węzłami systemu komunikacyjnego. Źródło: CNSSI-4009
Środki bezpieczeństwa (*Security Controls*)	Środki zarządcze, operacyjne i technologiczne (tj. zabezpieczenia lub środki zaradcze) przewidziane dla systemu w celu ochrony poufności, integralności i dostępności systemu i zawartych w nim informacji. Źródło: FIPS 199
Technologia informacyjna (*Information Technology*)	(A) w odniesieniu do organizacji oznacza każdy sprzęt, połączony system lub podsystem sprzętu, wykorzystywany do automatycznego pozyskiwania, przechowywania, analizowania, oceniania, manipulowania, zarządzania, przemieszczania, kontrolowania, wyświetlania, przełączania, wymiany, przekazywania lub odbierania danych lub informacji przez organizację, jeżeli sprzęt jest przez nią wykorzystywany bezpośrednio lub jest wykorzystywany przez wykonawcę w ramach umowy z nią, która wymaga wykorzystania (I) tego sprzętu; lub (II) tego sprzętu w znacznym stopniu przy świadczeniu usługi lub dostarczaniu produktu; (B)obejmuje komputery, urządzenia pomocnicze (w tym urządzenia peryferyjne do przetwarzania obrazu, urządzenia wejściowe, wyjściowe i pamięci masowej niezbędne do celów bezpieczeństwa i nadzoru), urządzenia peryferyjne przeznaczone do sterowania przez jednostkę centralną komputera, oprogramowanie, oprogramowanie układowe i podobne procedury, usługi (w tym usługi wsparcia) oraz powiązane zasoby; ale (C) nie obejmuje żadnego sprzętu nabytego przez kontrahenta rządowego w ramach umowy rządowej. Źródło: 40 U.S.C., pkt 11101

Terminologia	Opis
Testowanie penetracyjne (*Penetration Testing*)	Metoda testowania, w której osoby oceniające, zazwyczaj pracujące zgodnie z określonymi ograniczeniami, próbują obejść lub pokonać zabezpieczenia systemu. Źródło: NIST SP 800-53
Token (*Token*)	Coś, co znajduje się w posiadaniu i kontroli powoda (zazwyczaj klucz lub hasło), które jest wykorzystywane do uwierzytelniania tożsamości powoda. Źródło: NIST SP 800-63-2
Tylna furtka (B*ackdoor*)	Nieudokumentowany sposób uzyskania dostępu do systemu komputerowego. Tylna furtka to potencjalne zagrożenie dla bezpieczeństwa. Źródło: NIST SP 800-82 wer. 2
Uwierzytelnienie (*Authentication*)	Weryfikacja tożsamości użytkownika, procesu lub urządzenia. Często traktowana jako warunek wstępny udzielenia dostępu do zasobów w systemie. Źródło: FIPS 200
Walidacja (*Validation*)	Potwierdzenie (poprzez dostarczenie mocnych, solidnych, obiektywnych dowodów), że wymagania dotyczące określonego zamierzonego użycia lub zastosowania zostały spełnione (np. przedstawiono wiarygodne poświadczenie albo dane lub informacje zostały sformatowane zgodnie ze zdefiniowanym zestawem zasad, albo w ramach określonego procesu wykazano, że rozważana jednostka spełnia pod każdym względem swoje zdefiniowane atrybuty lub wymagania). Źródło: CNSSI-4009

Terminologia	Opis
Wiarygodność (*Assurance*)	Podstawy do przekonania, że wszystkie cztery cele bezpieczeństwa (integralność, dostępność, poufność i rozliczalność) zostały odpowiednio spełnione w konkretnym wdrożeniu. Wyrażenie „odpowiednio spełnione” oznacza, że: (1) funkcje działają prawidłowo, (2) istnieje wystarczająca ochrona przed niezamierzonymi błędami (popełnianymi przez użytkowników lub oprogramowanie) oraz (3) odporność na zamierzoną penetrację lub obejście jest wystarczająca. Źródło: NIST SP 800-27 wer. A
Wiarygodność Informacji (*Information Assurance*)	Środki, które chronią i zabezpieczają informacje i systemy informacyjne poprzez zapewnienie ich dostępności, integralności, uwierzytelnienia, poufności i niezaprzeczalności. Środki te obejmują zapewnienie możliwości przywrócenia systemów informacyjnych poprzez włączenie zdolności ochrony, wykrywania i reagowania. Uwaga: W publikacji DoDI 8500.01 zrezygnowano z terminu wiarygodność informacji na rzecz terminu cyberbezpieczeństwo. Może to mieć potencjalny wpływ na terminy związane z wiarygodnością informacji. Źródło: CNSSI-4009
Wirus (*Virus*)	Program komputerowy, który może się skopiować i zainfekować komputer bez zgody i wiedzy użytkownika. Wirus może uszkodzić lub usunąć dane na komputerze, wykorzystać programy pocztowe do rozprzestrzenienia się na inne komputery, a nawet wymazać wszystko z dysku twardego. Patrz *Kod złośliwy*. Źródło: CNSSI-4009

Terminologia	Opis
Wrażliwość (*Sensitivity*)	Miara znaczenia przypisanego informacjom przez ich właścicieli w celu wskazania potrzeby ich ochrony. Źródło: NIST SP 800-60
Wyłudzanie informacji (Phishing) (*Phishing*)	Technika polegająca na próbie pozyskania wrażliwych danych, takich jak numery kont bankowych, poprzez nakłanianie w wiadomości e-mail lub na stronie internetowej, w ramach której sprawca podszywa się pod legalnie działającą firmę lub osobę o dobrej reputacji. Źródło: IETF RFC 4949 wer. 2
Zabezpieczenia (*Safeguards*)	Środki ochronne przewidziane w celu spełnienia wymagań bezpieczeństwa (tj. poufności, integralności i dostępności) określonych dla systemu. Zabezpieczenia mogą obejmować funkcje bezpieczeństwa, ograniczenia w zarządzaniu, bezpieczeństwo personelu oraz bezpieczeństwo struktur fizycznych, obszarów i urządzeń. Synonim środków bezpieczeństwa i środków przeciwdziałania. Źródło: FIPS 200
Zagrożenie (*Threat*)	Wszelkie okoliczności lub zdarzenia mogące mieć negatywny wpływ na działalność organizacji (w tym misję, funkcje, wizerunek lub reputację), aktywa organizacji, osoby fizyczne, inne organizacje lub państwo za pośrednictwem systemu poprzez nieuprawniony dostęp, zniszczenie, ujawnienie, modyfikację informacji i/lub odmowę świadczenia usługi. Źródło: NIST SP 800-30
Zapora sieciowa (*Firewall*)	Brama, która ogranicza dostęp między sieciami zgodnie z lokalną polityką bezpieczeństwa. Źródło: NIST SP 800-32

Terminologia	Opis
Zarządzanie kluczami (*Key Management*)	Działania obejmujące obsługę kluczy kryptograficznych i innych powiązanych parametrów bezpieczeństwa (np. wektorów inicjalizacyjnych) w całym cyklu życia kluczy, w tym ich generowanie, przechowywanie, ustanawianie, wprowadzanie i wyprowadzanie, używanie i niszczenie. Źródło: NIST SP 800-57 część 1, wer. 4
Zarządzanie ryzykiem (*Risk Management*)	Program i procesy wspierające zarządzanie ryzykiem związanym z bezpieczeństwem informacji dla działalności organizacji (w tym misji, funkcji, wizerunku, reputacji), jej aktywów, osób fizycznych, innych organizacji oraz państwa. Obejmuje: (I) ustanowienie kontekstu dla działań związanych z ryzykiem; (II) szacowanie ryzyka; (III) reagowanie na ryzyko po jego określeniu; oraz (IV) monitorowanie ryzyka w czasie. Źródło: NIST SP 800-39
Zasada minimalnych uprawnień (*Least Privilege*)	Zasada mówiąca, że architektura bezpieczeństwa powinna być zaprojektowana w taki sposób, aby każdemu podmiotowi przyznawać minimalne zasoby systemowe i uprawnienia, których podmiot ten potrzebuje do pełnienia swojej funkcji. Źródło: CNSSI-4009
Zaufany system (*Trustworthy System*)	Sprzęt komputerowy, oprogramowanie i procedury, które są dostatecznie zabezpieczone przed włamaniem i nadużyciem; zapewniają dostateczny poziom dostępności, niezawodności i prawidłowego działania; są dostatecznie dostosowane do wykonywania zamierzonych funkcji; oraz są zgodne z ogólnie przyjętymi procedurami bezpieczeństwa. Źródło: NIST SP 800-32

Terminologia	Opis
Zdarzenie powodujące zagrożenie (*Threat Event*)	Zdarzenie lub sytuacja, która potencjalnie może spowodować niepożądane konsekwencje lub wpływ. Źródło: NIST SP 800-30

ZAŁĄCZNIK C - AKRONIMY

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

Wybrane akronimy i skróty użyte w niniejszej publikacji zostały rozwinięte poniżej.

Akronim	Terminologia angielska	Terminologia polska
AC	Access Control	Kontrola dostępu
AES	Advanced Encryption Standard	Zaawansowany standard szyfrowania
AO	Authorizing Official	Osoba autoryzująca
APT	Advanced Persistent Threat	Zaawansowane zagrożenie długotrwałe
AT	Awareness and Training	Świadomość i szkolenie
AU	Audit and Accountability	Audyt i rozliczalność
BYOD	Bring Your Own Device	Przynieś własne urządzenie
CA	Security Assessment and Authorization	Ocena bezpieczeństwa i autoryzacja
CAP	Cross Agency Priority	Priorytet międzyorganizacyjny
CC	Common Criteria	Wspólne kryteria
CEO	Chief Executive Officer - CEO	Najwyższa funkcja zarządzająca
CIO	Chief Information Officer - CIO	Funkcja odpowiedzialna za technologie informacyjne
CISO	Chief Information Security Officer - CISO	Funkcja kluczowa ds. Bezpieczeństwa informacji
CKMS	Cryptographic Key Management System	System zarządzania kluczami kryptograficznymi
CM	Configuration Management	Zarządzanie konfiguracją
CMVP	Cryptographic Module Validation Program	Program walidacji modułów kryptograficznych

Akronim	Terminologia angielska	Terminologia polska
CNSSI	Committee on National Security Systems Instruction	----------
COOP	Continuity of Operations Plan	Plan kontynuacji operacji)
COTS	Commercial Off The Shelf	Produkt standardowy
CP	Contingency Planning	Planowanie awaryjne
CSP	Cloud Service Provider	Dostawca usług w chmurze
CSRC	Computer Security Resource Center	Centrum zasobów bezpieczeństwa komputerowego
CUI	Controlled Unclassified Information	Nadzorowane informacje jawne
DRP	Disaster Recovery Plan	Plan odtworzenia po katastrofie
FIPS	Federal Information Processing Standard	Federalny standard przetwarzania informacji
FIRMR	Federal Resource Management Regulation	Federalne rozporządzenie w sprawie zarządzania zasobami
FIRST	Forum for Incident Response Teams	Forum zespołów reagowania na incydenty bezpieczeństwa
FISMA	Federal Information Security Management Act	----------
HTTP	Hypertext Transfer Protocol	Protokół http
IA	Identification and Authentication	Identyfikacja i uwierzytelnianie
ICS	Industrial Control System	System sterowania przemysłowego
ICT	Information and Communications Technology	Technologia informacyjno-komunikacyjna
IDS	Intrusion Detection System	System wykrywania włamań

Akronim	Terminologia angielska	Terminologia polska
IP	Individual Privacy	Ochrona prywatności
IR	Incident Response	Reagowanie na incydenty
IRM	Information Resource Management	Zarządzanie zasobami informacyjnymi
ISAC	Information Sharing and Analysis Center	Centrum Wymiany Informacji i Analiz
ISCM	Information Security Continuous Monitoring	Strategia ciągłego monitorowania bezpieczeństwa informacji
ISO	International Organization for Standardization	Międzynarodowa organizacja normalizacyjna
IT	Information Technology	Technologia informacyjna/informatyczna
ITL	Information Technology Laboratory	Laboratorium informatyczne
MA	Maintenance	Utrzymanie systemu
MAC	Message Authentication Code	Kod uwierzytelnienia wiadomości
MP	Media Protection	Ochrona nośników danych)
NARA	National Archives and Records Administration	Krajowa Administracja Archiwów i Rejestrów
NIST	National Institute of Standards and Technology	Narodowy Instytut Standaryzacji i Technologii
NVD	National Vulnerability Database	Krajowa baza danych dotyczących podatności na zagrożenia
OMB	Office of Management and Budget	Biuro Zarządzania i Budżetu
P.L.	Public Law	Prawo publiczne
PA	Personal Authorization	Autoryzacja prywatności
PBX	Private Branch Exchange	Prywatna centrala telefoniczna

Akronim	Terminologia angielska	Terminologia polska
PE	Physical and Environmental Protection	Ochrona fizyczna i środowiskowa
PGP	Pretty Good Privacy	Narzędzie służące do szyfrowania, odszyfrowywania i uwierzytelniania
PII	Personally Identifiable Information	Dane osobowe
PIN	Personal Identification Number	Osobisty numer identyfikacyjny
PKI	Public Key Infrastructure	Infrastruktura klucza publicznego
PL	Planning	Planowanie
PM	Project Management	Zarządzanie programem
PS	Personnel Security	Bezpieczeństwo osobowe
RA	Risk Assessment	Szacowanie ryzyka
RAID	Redundant Array of Independent Disks	Nadmiarowa macierz niezależnych dysków
RMF	Risk Management Framework	Ramy zarządzania ryzykiem
S/MIME	Secure/Multipurpose Internal Mail Extension (S/MIME)	----------
SA	Systems and Services Acquisition	Pozyskiwanie systemów i usług
SAISO	Senior Agency Information Security Officer	Funkcja zarządzająca ds. Bezpieczeństwa informacji
SAOP	Senior Agency Official for Privacy	Inspektor ochrony danych / funkcja zarządzająca ds. Prywatności
SC	System and Communications Protection	Ochrona systemu i komunikacji
SCP	System Contingency Plan	Plan awaryjny systemu

Akronim	Terminologia angielska	Terminologia polska
SI	System and Information Protection	Ochrona systemu i informacji
SP	Special Publication	Publikacja specjalna
SSE	System Security Engineer	Inżynier bezpieczeństwa systemu
SSO	System Security Officer	Funkcja ds. Bezpieczeństwa systemu
SSP	System Security Plan	Plan bezpieczeństwa systemu
TCB	Trusted Computing Base	Zaufana baza przetwarzania