PARP
Grupa PFR

Sektorowa Rada ds. Kompetencji
Telekomunikacja i Cyberbezpieczeństwo

PORADNIK CYBERBEZPIECZEŃSTWA

dla środowisk edukacyjnych i przedsiębiorstw

PORADNIK CYBERBEZPIECZEŃSTWA

dla środowisk edukacyjnych i przedsiębiorstw

WSTĘP

Oddajemy w Państwa ręce poradnik dotyczący sposobów zapewnienia cyberbezpieczeństwa niemal każdej organizacji. Dziś to już odrębna dziedzina wiedzy i praktyki, do której z powodu rosnących zagrożeń niemal codziennie dochodzą nowe elementy. Nie jest to więc proste i łatwe wyzwanie, a jednak odnosimy wrażenie, że liderki i liderzy wielu organizacji w Polsce nie przypisują mu dostatecznej wagi. Tymczasem koszty zaniechań w tej dziedzinie bywają okrutne.

Dlatego staramy się w tym opracowaniu wytłumaczyć zawiłości cyberbezpieczeństwa jak najszerszemu gronu odbiorczyń i odbiorców, realizujących różne role w swoich organizacjach. Spodziewamy się, że poradnik pomoże tym, którzy dopiero zaczynają zgłębiać temat, oraz tym wszystkim, którzy dostrzegają problem i chcieliby poprawić odporność ich organizacji w coraz bardziej przenikającej wszystko cyberprzestrzeni.

Mamy nadzieję, że nasze opracowanie w możliwie najprostszy sposób wesprze ich w odpowiedzi na trzy zasadnicze pytania:

- jakie działania muszą podejmować kadry zarządzające organizacjami, aby stworzyć systemowe i skuteczne rozwiązania w zakresie cyberbezpieczeństwa?
- na jakie role i kompetencje trzeba kłaść nacisk, aby rozwijać ekspertki i ekspertów cyberbezpieczeństwa w organizacjach działających w różnej skali?
- jakie kompetencje z zakresu cyberbezpieczeństwa są potrzebne pracowniczkom i pracownikom jutra, aby umieli realnie walczyć nie tylko z obecnymi, ale i nadchodzącymi cyberzagrożeniami?

W poradniku kładziemy też nacisk na rolę ludzi w cyberbezpieczeństwie. To ludzie często bywają słabym ogniwem w tym systemie, ale też tylko dobrze przygotowani ludzie mogą zapewnić swoim organizacjom najwyższą odporność. Dlatego dedykujemy poradnik także edukatorkom i edukatorom cyberbezpieczeństwa, niosącym ten „kaganek oświaty" na różnych poziomach edukacji.

A wszystkim naszym Czytelniczkom i Czytelnikom życzymy sukcesów w wysiłkach na rzecz cyberbezpieczeństwa ich organizacji!

Publikacja realizowana w ramach Projektu pn. „Utworzenie i funkcjonowanie Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo".

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza, Edukacja, Rozwój.

Autorzy opracowania: **ANDRZEJ BARTOSIEWICZ, JĘDRZEJ BIENIASZ, KRZYSZTOF SZCZYPIORSKI**

Realizator publikacji: Ośrodek THINKTANK

Redaktor: Zbigniew Gajewski

Korekta: Anna Chyckowska, Małgorzata Gerasimiuk

Opracowanie graficzne: Dorota Jędrkiewicz

ISBN 978-83-967447-4-6 Warszawa 2023

SPIS TREŚCI

SŁOWNIK

Cyberbezpieczeństwo – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy

CER (Critical Entities Resilience) – Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE

CRA (Cyber Resilience Act) – Rozporządzenie Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniające rozporządzenie (UE) 2019/1020

Dostępność – cecha klasycznej triady ochrony informacji w zakresie zapewniania niezawodnego i w adekwatnym czasie dostępu do informacji oraz ich wykorzystania

Incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo

Incydent krytyczny – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV

Incydent poważny – incydent powodujący lub mogący spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej

Incydent istotny – incydent, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia wykonawczego Komisji (UE) 2018/151 z 30 stycznia 2018 r. (ustanawia ono zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 precyzuje czynniki, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych oraz parametrów określających, czy incydent ma istotny wpływ)

Incydent w podmiocie publicznym – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny

Integralność – cecha klasycznej triady ochrony informacji w zakresie ochrony przed niewłaściwą modyfikacją lub zniszczeniem informacji (obejmuje zapewnienie niezaprzeczalności i autentyczności informacji)

Norma – dokument techniczny, który określa specyficzne wymagania, wytyczne, zasady lub charakterystyki dla produktów, usług, procesów lub działań. Normy mają na celu ułatwienie zrozumienia i interpretacji wymagań oraz zapewnienie spójności i jakości w danej dziedzinie lub branży; normy mogą być opracowywane przez organizacje międzynarodowe, krajowe instytuty standaryzacji lub branżowe grupy ekspertów

Obsługa incydentu – czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu

Podatność – właściwość systemu informacyjnego, która może spowodować zagrożenie cyberbezpieczeństwa

Poufność – cecha klasycznej triady ochrony informacji w zakresie zapewnienia autoryzowanych ograniczeń w dostępie i ujawnianiu informacji; dotyczy też środków ochrony prywatności i informacji zastrzeżonych

Ryzyko – kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji

Standard – ogólny termin odnoszący się do uznanych i zaakceptowanych reguł, norm, wytycznych lub wzorców, uznawanych za punkt odniesienia w określonej dziedzinie; standardy mogą być opublikowane przez różne organizacje lub władze regulacyjne i służą jako wytyczne lub modele do osiągnięcia ustalonych celów lub jakości; standardy często to bardziej ogólne wytyczne niż normy, ale niekoniecznie są mniej ważne czy mniej wymagające

Szacowanie ryzyka – całościowy proces identyfikacji, analizy i oceny ryzyka

Usługa kluczowa – ma podstawowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej; jest wymieniana w wykazie usług kluczowych

Zagrożenie cyberbezpieczeństwa – potencjalna przyczyna wystąpienia incydentu

Zarządzanie incydentem – obsługa incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu

Zarządzanie ryzykiem – skoordynowane działania dotyczące kierowania cyberbezpieczeństwem w organizacji w związku z oszacowanym ryzykiem

CZYM JEST CYBERBEZPIECZEŃSTWO I DLACZEGO DOTYCZY CIEBIE ORAZ TWOJEJ FIRMY?

SKĄD WZIĘŁA SIĘ CYBERPRZESTRZEŃ?

Cyfryzacja przenika już prawie każdą sferę ludzkiego życia. Coraz trudniej wskazać obszary, w których nie ma jakiegoś rodzaju procesora czy rozwiązania służącego łączności z innymi obiektami. Przez ostatnie 70 lat obserwujemy i bierzemy udział w rewolucji cyfrowej, która rozpoczęła się od m.in. praktycznego opracowania tranzystora (1947–1950) oraz stworzenia podstaw współczesnej komunikacji (Shannon, 1948).

Następne dekady to stałe przyspieszanie budowy i integracji wielowymiarowych rozwiązań dla gospodarki cyfrowej, a sprzyjało termu stworzenie powszechnego Internetu (1969). Dzięki niemu w kolejnych 50 latach coraz szybciej rozwijały się aplikacje obliczeniowe oraz służące łączności. Były one coraz mocniejsze, coraz szybsze, coraz bardziej niezawodne, a co najważniejsze – komunikujące się niemalże bez przeszkód.

Pojęcie „cyberprzestrzeń" powstało niemalże wraz z początkiem rewolucji cyfrowej w wymiarze technicznym. Zostało użyte po raz pierwszy pod koniec lat 60. w nazwie cyklu instalacji artystycznych autorstwa Susanne Ussing. W latach 80. wykorzystał je następnie William Gibson, pisarz podgatunku science-fiction „cyberpunk". A teraz, w 2023 r., większość z nas ma osobisty komputer w domu, a często także komputer przenośny, smartfon z łącznością telefoniczną i internetową docierającą w każdy niemal zakątek świata, smarttelewizor, smartzegarek, inteligentne urządzenia domowe, inteligentny samochód itp. Nasz świat fizyczny przenika się z wirtualnym i zupełnie naturalnie funkcjonujemy w przestrzeni, która jest jednocześnie cyberprzestrzenią.

Istotnym katalizatorem rozwoju cyberprzestrzeni było bez wątpienia powstanie rozległej, otwartej sieci teleinformatycznej określanej jako Internet. Dzisiaj wiele użytkowniczek i wielu użytkowników utożsamia Internet z cyberprzestrzenią, jednak trzeba zauważyć, że poza nim istnieje wiele różnych rodzajów sieci, które pomagają m.in. Twojej organizacji i od których zależy jej biznesowa codzienność.

Niezależnie od tego, rzeczywiście to Internet jest podstawową, ogólnie dostępną na całym świecie siecią teleinformatyczną, a jego historia liczy już 60 lat. Główną ideą stojącą za stworzeniem Internetu było umożliwienie użytkowniczkom i użytkownikom z różnych lokalizacji geograficznych swobodnej komunikacji za pośrednictwem ich komputerów. Powstała w tym celu rozległa infrastruktura telekomunikacyjna, obejmująca lądy (światłowody i kable miedziane), oceany (światłowody międzykontynentalne), a także powietrze (bezprzewodowa komunikacja radiowa oraz technologie satelitarne). Infrastruktura ta jest utrzymywana i rozwijana przez wiele państwowych i prywatnych firm telekomunikacyjnych, które porozumiały się co do standardów wymiany danych między ich sieciami na potrzeby globalnej komunikacji.

Dedykowanym protokołem komunikacji internetowej jest IP (ang. *Internet Protocol*). To mechanizm adresacji logicznej zasobów podłączonych do sieci, np. komputerów czy serwerów, a także technologie kierowania komunikacji do wskazanych adresów logicznych, określanych jako trasowanie (ang. *routing*). Najbardziej upowszechnioną wersją protokołu IP jest IPv4, ale postępuje także adaptacja protokołu IP w wersji 6.

Inną kluczową technologią dla sieci Internet jest DNS (ang. *Domain Name System*). Oferuje ona możliwość wykorzystywania tekstowych nazw zasobów przy ich adresowaniu, a DNS odpowiada za przetłumaczenie nazwy zasobu na jego adres IP, wykorzystywany bezpośrednio w trasowaniu komunikacji. Jako użytkowniczki i użytkownicy najczęściej mamy z tym do czynienia, korzystając

z podstawowej usługi sieci Internet, czyli stron WWW (ang. *World Wide Web*). Przy wchodzeniu na stronę WWW użyjemy bezpośrednio w przeglądarce internetowej adresu np. www.google.pl, a nie adresu IP, pod którym również można odnaleźć tę stronę i pobrać ją do przeglądarki za pomocą protokołu HTTP (ang. *Hyper Text Transfer Protocol*). W tym przypadku pomocny DNS ustala na podstawie adresu domenowego odpowiedni adres IP.

Warto podkreślić, że sieć teleinformatyczna to nie tylko Internet. Na przykład w biurze firmy komunikacja między komputerami odbywa się bezpośrednio za pomocą sieci lokalnej (ang. LAN – *Local Area Network*), przewodowej lub bezprzewodowej (ang. *WLAN, Wireless LAN*). Wspomniane sieci telekomunikacyjne, określane jako operatorskie sieci rozległe (ang. *WAN, Wide Area Network*), służą m.in. do oferowania połączeń sieciowych między biurami firmy zlokalizowanych w różnych miejscach oraz do świadczenia wielu innych usług poza samym Internetem.

Oddzielnym typem sieci operatorskiej są sieci teleinformatyczne operatorów komunikacji mobilnej, które posługują się wyspecjalizowanymi rozwiązaniami usługowymi oraz protokołami umożliwiającymi połączenia głosowe, tekstowe, a także udostępniają Internet w telefonach komórkowych. Ważnym obszarem rozwoju sieci teleinformatycznych jest ponadto ich wirtualizacja w systemach typu *datacenter* oraz *cloud*, tj. farmach serwerów, które są oferowane w formie różnych usług.

Wspomniane wcześniej sieci teleinformatyczne – lokalne, operatorskie, *datacenter*, *cloud* – są często zaliczane do wspólnej kategorii sieci IT (ang. *information technology*), w których większość technologii protokołowych jest wspólna, uniwersalna, oparta na jednolitych standardach. Ewentualne różnice wynikają najczęściej z trybu działania danej sieci, czyli sposobu wykorzystania danych protokołów i usług stowarzyszonych.

Obok powyższych powstała też kategoria sieci teleinformatycznych dla specyficznych systemów używanych w rozwiązaniach przemysłowych. Są one określane jako sieci OT (ang. *operational technology*). Mają one dedykowane protokoły komunikacji, a także wykorzystują sieci do sterowania procesami, obok samej usługi wymiany danych. Wspomniane protokoły komunikacji dla systemów OT są dzisiaj coraz częściej wspólne z protokołami sieci IT, ale nadal w sieciach tych występują różne technologie komunikacyjne. Warto wspomnieć, że tego typu sieci na poziomie fizycznym muszą m.in. nadal wspierać połącze-

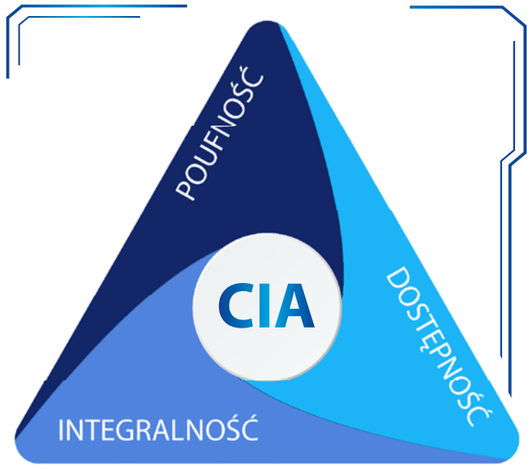
nia szeregowe, podczas gdy typowa sieć teleinformatyczna IT jest fizycznie oparta na standardzie Ethernet (IEEE 802.3). Warto jednak pamiętać o tych sieciach ze względu na ich zastosowanie w kluczowych obszarach gospodarki, m.in. w fabrykach, ale także w energetyce, transporcie czy w dostawach wody. Tym samym sieci te mogą mieć charakter strategiczny (infrastruktura krytyczna), co powoduje, że ich przydatność wykracza poza typową wymianę informacji, a ich niezawodność i ciągłość działania jest ważna dla szeroko rozumianego bezpieczeństwa.

CYBER…BEZPIECZEŃSTWO

W utopijnej wizji cyberprzestrzeń jest nieskrępowanym miejscem komunikacji i wymiany wiedzy – i jako taka jest pozytywną wartością dla jej użytkowniczek i użytkowników. Wierzą oni ponadto, że tak będzie zawsze. W praktyce nowa przestrzeń technologiczna od początku przyciąga też siły chcące jej używać do negatywnych, w tym przestępczych celów.

W cyberprzestrzeni, tak jak w realu, pojawia się więc coraz więcej szkodliwych zjawisk i działań wymierzonych w ich użytkowniczki i użytkowników. Początkowo traktowano je jako m.in. nową formę zabawy czy złośliwie żarty. Jednak pomysłowość ludzi została użyta do działań jednoznacznie negatywnych, takich jak kradzież pieniędzy i informacji. Tak zaczęła się burzliwa historia rozwoju różnych form i rodzajów cyberataków.

Jak przy wszystkich nowych technologiach, ich twórczynie i twórcy zdawali sobie sprawę, że świat cyfrowy nie będzie miejscem wyłącznie pozytywnych aktywności. Od samego początku trwają dyskusje o najlepszych sposobach zabezpieczania komputerów i przesyłanych przez nie danych. W efekcie wytypowano triadę właściwości informacji w cyberprzestrzeni, które mają być chronione przed atakującymi. Są to: poufność (**C** – *confidentiality*), integralność (**I** – *integrity*) oraz dostępność (**A** – *availability*), co układa się w łatwy do zapamiętania trzyliterowy skrót **CIA**.



Poufność jest rozumiana jako ochrona treści przed odczytaniem ich przez osoby nieuprawnione. W tym celu rozwija się m.in. kryptografia, która oferuje fundamentalne matematyczne rozwiązania szyfrowania, skracana informacji czy potwierdzania tożsamości osób uprawnionych (podpisy).

Ochrona **integralności** ma sprawić, żeby dane nie były naruszane pod względem zawartości, czyli nie zostały zmienione lub usunięte przez nikogo poza osobami uprawnionymi. Tylko wtedy możliwe jest określenie takich danych jako autentycznych. Jeśli natomiast dokonano ich modyfikacji, to trzeba sprawić, aby modyfikujący nie mógł zaprzeczyć, że tego dokonał.

Dostępność natomiast określa, że zapewniona jest możliwość pracy z danymi w sposób niezawodny i w określonym, adekwatnym czasie. Wszelkie cyberataki skutkujące odmową usługi w różnej skali i formie – ang. *denial-of-service*, *DoS* – to właśnie zagrożenia dostępności.

Dziś świadomość, na jak wiele sposobów cyberprzestrzeń może zostać wykorzystana do przeprowadzania działań o negatywnych skutkach dla jej użytkowniczek i użytkowników, staje się powszechna. Dlatego stałym zjawiskiem w tym świecie jest wyścig między cyberbezpieczeństwem (działaniami chroniącymi bezpieczeństwo cyberprzestrzeni) a cyberatakami (atakami na cyberprzestrzeń). Odpowiedzialni za cyberbezpieczeństwo starają się przyjmować postawę proaktywną, tj. przewidywać kolejne oraz nowe formy cyberataków i zalecać najlepsze w danym momencie formy zabezpieczania się przed nimi (prewencyjna funkcja cyberbezpieczeństwa).

W 2023 r. temat ten nabrał jeszcze większej wagi w związku z przyspieszonym rozwojem sztucznej inteligencji. Rozwinęła się globalna dyskusja angażująca m.in. rządy, organizacje międzynarodowe, wyspecjalizowane instytucje zajmujące się cyberbezpieczeństwem, firmy technologiczne, thinktanki i naukowców, czym jest (cyber)bezpieczeństwo sztucznej inteligencji oraz w ogólności systemów informatycznych opartych na rozwiązaniach AI/ML.

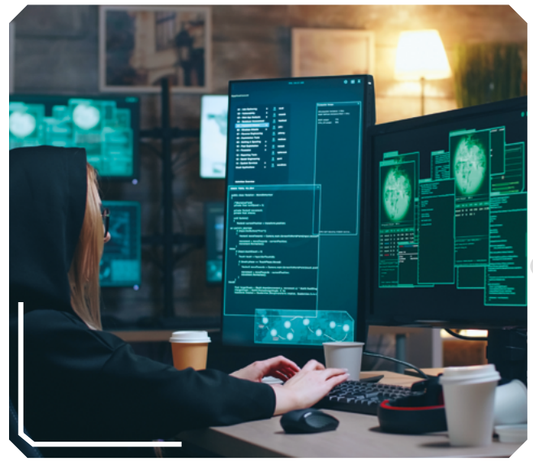
Często jednak nie da się wszystkiego przewidzieć z góry i odpowiednio zabezpieczyć wszystkich zasobów, dlatego drugą istotną funkcją cyberbezpieczeństwa jest zdolność do wykrywania cyberzagrożeń. Polega to na ciągłym ich obserwowaniu, analizowaniu i wyciąganiu wniosków. To praca, która często stanowi duże, oddzielne wyzwanie w sieciach i systemach informatycznych.

A co, jeżeli nie jesteśmy w stanie dobrze się zabezpieczyć (prewencja) ani wykryć cyberataku odpowiednio wcześnie? Na taką okoliczność trzeba być przygotowanym do odtwarzania utraconych zasobów i minimalizowania skutków cyberataku. Służą temu m.in. systemy kopii zapasowych. Jednak coraz ważniejsza staje się funkcja odtworzeniowa cyberbezpieczeństwa, obejmująca także przygotowanie procesowo-operacyjne do incydentów. Oznacza to zarządzanie ciągłością działania, szybkie odtwarzanie zdolności operacyjnych i minimalizowanie skutków cyberataków. Jedną z form takich przygotowań są też wszelkiego rodzaju regularne testy kryzysowe czy odtworzeniowe.

Zdarza się, że mimo właściwej realizacji przez organizację wymienionych funkcji cyberbezpieczeństwa, stosowane przez nią rozwiązania przestają być wystarczające. Co jakiś czas zdarzają się bowiem spektakularne cyberataki, jak np. wyjątkowo złożony atak na rozwiązania producenta systemów zarządzania środowiskami IT SolarWinds, które pośrednio naraziły też takie organizacje, jak Microsoft, FireEye czy Departament Obrony USA.

Dla wszelkich organizacji, także dla firm z sektora MŚP, wynika z tego wniosek: zapewnienie cyberbezpieczeństwa to nie punktowy czy jednorazowy projekt informatyczny, lecz ciągły proces wzmacniania odporności systemów informatycznych, na których oparty jest biznes. Środkiem do realizacji tego celu jest włączenie zarządzania cyberbezpieczeństwem w obszar zarządzania wszystkimi najważniejszymi ryzykami organizacji, jak ryzyka operacyjne, finansowe, wizerunkowe czy prawne.

Cyberryzyka, obok innych ryzyk, to prawdopodobieństwo ich wystąpienia (ang. *probability*, *likelihood*) oraz ocena wpływu lub skutku (ang. *impact*). Warto wskazać jeszcze dodatkowe zależności pomiędzy kluczowymi pojęciami charakterystycznymi dla cyberbezpieczeństwa. To przede wszystkim podatność (ang. *vulnerability*) i zagrożenie (ang. *threat*), a także środki zaradcze (ang. *countermeasures*).



OGÓLNY MODEL KLUCZOWYCH CZYNNIKÓW RYZYKA

Źródło: Narodowy Standard Cyberbezpieczeństwa 800-30
https://www.gov.pl/attachment/7c1839f3-e93d-48f4-9ee2-9036910ff7d4

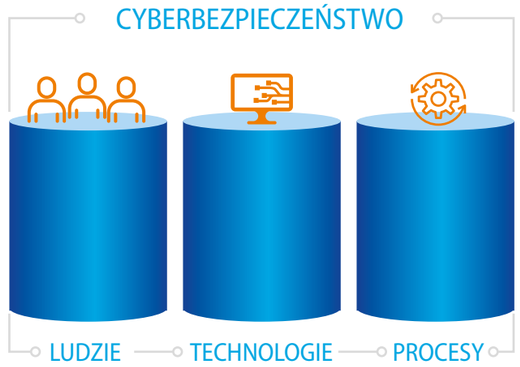
Rysunek odzwierciedla ideę zamkniętego cyklu zarządzania ryzykiem, od uświadamiania potencjalnych zagrożeń i podatności, które mogą zostać wykorzystane przez atakujących (z określonym prawdopodobieństwem), przez negatywny wpływ tych zagrożeń na zasoby organizacji po dobieranie środków zaradczych, które mogą osłabiać zagrożenie albo redukować jego wystąpienie w przyszłości. W ostatnim rozdziale omawiamy bardziej szczegółowo różne metodyki zarządzania ryzykiem w cyberbezpieczeństwie.

DLACZEGO CYBERBEZPIECZEŃSTWO TWOJEJ ORGANIZACJI JEST DZISIAJ TAK ISTOTNE?

Cyberbezpieczeństwo Twojej organizacji to dzisiaj element większej całości. Dlatego każda organizacja, mała, średnia, duża, publiczna czy prywatna, powinna dążyć do organicznego wdrażania aspektów cyberbezpieczeństwa. W scyfryzowanej gospodarce stanowi to fundament odporności i jest wręcz warunkiem udanej realizacji własnych celów strategicznych. W oparciu o takie podejście od lat budowane są na świecie systemy cyberbezpieczeństwa: na poziomach regionalnych (np. województwa), krajowych, międzynarodowych regionalnych (np. UE) i międzynarodowych ponadregionalnych (np. NATO).

Tworzenie systemów cyberbezpieczeństwa, od tych najmniejszych, w małych organizacjach, po te największe, opiera się zawsze na trzech fundamentach. Są to: ludzie, procesy oraz technologie. Tylko balans między nimi zapewnia właściwy rozwój i efektywność wdrażanych środków.

Kategoria „Ludzie" w cyberbezpieczeństwie oznacza zarówno szeroką świadomość wagi cyberbezpieczeństwa wśród pracowniczek i pracowników organizacji, jak i zgromadzenie przez nią adekwatnych kompetencji, wewnętrznych bądź zewnętrznych. Kategoria „Procesy" dotyczy ustanawiania i dokumentowania systemów zarządzania cyberbezpieczeństwem w organizacji. Obejmuje również kulturę samonaprawiania błędów w tym obszarze poprzez regularne audyty i planowanie na ich podstawie nowych działań poprawiających cyberbezpieczeństwo.



„Ludzie" i „Procesy" nie mogą istnieć dzisiaj bez przemyślanej aktywności w obszarze „Technologie". Zadania cyberbezpieczeństwa muszą być bowiem realizowane przy wsparciu adekwatnych narzędzi i mechanizmów technicznych, które pozwalają egzekwować założenia polityk cyberbezpieczeństwa w systemach informatycznych. W technologiach tego rodzaju w ostatnich latach nastąpił duży postęp. Stają się bardziej wyrafinowane, a jednocześnie tańsze i bardziej dostępne dla różnych rozmiarów organizacji. Warto też zwrócić uwagę na dość liczne programy krajowe czy europejskie dofinansowujące podnoszenie poziomu cyberbezpieczeństwa w organizacjach. Jest to jeden z przejawów realizacji idei systemowego cyberbezpieczeństwa już od poziomu małej organizacji. Dlatego mamy nadzieję, że niniejszy poradnik sprawi, że Twoja firma czy instytucja przyłączy się do tej podróży.

SYSTEM ORGANIZACJI CYBERBEZPIECZEŃSTWEM W POLSCE

POPULARNE STANDARDY CYBERBEZPIECZEŃSTWA

Obecnie jednym z kluczowych czynników wpływających na działania firm i instytucji w zakresie cyberbezpieczeństwa są wymagania prawne. Zanim się pojawiły, istotnym czynnikiem wymuszającym stosowanie odpowiednich procesów i zabezpieczeń były normy i standardy, w tym standardy branżowe.

Standardy cyberbezpieczeństwa różnią się w zależności od kraju, regionu, a także branży oraz rodzaju organizacji. Istnieją standardy przyjęte ogólnie jako normy międzynarodowe (np. ISO 27001), uzupełniane coraz częściej wymaganiami prawnymi (jak DORA czy NIS2) oraz wymaganiami branżowymi (np. normy CENELEC).

Jak do tej wielości standardów powinno podchodzić przedsiębiorstwo? Musi ono brać pod uwagę zarówno normy ogólne, jak i branżowe (sektorowe). W praktyce normy ogólne (np. IEC 62443) implementowane są często w wybranych sektorach (np. norma IEC 62443 implementowana jako CENELEC 50701 w sektorze transportu szynowego). Niektóre sektory i branże posługują się własnymi, wypracowanymi normami (np. ISO/SAE 21434 w sektorze automotive). Warto zaznaczyć, że od niedawna niektóre branżowe normy inżynieryjne definiujące proces projektowania i wytwarzania zawierają już komponent cybersecurity (np. norma definiująca cykl produkcyjny, tzw. model V, dla sektora transportowego – EN 50126). To wszystko przekłada się bezpośrednio na rozszerzenie wymagań wobec specjalistek i specjalistów cyberbezpieczeństwa pracujących w poszczególnych branżach.

Wśród głównych międzynarodowych standardów i norm, które są powszechnie uznawane w dziedzinie cyberbezpieczeństwa, są:

- **ISO/IEC 27001**: to międzynarodowy standard określający wymagania dla systemów zarządzania bezpieczeństwem informacji. Pomaga organizacjom w identyfikowaniu, zarządzaniu i minimalizowaniu ryzyka w tym obszarze. Standard jest generalnie neutralny, jeśli chodzi o branżę, państwo czy wielkość firmy.

- **NIST SP 800-53:** to opracowany przez National Institute of Standards and Technology (NIST) w Stanach Zjednoczonych zbiór wymagań bezpieczeństwa informacji, które powinny być wdrożone przez agencje rządowe i inne organizacje podlegające ustawodawstwu amerykańskiemu. Ze względu na swoje zaawansowanie i praktyczność często są przyjmowane przez podmioty poza USA. Między innymi polski rząd wprowadza Narodowe Standardy Cyberbezpieczeństwa oparte na NIST. Uwzględnienie standardów rodziny NIST jest szczególnie ważne dla podmiotów będących częścią międzynarodowych korporacji z siedzibą w USA.

- **CIS Controls**: to stworzony przez Center for Internet Security (CIS) zbiór 20 list kontrolnych; obejmuje podstawowe środki bezpieczeństwa, które powinny być wdrażane przez organizacje w celu ochrony przed zaawansowanymi cyberatakami.

- **HIPAA (Health Insurance Portability and Accountability Act):** to amerykański standard ochrony danych medycznych, określający wymagania dotyczące ich bezpieczeństwa i prywatności.

- **PCI DSS (Payment Card Industry Data Security Standard):** to standard dotyczący firm, które przetwarzają płatności kartami kredytowymi; określa wymagania bezpieczeństwa w celu ochrony przechowywanych na nich danych.

- I**EC 62443:** to standard dotyczący bezpieczeństwa systemów kontroli przemysłowych (ICS); skupia się na zapewnieniu cyberbezpieczeństwa w sektorze przemysłowym.

EKOSYSTEM CYBERBEZPIECZEŃSTWA W POLSCE

Ekosystem ten obejmuje wiele podmiotów państwowych i prywatnych, regulowanych przez liczne europejskie i polskie akty prawne oraz regulacje branżowe, a także wymagania biznesowe ustalane pomiędzy podmiotami komercyjnymi i odpowiadające na oczekiwania konsumentów.

Do najważniejszych regulacji mających wpływ na wspomniany ekosystem należą m.in. RODO, NIS/NIS2, Ustawa o Krajowym Systemie Cyberbezpieczeństwa, DORA, CRA oraz CER. Poniżej zostaną opisane kluczowe z nich, a w kolejnym podrozdziale opiszemy podmioty, które są ważnymi elementami ekosystemu.

PRZEGLĄD REGULACJI

RODO

RODO to skrót od „Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych" (ang. *General Data Protection Regulation, GDPR*). Jest europejskim rozporządzeniem, które weszło w życie 25 maja 2018 r. i wprowadziło nowe zasady i normy dotyczące ochrony danych osobowych w krajach członkowskich Unii Europejskiej oraz Europejskiego Obszaru Gospodarczego (EOG). Głównym celem tego aktu jest zapewnienie większej ochrony prywatności i bezpieczeństwa danych osobowych obywateli, a także jednolitej regulacji w tej sprawie we wszystkich państwach członkowskich UE.

RODO wskazuje zadania zarówno podmiotów prywatnych, jak i instytucji państwowych i powierza nadzór nad ich realizacją Prezesowi Urzędu Ochrony Danych Osobowych.

Najważniejsze zasady RODO:

- Podmioty przetwarzające dane osób muszą uzyskać ich uprzednią, wyraźną i jednoznaczną zgodę.

- Obywatelki i obywatele mają szereg praw związanych z ich danymi, takich jak prawo dostępu do nich, prawo do ich sprostowania, prawo do usunięcia, prawo do przenoszenia danych itp.

- Firmy i organizacje przetwarzające dane osobowe muszą przestrzegać określonych zasad bezpieczeństwa danych, zgłaszać naruszenia ochrony danych i powoływać Inspektora Ochrony Danych (IOD) w niektórych przypadkach.

- RODO wprowadza zasady przetwarzania danych, takie jak zasada ograniczenia celu, minimalizacji danych, ograniczenia przechowywania, integralności i poufności.

- Firmom, które nie przestrzegają przepisów RODO, grożą poważne sankcje finansowe. Kary mogą sięgać nawet 4 proc. całkowitego rocznego obrotu przedsiębiorstwa.

Celem RODO jest zwiększenie zaufania obywatelek i obywateli UE i EOG do przetwarzania danych osobowych, ochronę ich prywatności i zapewnienie lepszej nad nimi kontroli. Wdrożenie RODO miało istotny wpływ na wiele firm i organizacji na całym świecie, ponieważ każda firma, która oferuje swoje produkty lub usługi w UE, musi przestrzegać tych przepisów, niezależnie od tego, gdzie jest zlokalizowana.

Każde państwo członkowskie UE (i EOG) ma obowiązek zapewnić, by za monitorowanie stosowania rozporządzenia RODO odpowiadał co najmniej jeden niezależny organ publiczny. Jego rola to ochrona podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem ich danych oraz ułatwianie swobodnego przepływu danych osobowych. W Polsce taką funkcję pełni Prezes Urzędu Ochrony Danych.

Dyrektywa NIS

Dyrektywa NIS (ang. *Directive on Security of Network and Information Systems*) to akt prawny Unii Europejskiej w sprawie bezpieczeństwa sieci i systemów informatycznych. Została przyjęta przez Parlament Europejski i Radę UE w 2016 r. Oficjalnie nosi nazwę „Dyrektywa (UE) 2016/1148 w sprawie środków mających zapewnić wysoki wspólny poziom bezpieczeństwa sieci i systemów informatycznych we wszystkich państwach członkowskich i uchylająca dyrektywę 2008/114/WE".

Celem NIS jest podniesienie poziomu ochrony i bezpieczeństwa sieci komputerowych i systemów informatycznych w państwach członkowskich UE. Przepisy dyrektywy opierają się na założeniu, że spójny i skoordynowany system bezpieczeństwa cybersieci w całej Unii jest kluczowy dla skutecznej jej ochrony przed zagrożeniami cybernetycznymi i zapobiegania atakom na infrastrukturę krytyczną oraz usługi cyfrowe.

Główne elementy dyrektywy NIS:

- Państwa członkowskie są zobowiązane do wyznaczenia odpowiednich instytucji i organów krajowych ds. bezpieczeństwa sieci i informacji.
- Dyrektywa określa wymagania dotyczące zapewnienia bezpieczeństwa sieci i informacji dla operatorów usług kluczowych (np. dostawcy energii, transportu, usług bankowych itp.) oraz dostawców usług cyfrowych, takich jak platformy internetowe, chmura obliczeniowa, rynki elektroniczne itp.
- Operatorzy usług kluczowych i dostawcy usług cyfrowych zobowiązani są do zapewnienia odpowiedniego poziomu bezpieczeństwa oraz zgłaszania istotnych incydentów bezpieczeństwa do właściwych władz.
- Państwa członkowskie mają obowiązek wymiany między sobą informacji o zagrożeniach oraz współpracy w zakresie reagowania na cyberataki i incydenty związane z bezpieczeństwem.

Dyrektywa NIS wzmacnia współpracę pomiędzy państwami członkowskimi i ułatwia spójne podejście do ochrony przed zagrożeniami cybernetycznymi w całej Unii Europejskiej. Państwa członkowskie są zobowiązane do jej wdrożenia do swojego prawa krajowego, co ma przyczynić się do zwiększenia odporności cyfrowej Unii Europejskiej jako całości.

Ustawa o Krajowym Systemie Cyberbezpieczeństwa

Ustawa o krajowym systemie cyberbezpieczeństwa implementuje do polskiego porządku prawnego dyrektywę Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa 2016/1148, tzw. Dyrektywa NIS). Ustawa została opublikowana w Dzienniku Ustaw RP 13 sierpnia 2023 r. i obowiązuje po 14 dniach od jej ogłoszenia tj. od 28 sierpnia 2023 r.

Pełne wdrożenie Dyrektywy NIS wymaga jeszcze przyjęcia dwóch rozporządzeń Rady Ministrów: w sprawie uznania incydentu za poważny, jak i w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych. Obecnie w tej sprawie trwają prace legislacyjne i konsultacje społeczne.

Celem przygotowanej przez Ministerstwo Cyfryzacji ustawy o krajowym systemie cyberbezpieczeństwa było opracowanie uregulowań prawnych umożliwiających implementację dyrektywy NIS oraz utworzenie efektywnego systemu bezpieczeństwa teleinformatycznego na poziomie krajowym.

Krajowy system cyberbezpieczeństwa ma w szczególności umożliwić:

- niezakłócone świadczenie usług kluczowych i usług cyfrowych,
- osiągnięcie odpowiednio wysokiego poziomu bezpieczeństwa systemów teleinformatycznych służących do świadczenia tych usług.

Budowany system obejmuje:

- operatorów usług kluczowych (m.in. z sektorów energetycznego, transportowego, zdrowotnego i bankowości),
- dostawców usług cyfrowych,
- zespoły CSIRT (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego) poziomu krajowego,
- sektorowe zespoły cyberbezpieczeństwa,
- podmioty świadczące usługi z zakresu cyberbezpieczeństwa,
- organy właściwe do spraw cyberbezpieczeństwa,
- oraz punkt kontaktowy do komunikacji w ramach współpracy w Unii Europejskiej w dziedzinie spraw cyberbezpieczeństwa.

Operatorzy usług kluczowych są zobowiązani do wdrożenia skutecznych zabezpieczeń, szacowania ryzyka związanego z cyberbezpieczeństwem oraz przekazywania informacji o poważnych incydentach oraz ich obsługi we współpracy z CSIRT poziomu krajowego. Wymienione podmioty są również zobowiązane do wyznaczenia osoby odpowiedzialnej za cyberbezpieczeństwo świadczonych usług, obsługi i zgłaszania incydentów oraz udostępniania wiedzy na temat cyberbezpieczeństwa. Do krajowego systemu cyberbezpieczeństwa będą również włączone organy administracji publicznej, a także przedsiębiorczynie i przedsiębiorcy telekomunikacyjni – w sposób zharmonizowany z istniejącymi uregulowaniami w tym zakresie.

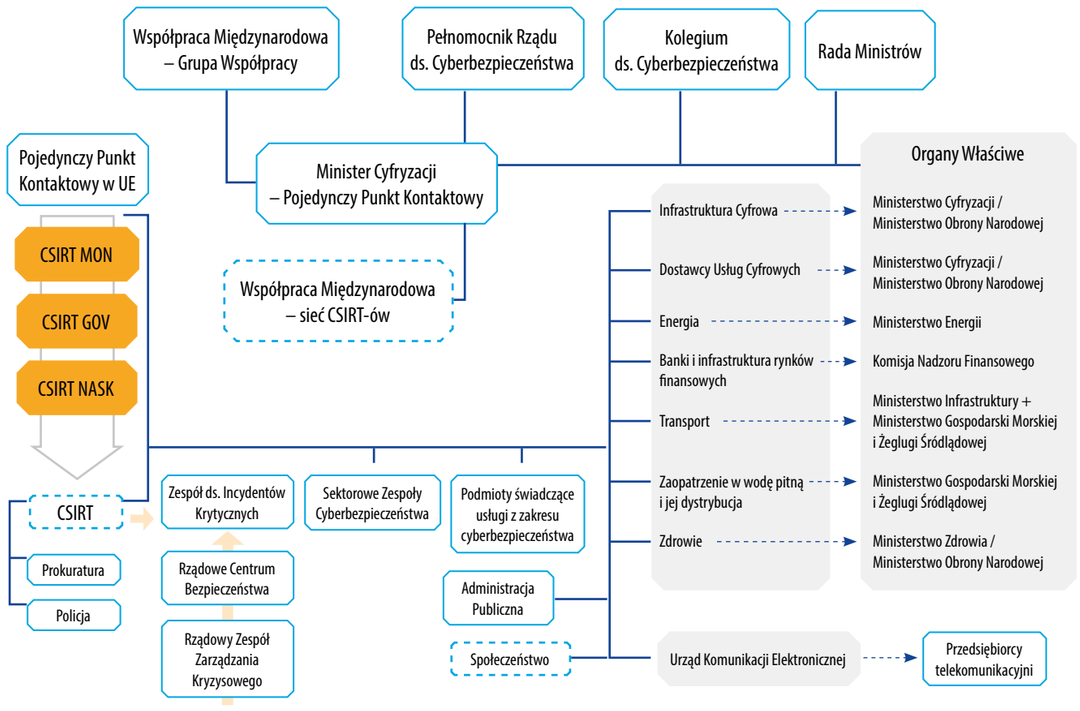
Wymaganiami z zakresu cyberbezpieczeństwa zostali także objęci dostawcy usług cyfrowych, czyli internetowe platformy handlowe, usługi przetwarzania w chmurze i wyszukiwarki internetowe. Z racji międzynarodowej specyfiki tych podmiotów, obowiązki dla dostawców usług cyfrowych są objęte zharmonizowanym na poziomie UE reżimem regulacyjnym. Ustawa odwołuje się tutaj do decyzji wykonawczej Komisji Europejskiej.

Na poziomie instytucjonalnym w skład Krajowego system cyberbezpieczeństwa wchodzą:

- operatorzy usług kluczowych,
- dostawcy usług cyfrowych,
- CSIRT MON (CSIRT – Computer Security Incident Response Team),
- CSIRT NASK,
- CSIRT GOV,
- sektorowe zespoły cyberbezpieczeństwa,
- jednostki sektora finansów publicznych,
- instytuty badawcze, Narodowy Bank Polski, Bank Gospodarstwa Krajowego, Urząd Dozoru Technicznego, Polska Agencja Żeglugi Powietrznej, Polskie Centrum Akredytacji, Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej,
- spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej,
- podmioty świadczące usługi z zakresu cyberbezpieczeństwa,
- organy właściwe do spraw cyberbezpieczeństwa,
- Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa,
- Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa,
- Kolegium do Spraw Cyberbezpieczeństwa.

Z punktu widzenia przedsiębiorców najważniejsze podmioty ekosystemu wynikającego z Ustawy KSC to CSIRT-y, a w szczególności CSIRT NASK, sektorowy zespół cyberbezpieczeństwa.

SCHEMAT ORGANIZACYJNY KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA



Źródło grafiki: prezentacja „Funkcjonowanie KSC oraz plany jego rozwoju", KSC Forum 2019, prezentacja MC/KPRM

DORA

DORA to rozporządzenie Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014. Zostało ono opublikowane w Dzienniku Urzędowym Unii Europejskiej 27 grudnia 2022 r., a dwadzieścia dni później, tj. 16 stycznia 2023 r., weszło w życie.

Jego głównym zadaniem jest stworzenie zharmonizowanego, bezpiecznego i odpornego na turbulencje cyfrowego sektora finansowego w UE. DORA ustanawia jednolite wymogi dotyczące bezpieczeństwa sieci i systemów informatycznych przedsiębiorstw i instytucji działających w sektorze finansowym, a także kluczowych zewnętrznych dostawców usług związanych z ICT (technologiami informacyjno-komunikacyjnymi), takich jak platformy w chmurze czy usługi analizy danych. Powstają w ten sposób ramy regulujące operacyjną odporność cyfrową, zgodnie z którymi wszystkie przedsiębiorstwa sektora finansów muszą upewnić się, że są w stanie wytrzymać wszelkiego rodzaju zakłócenia i zagrożenia związane z ICT, reagować na nie i przezwyciężać ich skutki. Wymogi te są jednolite we wszystkich państwach członkowskich UE.

DORA dotyczy wielu podmiotów finansowych regulowanych na szczeblu unijnym, takich jak instytucje kredytowe, płatnicze, instytucje pieniądza elektronicznego, firmy inwestycyjne, dostawców usług w zakresie kryptoaktywów, centralne depozyty papierów wartościowych, kontrahentów centralnych, systemy obrotu, repozytoria transakcji, zarządzających alternatywnymi funduszami inwestycyjnymi, dostawców usług w zakresie udostępniania informacji, zakłady ubezpieczeń i zakłady reasekuracji, pośredników ubezpieczeniowych, instytucje pracowniczych programów emerytalnych, agencje ratingowe, biegłych rewidentów i firmy audytorskie, administratorów kluczowych wskaźników referencyjnych oraz dostawców usług finansowania społecznościowego czy też repozytoriów sekurytyzacji.

W szczególności rozporządzenie DORA wskazuje:

- wymogi mające nakładać na podmioty finansowe obowiązki:
- zarządzania ryzykiem związanym z wykorzystaniem technologii informacyjno-komunikacyjnych (ICT),
- zgłaszania poważnych incydentów związanych z ICT właściwym organom oraz dobrowolnego informowania ich o znaczących cyberzagrożeniach,
- zgłaszania właściwym organom poważnych incydentów operacyjnych lub poważnych incydentów bezpieczeństwa związanych z płatnościami,
- testowania operacyjnej odporności cyfrowej,
- wymiany informacji i analiz w związku z cyberzagrożeniami i podatnościami w tym obszarze,
- podjęcia działań na rzecz należytego zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT,
- wymogi w odniesieniu do ustaleń umownych zawartych między zewnętrznymi dostawcami usług ICT a podmiotami finansowymi,
- zasady dotyczące ustanowienia i funkcjonowania ram nadzoru nad kluczowymi zewnętrznymi dostawcami usług ICT świadczącymi usługi na rzecz podmiotów finansowych,
- zasady współpracy między właściwymi organami oraz zasady nadzoru i egzekwowania przepisów przez właściwe organy w odniesieniu do wszystkich kwestii objętych tym rozporządzeniem.

CRA – Akt o Cyberodporności

Celem Rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa

w odniesieniu do produktów z elementami cyfrowymi i zmieniające rozporządzenie (UE) 2019/1020 jest ustanowienie standardów w zakresie zasad cyberbezpieczeństwa urządzeń łączących się z Internetem. Priorytety regulacji mają zostać osiągnięte m.in. poprzez wyeliminowanie luk w zabezpieczeniach produktów cyfrowych i usług pomocniczych oraz lepsze informowanie użytkowników o dobrych praktykach zwiększających ich bezpieczeństwo. **Rozporządzenie wprowadza wymogi dla producentów oprogramowania i sprzętu, w szczególności:**

- zapewnienie, że przez przewidywany okres użytkowania produktu lub przez pięć lat po wprowadzeniu na rynek podatności na zagrożenia będą skutecznie usuwane,
- powiadamianie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) o zidentyfikowanych lukach w produkcie lub usłudze w ciągu 24 godzin,
- uwzględnienie przez producentów sprzętów elektronicznych zasad cyberbezpieczeństwa już na etapie projektowania swoich towarów i usług.

CRA jest uzupełnieniem Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (NIS2). Podczas gdy NIS2 obejmuje kwestie bezpieczeństwa krytycznych łańcuchów dostaw, rozporządzenie CRA stanowi uzupełnienie kwestii bezpieczeństwa urządzeń podłączonych do Internetu (zwłaszcza Internetu Rzeczy). Jest to bardzo istotne dla użytkowników, którzy powszechnie korzystają z takich urządzeń.

Dyrektywa CER

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE nakłada na państwa członkowskie obowiązek podjęcia konkretnych kroków w celu zapewnienie niezakłóconego świadczenia na rynku wewnętrznym usług kluczowych. Chodzi o utrzymanie bezpieczeństwa niezbędnych funkcji społecznych lub niezbędnej działalności gospodarczej, w szczególności poprzez wspieranie podmiotów krytycznych. Określa też obowiązki podmiotów krytycznych w zwiększeniu ich odporności i zdolności do świadczenia usług na rynku wewnętrznym.

Zgodnie z Dyrektywą państwa członkowskie powinny dokonać analizy ryzyka, uwzględniając sektorowe oceny ryzyka przeprowadzone na podstawie innych aktów prawnych UE oraz zależności pomiędzy sektorami krajowymi i międzynarodowymi. Wyniki oceny ryzyka należy wykorzystać w procesie wskazywania podmiotów krytycznych.

Podmioty krytyczne będą miały obowiązek ochrony infrastruktury niezbędnej do utrzymania usług kluczowych. Taka infrastruktura jest nazywana infrastrukturą krytyczną. Za niewywiązywanie się z tych obowiązków dyrektywa przewiduje sankcje finansowe. Jednocześnie podmioty krytyczne będą mogły liczyć na wsparcie finansowe ze strony państwa, jeśli będzie to uzasadnione bezpieczeństwem publicznym. Takie wsparcie nie będzie traktowane jako niedozwolona pomoc publiczna.

Przepisy Dyrektywy mówią także o konieczności wyznaczenia przez państwa członkowskie właściwego organu odpowiedzialnego za prawidłowe stosowanie dyrektywy na szczeblu krajowym.

Według przepisów Dyrektywy CER państwa członkowskie są zobowiązane do przyjęcia strategii, której celem będzie wzmocnienie odporności podmiotów krytycznych. Kompleksowe podejście do odporności podmiotów krytycznych powinno uwzględniać m.in. właściwą koordynację wyznaczonych organów, a także przepisy prawne umożliwiające wymianę informacji na temat incydentów i cyberzagrożeń oraz właściwe wykonywanie zadań nadzorczych.

Wdrażanie dyrektywy CER zostało zaplanowane na trzy lata. Biorąc pod uwagę istniejące zagrożenia oraz zdarzenia, jakie już wystąpiły (zniszczenie NORD Stream I i II, cyberataki na infrastrukturę krytyczną oraz ataki sabotażowe na systemy sterowania ruchem pociągów w Niemczach), Rada Europejska zdecydowała się na wprowadzenie rozwiązań przejściowych w formie rekomendacji. Rekomendacje powinny doprowadzić do poprawy bezpieczeństwa infrastruktury krytycznej w Europie w ciągu kilku najbliższych miesięcy.

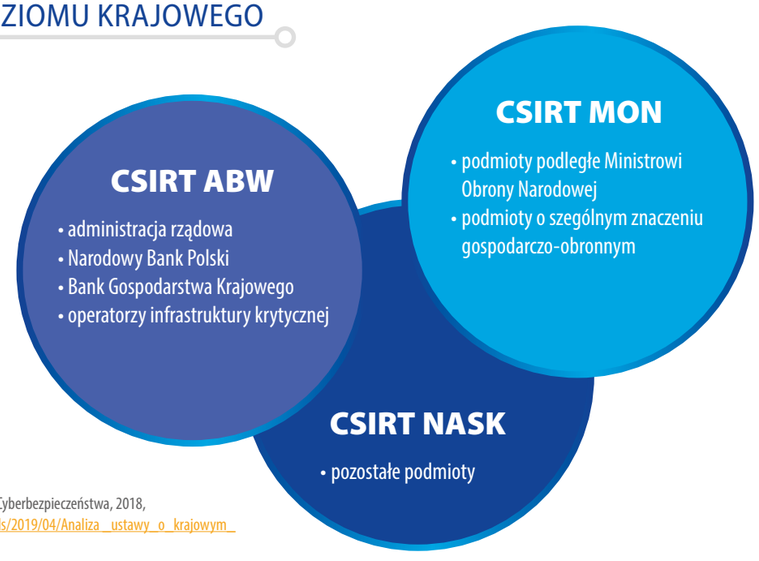
KLUCZOWE PODMIOTY Z PUNKTU WIDZENIA ŚRODOWISKA PRZEDSIĘBIORCÓW W POLSCE

Zespoły CSIRT Poziomu Krajowego

Krajowy System Cyberbezpieczeństwa w Polsce określa trzy zespoły CSIRT poziomu krajowego:

1. **CSIRT GOV** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego
2. **CSIRT MON** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej
3. **CSIRT NASK** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy. Jest to podstawowy zespół dla przedsiębiorców w Polsce przyjmujący zgłoszenia o cyberatakach.

ZESPOŁY CSIRT POZIOMU KRAJOWEGO



Źródło: NASK, Analiza Ustawy o krajowym systemie Cyberbezpieczeństwa, 2018, URL: https://cyberpolicy.nask.pl/wp-content/uploads/2019/04/Analiza__ustawy__o__krajowym__systemie__cyberbezpieczenstwa.pdf

Prezes Urzędu Ochrony Danych Osobowych

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r., zwane w skrócie RODO, nakłada na każde państwo członkowskie UE obowiązek monitorowania jego stosowania przez co najmniej jeden niezależny organ publiczny (zwany dalej „organem nadzorczym"). Jego celem ma być ochrona podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem ich danych oraz ułatwianie swobodnego przepływu danych osobowych w UE. W Polsce takim organem nadzorczym jest Prezes Urzędu Ochrony Danych Osobowych. Podstawę prawną działania jego urzędu stanowi w/w rozporządzenie RODO oraz ustawa z 10 maja 2018 r. o ochronie danych osobowych, a także wydane na jej podstawie akty wykonawcze.

Organ nadzorczy (UODO) w Polsce:

- monitoruje i egzekwuje stosowanie rozporządzenia RODO,
- upowszechnia w społeczeństwie wiedzę o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem danych osobowych oraz rozumienie tych zjawisk; szczególną uwagę poświęca działaniom skierowanym do dzieci,
- doradza, zgodnie z prawem państwa członkowskiego, parlamentowi narodowemu, rządowi oraz innym instytucjom i organom w sprawie aktów prawnych i administracyjnych środków ochrony praw i wolności osób fizycznych w związku z przetwarzaniem danych,
- upowszechnia wśród administratorów i podmiotów przetwarzających dane wiedzę o obowiązkach spoczywających na nich na mocy rozporządzenia RODO,
- udziela osobie, której dane dotyczą, na jej żądanie informacji o wykonywaniu praw przysługujących jej na mocy rozporządzenia, a w stosownym przypadku współpracuje w tym celu z organami nadzorczymi innych państw członkowskich,
- rozpatruje skargi wniesione przez osobę, której dane dotyczą, lub przez podmiot, organizację czy zrzeszenie; w odpowiednim zakresie prowadzi postępowania w przedmiocie tych skarg i w rozsądnym terminie informuje skarżącego o postępach i wynikach postępowań, w szczególności, jeżeli niezbędne jest ich dalsze prowadzenie lub koordynacja działań z innym organem nadzorczym,
- współpracuje z innymi organami nadzorczymi, w tym dzieli się informacjami oraz świadczy wzajemną pomoc, w celu zapewnienia spójnego stosowania i egzekwowania rozporządzenia,
- prowadzi postępowania w sprawie stosowania rozporządzenia RODO, w tym na podstawie informacji otrzymanych od innego organu nadzorczego lub innego organu publicznego,
- monitoruje zmiany w stosownych dziedzinach, o ile zmiany te mają wpływ na ochronę danych osobowych, w szczególności monitoruje rozwój technologii informacyjno-komunikacyjnych i praktyk handlowych,
- przyjmuje standardowe klauzule umowne,
- ustanawia i prowadzi wykaz związany z wymogiem dokonania oceny skutków dla ochrony danych,
- udziela zaleceń dotyczących operacji przetwarzania danych,
- zachęca do sporządzania kodeksów postępowania, wydaje opinie na ich temat oraz zatwierdza te kodeksy, w których znajdują się odpowiednie zabezpieczenia,
- zachęca do ustanawiania mechanizmów certyfikacji w dziedzinie ochrony danych oraz znaków jakości i oznaczeń z tej dziedziny, a także zatwierdza kryteria certyfikacji,
- opracowuje i publikuje kryteria akredytacji podmiotu monitorującego kodeksy postępowania oraz podmiotu certyfikującego,
- akredytuje podmiot monitorujący kodeksy postępowania oraz podmiot certyfikujący,
- wydaje zezwolenia na klauzule umowne i przepisy,
- zatwierdza wiążące reguły korporacyjne,
- bierze udział w pracach Europejskiej Rady Ochrony Danych,
- prowadzi wewnętrzny rejestr naruszeń rozporządzenia RODO.

Sektorowe zespoły bezpieczeństwa / ISAC

Sektorowe zespoły bezpieczeństwa (ang. *Information Sharing and Analysis Center*) można tworzyć na podstawie dyrektywy NIS oraz NIS2. Organ właściwy do spraw cyberbezpieczeństwa może ustanowić, zgodnie z odrębnymi przepisami, sektorowy zespół cyberbezpieczeństwa dla danego sektora lub podsektora, odpowiedzialny w szczególności za:

- przyjmowanie zgłoszeń o incydentach poważnych oraz wsparcie w obsłudze tych incydentów,
- wspieranie operatorów usług kluczowych w wykonywaniu ich obowiązków,
- analizowanie incydentów poważnych, wyszukiwanie powiązań pomiędzy incydentami oraz opracowywanie wniosków z ich obsługi,
- współpracę z właściwym CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie koordynowania obsługi incydentów poważnych.

Sektorowy zespół cyberbezpieczeństwa może przekazywać informacje do innych państw, w tym państw członkowskich Unii Europejskiej i przyjmować z tych państw informacje o incydentach poważnych, w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej.

Sektorowy zespół cyberbezpieczeństwa może otrzymywać zgłoszenia incydentu poważnego z innego państwa członkowskiego Unii Europejskiej dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej. Zespół przekazuje te zgłoszenia do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV oraz Pojedynczego Punktu Kontaktowego.

W przypadku ustanowienia sektorowego zespołu cyberbezpieczeństwa organ właściwy do spraw cyberbezpieczeństwa informuje o tym operatorów usług kluczowych w danym sektorze oraz CSIRT MON, CSIRT NASK i CSIRT GOV.

W Polsce działa jeden sektorowy zespół cyberbezpieczeństwa, koordynujący działania w zakresie cyberbezpieczeństwa w sektorze finansowym. To tam powinny być zgłaszane wszelkie incydenty z tego sektora.

CSIRT KNF

Sektorowy Zespół Cyberbezpieczeństwa (CSIRT KNF) został utworzony przez Komisję Nadzoru Finansowego w celu prowadzenia koordynacji działań i wsparcia obsługi incydentów bezpieczeństwa w podmiotach rynku finansowego uznanych za Operatorów Usług Kluczowych (OUK) w rozumieniu Ustawy o Krajowym Systemie Cyberbezpieczeństwa.

Zespół realizuje swoje zadania we współpracy z podmiotami krajowego systemu cyberbezpieczeństwa, a w szczególności zespołami CSIRT poziomu krajowego. Wspiera on Operatorów Usług Kluczowych w obsłudze incydentów poważnych występujących w tych podmiotach, a także prowadzi analizy pozostałych incydentów, trendów i zagrożeń w obszarze cyberbezpieczeństwa.

W szczególności celem działań Zespołu jest realizacja zadań określonych w Ustawie:

- przyjmowanie zgłoszeń o incydentach poważnych oraz wsparcie w obsłudze tych incydentów,
- wspieranie OUK w wykonywaniu obowiązków określonych w Ustawie,
- analizowanie incydentów poważnych, wyszukiwanie powiązań pomiędzy incydentami oraz opracowywanie wniosków z obsługi incydentu,
- współpracę z właściwym CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie koordynowania obsługi incydentów poważnych.

Kontakt w sprawie zgłoszeń incydentów: csirt@knf.gov.pl

Centra Wymiany i Analizy Informacji (ISAC)

Obok formalnych, sektorowych zespołów bezpieczeństwa, w sektorach mogą istnieć różne formy wspierające cyberbezpieczeństwo, w tym organizacje ISAC (ang. *Information Sharing and Analysis Center*).

ISAC tłumaczony jest na język polski jako Centrum Wymiany i Analizy Informacji. Centra wymieniają się wiedzą i doświadczeniami dotyczącymi incydentów cyberbezpieczeństwa w danym sektorze gospodarki (np. finansowym, energetyki czy lotnictwa). ISAC jest formą partnerstwa publiczno-prywatnego (PPP), rozumianego jako długookresowe porozumienie przynajmniej dwóch przedstawicieli sektora prywatnego lub publicznego. W tej inicjatywie chodzi także o budowanie relacji pomiędzy różnymi sektorami gospodarki oraz pomiędzy różnymi instytucjami publicznymi.

PPP wydaje się być szczególnie istotne dla cyberbezpieczeństwa, ponieważ operatorzy usług kluczowych to przede wszystkim prywatne przedsiębiorstwa. Dodatkowo zagrożenia teleinformatyczne rzadko dotyczą tylko jednej instytucji, a nawet jednego sektora. Dobra współpraca i właściwa wymiana wiedzy mogą znacznie podnieść poziom cyberbezpieczeństwa. Nie tylko z uwagi na wymianę informacji o samych incydentach czy też zagrożeniach, ale także dzięki możliwości uczenia się od siebie nawzajem.

Z danych zebranych przez Europejską Agencję Bezpieczeństwa Sieci i Informacji (ENISA) wynika, że rozwinięcie systemu partnerstw publiczno-prywatnych w dziedzinie cyberbezpieczeństwa, a w szczególności powstanie ISAC, wyraźnie przyczyniło się do zwiększenia ogólnego poziomu wiedzy na temat zagrożeń w państwach UE, a także do wzrostu kompetencji poszczególnych firm i instytucji w przeciwdziałaniu zagrożeniom [źródło: Poradnik-NASK--na-temat-tworzenia-ISAC.pdf].

W Polsce działa kilka zespołów sektorowych. Przedsiębiorstwa z niżej wymienionych branż powinny nawiązać z nimi współpracę z obopólną korzyścią.

ISAC-Kolej zajmuje się cyberbezpieczeństwem w podsektorze transportu kolejowego. Głównym celem centrum jest stała wymiana wiedzy oraz doświadczeń dotyczących incydentów i zagrożeń cyberbezpieczeństwa pomiędzy uczestniczącymi w przedsięwzięciu podmiotami. Ma się do tego przyczynić wypracowanie spójnych standardów, dobrych praktyk, polityk i procedur w tym zakresie oraz usprawnienie współpracy z krajowymi oraz międzynarodowymi zespołami cyberbezpieczeństwa.

Powołanie ISAC-Kolej to także jeden z elementów opracowanego już projektu „Polityki współpracy w zakresie informatyki i telekomunikacji w ramach Grupy PKP i PKP PLK" i jest krokiem w kierunku budowy kolejowego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego – CSIRT.

Jednym z celów tego projektu jest standaryzacja oraz ustanowienie wspólnych zasad zarządzania obszarem cyberbezpieczeństwa w transporcie kolejowym oraz ochrona wszystkich aspektów jego cyberprzestrzeni, a także aktywne wsparcie budowy Krajowego Systemu Cyberbezpieczeństwa.

Kontakt: admin@isac-kolej.pl

ISAC-GIG to Centrum Wymiany i Analizy Informacji w Zakresie Cyberbezpieczeństwa dla sektora wydobywczo-energetycznego. Zostało powołane przez sześć największych podmiotów tego sektora. W dokumencie powołującym zadeklarowano stałą wymianę wiedzy oraz doświadczeń dotyczących bezpieczeństwa cyfrowego i przeciwdziałania cyberzagrożeniom. Inicjatorem projektu jest Główny Instytut Górnictwa w Katowicach, a wspiera go Ministerstwo Aktywów Państwowych. Centrum będzie opracowywać oraz promować standardy i rekomendacje dla branży wydobywczo-energetycznej, a także współpracować przy obsłudze incydentów bezpieczeństwa, dotykających jednostki sektora.

Kontakt: isac@gig.eu

W ramach **Fundacji non-profit CISO #Poland**, powstałej na początku 2023 r., skupiającej szefów bezpieczeństwa około 200 polskich firm i instytucji, działają sektorowe zespoły robocze pełniące funkcje tożsame z zespołami ISAC:

- **CISO #Poland #transport** to grupa robocza sektora transportu, w tym transportu kolejowego, drogowego, morskiego i lotniczego.

Kontakt: transport@cisopoland.org

- **CISO #Poland #energy** to grupa robocza sektora energetycznego, w tym wytwarzania i dystrybucji energii elektrycznej, a także wydobycia, przetwarzania i dystrybucji węglowodorów.

Kontakt: energy@cisopoland.org

- **CISO #Poland #finance** to grupa robocza sektora bankowego i szeroko rozumianego sektora finansowego.

Kontakt: finance@cisopoland.org

- **CISO #Poland #pharma** to grupa robocza sektora farmaceutycznego oraz ochrony zdrowia.

Kontakt: pharma@cisopoland.org

FUNDAMENTY CYBERBEZPIECZEŃSTWA KAŻDEJ ORGANIZACJI

STRATEGIA OBRONY WIELOPOZIOMOWEJ

Defence-in-depth (Obrona wielopoziomowa) to strategia i podejście w dziedzinie cyberbezpieczeństwa, które polega na stosowaniu wielu warstw zabezpieczeń w celu ochrony systemów, sieci, danych i aplikacji przed różnymi rodzajami zagrożeń i ataków. Celem tej strategii jest zwiększenie odporności na ataki. Nawet jeśli jedna z warstw zabezpieczeń zostanie złamana, pozostałe warstwy nadal chronią system przed naruszeniem.

Obrona wielopoziomowa w organizacji zakłada, że nie można polegać wyłącznie na pojedynczej linii obrony, ponieważ żadne pojedyncze zabezpieczenie nie jest doskonałe i może łatwo być przezwyciężone przez wyrafinowane ataki. Dlatego stosuje się wiele warstw zabezpieczeń, które uzupełniają się nawzajem, tworząc bardziej złożoną i trudniejszą do sforsowania barierę ochronną.

Przykładowe warstwy obrony wielopoziomowej mogą obejmować:

- zapory sieciowe (firewalle) na granicach sieci, które kontrolują ruch wchodzący i wychodzący,
- systemy wykrywania intruzów (IDS) i systemy zapobiegania intruzom (IPS), które monitorują ruch sieciowy w poszukiwaniu podejrzanych aktywności i ataków, a także podejmują działania w celu blokowania niebezpiecznych aktywności,
- antywirusy i oprogramowanie antymalware na poziomie hosta, które chronią indywidualne urządzenia przed szkodliwym oprogramowaniem,
- oprogramowanie do zarządzania uprawnieniami, które kontroluje dostęp do zasobów i danych, aby zapobiegać nieautoryzowanemu dostępowi,
- szyfrowanie danych, które chroni poufność i integralność informacji,
- przestrzeganie polityk bezpieczeństwa, szkolenia pracowników w zakresie świadomości cyberbezpieczeństwa oraz audyty bezpieczeństwa, aby zapewnić zgodność z wytycznymi.

Zastosowanie obrony wielopoziomowej umożliwia organizacjom lepszą ochronę przed zaawansowanymi zagrożeniami i pozwala na reagowanie na różne typy ataków w skuteczny sposób. Obrona wielopoziomowa jest zalecana i szeroko stosowana jako kluczowa strategia w dzisiejszym środowisku cyfrowym, gdzie zagrożenia i ataki cybernetyczne są powszechne, a ich metody stale się rozwijają.

ZARZĄDZANIE RYZYKIEM W KONTEKŚCIE CYBERBEZPIECZEŃSTWA ORGANIZACJI

Analiza ryzyka w bezpieczeństwie informacji

Analiza ta jest podstawowym wymaganiem nie tylko wynikającym z dobrych praktyk, ale też obowiązkowym elementem każdego standardu i normy z obszaru bezpieczeństwa informacji (w tym rodziny standardów ISO, NIST, IEC czy CENELEC), a także elementem każdej z regulacji prawnych Unii Europejskiej dotyczącej bezpieczeństwa sieci i systemów, w tym NIS, NIS2, Cybersecurity Act czy DORA.

Analiza ryzyka dla bezpieczeństwa informacji to proces oceny i identyfikacji potencjalnych zagrożeń i ryzyk związanych z bezpieczeństwem danych i informacji w organizacji. Celem analizy jest zrozumienie, jakie zagrożenia mogą wystąpić, jakie konsekwencje mogą mieć dla organizacji i jakie środki ochrony można podjąć, aby zminimalizować ryzyko i skutki incydentów.

Główne kroki w procesie analizy ryzyka dla bezpieczeństwa informacji to:

- **Identyfikacja aktywów.** Pierwszym krokiem jest określenie aktywów informacyjnych, które wymagają ochrony. Mogą to być dane, systemy komputerowe, aplikacje, urządzenia, infrastruktura sieciowa, a także ludzie (np. pracownicy) zaangażowani w zarządzanie i dostęp do tych aktywów.
- **Identyfikacja zagrożeń.** Następnie identyfikuje się potencjalne zagrożenia, które mogą wpłynąć na bezpieczeństwo tych aktywów. Mogą to być ataki hakerskie, złośliwe oprogramowanie, awarie systemowe, błędy ludzkie, klęski żywiołowe itp.
- **Określenie podatności.** W tym kroku analizuje się, jakie podatności występują w systemach, aplikacjach i procesach i jak mogą one mogą ułatwić wystąpienie zagrożenia. Podatności to słabe punkty w infrastrukturze lub programach, które mogą być wykorzystane przez atakujących.
- **Ocena ryzyka.** Na podstawie zidentyfikowanych zagrożeń i podatności przeprowadza się ocenę ryzyka, czyli określenie prawdopodobieństwa wystąpienia zagrożenia oraz jego wpływu na organizację.
- **Zarządzanie ryzykiem.** Po ocenie ryzyka podejmuje się decyzje dotyczące zarządzania ryzykiem. Możliwe działania obejmują unikanie ryzyka, redukcję ryzyka, przenoszenie ryzyka na inny podmiot (np. ubezpieczyciela) lub zaakceptowanie ryzyka, jeśli jest ono akceptowalne dla organizacji.
- **Wdrażanie środków ochronnych.** Na podstawie wyników analizy ryzyka organizacja wdraża odpowiednie środki ochronne, takie jak zabezpieczenia techniczne, polityki bezpieczeństwa, szkolenia załogi itp., które pomogą zminimalizować ryzyko i zwiększyć poziom bezpieczeństwa informacji.

Analiza ryzyka dla bezpieczeństwa informacji jest procesem ciągłym i powinna być regularnie aktualizowana, aby uwzględnić nowe zagrożenia, zmiany w infrastrukturze czy wprowadzenie nowych technologii. Jest to ważny element strategii zarządzania ryzykiem i zapewnienia odpowiedniego poziomu bezpieczeństwa dla organizacji.

W bezpieczeństwie informacji istnieje kilka różnych metodyk analizy ryzyka, które pomagają organizacjom ocenić i zarządzać ryzykiem związanym z bezpieczeństwem danych i informacji. Oto niektóre z popularnych metodyk:

- **Analiza ryzyka oparta na ISO 27005.** Ta metodyka jest związana z normą ISO/IEC 27005, która określa wytyczne dotyczące zarządzania ryzykiem w bezpieczeństwie informacji. Opiera się na identyfikacji aktywów, zagrożeń, podatności i ocenie ryzyka w oparciu o skalę prawdopodobieństwa i skutków.
- **Analiza ryzyka oparta na NIST.** NIST Risk Management Framework (RMF) to podejście opracowane przez National Institute of Standards and Technology (NIST) w celu zarządzania ryzykiem związanym z bezpieczeństwem informacji w instytucjach federalnych Stanów Zjednoczonych. RMF to kompletne, wieloetapowe podejście, które pomaga organizacjom identyfikować, oceniać i zarządzać ryzykiem w kontekście bezpieczeństwa informacji i zarządzania informacją.
- **Metoda OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)**, opracowana przez Carnegie Mellon University. Koncentruje się na identyfikacji i ocenie zagrożeń związanych

z działalnością organizacji, a także analizie podatności i zarządzaniu ryzykiem w kontekście działalności operacyjnej.

Analiza ryzyka oparta na FAIR (Factor Analysis of Information Risk). FAIR jest metodyką, która skupia się na wykorzystaniu kwantytatywnych danych do analizy ryzyka. Pomaga organizacjom ocenić ryzyko w sposób liczbowy, biorąc pod uwagę czynniki takie jak prawdopodobieństwo wystąpienia incydentu, skutki finansowe i inne parametry.

Metoda FMEA (Failure Mode and Effects Analysis). Jest techniką wywodzącą się z inżynierii, ale jest również stosowana w bezpieczeństwie informacji. Polega na identyfikacji różnych sposobów wystąpienia niepowodzenia (tzw. *mode of failure*) oraz analizie wpływu tych niepowodzeń na funkcjonowanie organizacji.

Analiza ryzyka kwalitatywna i ilościowa. To podejście obejmuje zarówno ocenę ryzyka jakościowego, opartego na ocenie subiektywnych czynników i ekspertyzie, jak i analizę ryzyka ilościowego, która polega na wykorzystaniu danych liczbowych i statystycznych do oceny ryzyka.

Wybór odpowiedniej metodyki analizy ryzyka w bezpieczeństwie informacji zależy od wielu czynników, takich jak wielkość organizacji, rodzaj przetwarzanych danych, dostępne zasoby i preferencje zarządu. W niektórych przypadkach organizacje mogą wykorzystywać kombinację różnych metodyk, aby uzyskać kompleksową ocenę ryzyka i wdrożyć odpowiednie środki ochronne.

Analiza ryzyka oparta na ISO 27005

Norma ta, zatytułowana „Information technology – Security techniques – Information security risk management" zawiera wytyczne dotyczące zarządzania ryzykiem związanym z bezpieczeństwem informacji. Głównym celem jest identyfikacja, ocena i zarządzanie ryzykiem związanym z aktywami informacyjnymi i infrastrukturą IT w organizacji. Metodyka ISO 27005 skupia się na podejściu procesowym, które pozwala organizacji podejmować decyzje w zakresie bezpieczeństwa informacji.

Podstawowe kroki w analizie ryzyka opartej na ISO 27005 to:

Identyfikacja aktywów. Pierwszym krokiem jest określenie aktywów informacyjnych wymagających ochrony, takich jak dane, systemy, aplikacje, urządzenia.

Identyfikacja zagrożeń. Następnie identyfikuje się potencjalne zagrożenia, czyli źródła ryzyka, które mogą wpłynąć na bezpieczeństwo aktywów informacyjnych.

Określenie podatności. W tym etapie analizuje się słabe punkty w systemach, które mogą być wykorzystane przez zainteresowanych naruszeniem bezpieczeństwa.

Ocena ryzyka. Na podstawie zidentyfikowanych zagrożeń i podatności przeprowadza się ocenę ryzyka, czyli określenie prawdopodobieństwa wystąpienia zagrożenia oraz jego wpływu na aktywa informacyjne.

Zarządzanie ryzykiem. Po ocenie ryzyka organizacja podejmuje decyzje dotyczące zarządzania ryzykiem. Może to obejmować wdrożenie odpowiednich środków ochronnych, przeniesienie ryzyka na ubezpieczyciela, zaakceptowanie ryzyka lub unikanie ryzyka poprzez unikanie określonych działań.

Monitorowanie i aktualizacja. Analiza ryzyka jest procesem dynamicznym, dlatego ważne jest regularne monitorowanie i aktualizacja analizy ryzyka, aby uwzględnić nowe zagrożenia i zmiany w środowisku organizacyjnym.

Metodyka analizy ryzyka oparta na ISO 27005 jest używana przez wiele organizacji jako narzędzie do efektywnego zarządzania ryzykiem związanym z bezpieczeństwem informacji i dostosowywania działań ochronnych do zidentyfikowanych zagrożeń.

NIST Risk Management Framework

Główne cele NIST Risk Management Framework to:

ustanowienie procesu zarządzania ryzykiem; RMF dostarcza struktury i wytyczne w celu stworzenia skoordynowanego i powtarzalnego procesu zarządzania ryzykiem w organizacji,

skupienie na kontynuowaniu działalności; RMF pomaga organizacjom w identyfikacji i ochronie kluczowych aktywów informacyjnych, które są niezbędne do kontynuacji działalności w obliczu różnych zagrożeń,

integracja z systemem zarządzania informacją; RMF integruje podejście do zarządzania ryzykiem z ogólnym systemem zarządzania informacją w organizacji, aby zapewnić spójność i skuteczność działań.

NIST Risk Management Framework składa się z następujących faz:

Faza Kontekstualizacji. W tej fazie organizacja określa kontekst, w którym prowadzone są działania, identyfikuje cele i cele bezpieczeństwa informacji, a także określa zasoby do ochrony.

Faza Oceny. W tej fazie organizacja identyfikuje zagrożenia, podatności i ocenia ryzyko związane z jej aktywami informacyjnymi.

Faza Wybierania Środków Ochronnych. Na podstawie wyników oceny ryzyka organizacja wybiera odpowiednie środki ochrony i strategie zarządzania ryzykiem.

Faza Wdrożenia. W tej fazie organizacja wdraża wybrane środki ochrony i podejmuje działania mające na celu zminimalizowanie ryzyka.

Faza Monitorowania. Organizacja nadzoruje i analizuje skuteczność wdrożonych środków ochrony oraz ocenia nowe zagrożenia, które mogą się pojawić.

Faza Reagowania. W razie potrzeby organizacja przyjmuje odpowiednie działania w odpowiedzi na nowe zagrożenia lub incydenty.

NIST Risk Management Framework jest szeroko stosowany w agencjach rządowych Stanów Zjednoczonych, a ponadto używają go jako punkt odniesienia inne organizacje i instytucje, które chcą wdrożyć kompleksowe podejście do zarządzania ryzykiem związanym z bezpieczeństwem informacji.

ROLA ZARZĄDU W ZARZĄDZANIU RYZYKIEM W CYBERBEZPIECZEŃSTWIE ORGANIZACJI

Zarząd każdej organizacji, czy to małej firmy, czy dużej korporacji, powinien zadać sobie pytanie o swój stosunek do cyberbezpieczeństwa. To Zarząd powinien określić własny poziom akceptacji ryzyka. Dopiero na tej podstawie, po wykonaniu analizy ryzyka, powinien zostać wyznaczony cel w zakresie bezpieczeństwa informacji, przekładający się na budżet dedykowany dla jego realizacji.

Apetyt na ryzyko (ang. *risk appetite*) odnosi się do poziomu ryzyka, który jest akceptowalny dla danej organizacji lub jednostki. Jest to z góry określony zakres ryzyka, jaki organizacja jest gotowa podjąć w działaniach na rzecz realizacji swoich celów biznesowych. Wyraża się on w specyficznych terminach i wskaźnikach, które pomagają zrozumieć, jakie zagrożenia i możliwości organizacja jest skłonna zaakceptować.

Apetyt na ryzyko jest integralnym elementem zarządzania ryzykiem, ponieważ pozwala na zdefiniowanie granic i wytycznych, które pomagają organizacji podejmować decyzje dotyczące ryzyka. Poziom apetytu na ryzyko jest różny dla różnych organizacji i może się znacznie różnić w zależności od branży, rodzaju działalności i tolerancji ryzyka.

W praktyce apetyt na ryzyko może być wyrażany za pomocą różnych mierników i wskaźników, takich jak:

- maksymalna wartość strat finansowych akceptowanych przez organizację w związku z incydentem bezpieczeństwa,
- maksymalny czas przestoju usług lub systemów w wyniku ataku lub awarii,
- maksymalny poziom wystąpienia incydentów bezpieczeństwa (np. liczba ataków na miesiąc),
- maksymalny poziom ryzyka związanego z konkretnym projektem czy inicjatywą.

W celu określenia apetytu na ryzyko organizacja (Zarząd) powinna dokładnie przeanalizować swoje cele, strategie biznesowe, tolerancję ryzyka oraz potencjalne skutki wystąpienia różnych rodzajów zagrożeń. Wypracowanie spójnej polityki apetytu na ryzyko pozwala organizacji na podejmowanie bardziej świadomych decyzji dotyczących inwestycji w bezpieczeństwo i zarządzania ryzykiem.

Jeśli organizacja prowadzi sprzedaż internetową, która generuje 100 proc. jej przychodów, to ewentualna przerwa w funkcjonowaniu systemu sprzedaży będzie miała bezpośrednie przełożenie na wyniki firmy. Dla warsztatu stolarskiego produkującego meble dla jednego odbiorcy prawdopodobnie przerwa w działaniu witryny internetowej nie będzie miała przełożenia na wyniki finansowe.

Apetyt na ryzyko firmy może być kształtowany przez wiele różnych czynników. Poniżej wymieniam niektóre z kluczowych czynników, które wpływają na poziom akceptowalnego ryzyka dla organizacji:

- **Ogólne wymagania prawne.** Wymagania prawne w szczególności rozporządzenie RODO mają istotny wpływ na decyzje Zarządu w zakresie cyberbezpieczeństwa i apetyt na ryzyko (np. poziom kar wynikających z RODO).
- **Branża i rodzaj działalności.** Różne branże mają różne poziomy ryzyka związane z ich charakterystyką działalności oraz specyficznymi wymaganiami prawnymi. Na przykład branże finansowa lub opieki zdrowotnej mogą mieć mniejszy apetyt na ryzyko niż branża transportowa.
- **Cele i strategie biznesowe**. Wpływają one na poziom akceptowalnego ryzyka. Firmy dążące do szybkiego wzrostu i ekspansji mogą być bardziej skłonne podjąć większe ryzyko w porównaniu z firmami, które skupiają się na stabilności i utrzymaniu status quo.
- **Polityka zarządzania ryzykiem.** Określa ona podejście organizacji do oceny, monitorowania i zarządzania ryzykiem. Czy organizacja preferuje zachowanie, unikanie, przenoszenie czy akceptację ryzyka?
- **Poziom tolerancji ryzyka.** Poziom ten wskazuje, jak bardzo organizacja jest komfortowa z podejmowaniem ryzyka. Niektóre organizacje mogą być bardziej konserwatywne i preferować minimalizację ryzyka, podczas gdy inne mogą być bardziej innowacyjne i tolerować większe ryzyko.
- **Regulacje i wymogi prawne.** Mogą narzucać określone limity i wymagania dotyczące bezpieczeństwa i zarządzania ryzykiem, co może wpływać na apetyt na ryzyko firmy.
- **Wartość aktywów.** Wartość ta ma w organizacji istotny wpływ na decyzje dotyczące zabezpieczeń. Firmy o dużej wartości aktywów mogą być bardziej ostrożne w zakresie ryzyka, aby uniknąć potencjalnych strat finansowych.
- **Wizerunek i reputacja.** Firma, która stawia duży nacisk na swoją reputację i wizerunek, może być bardziej ostrożna w zakresie ryzyka, aby uniknąć incydentów mogących wpłynąć negatywnie na jej renomę.
- **Doświadczenia z przeszłości.** Wcześniejsze incydenty związane z bezpieczeństwem i ryzykiem mogą wpłynąć na podejście organizacji do akceptacji lub unikania pewnych ryzyk.

Łączne oddziaływanie tych czynników kształtuje apetyt na ryzyko firmy i może prowadzić do różnic w podejściu organizacji do zarządzania bezpieczeństwem i ryzykiem. Ważne jest jednak, aby apetyt ten był dobrze zdefiniowany i zrozumiany przez Zarząd oraz załogę i aby podejmowane decyzje były spójne z celami i strategią organizacji.

PROGRAM POPRAWY CYBERBEZPIECZEŃSTWA W TWOJEJ ORGANIZACJI

Dobór ram zarządzania cyberbezpieczeństwem

Istnieje wiele ram zarządzania (ang. *framework*) i standardów w dziedzinie cyberbezpieczeństwa, które organizacje i przedsiębiorstwa mogą wykorzystać do skutecznego wzmocnienia swoich praktyk bezpieczeństwa. Niektóre z najpopularniejszych to:

- **NIST Cybersecurity Framework (NIST CSF), opracowany przez National Institute of Standards and Technology (NIST**). Jest jedną z najbardziej rozpoznawalnych ram pracy w zakresie cyberbezpieczeństwa. Składa się z pięciu głównych funkcji: identyfikacji, ochrony, wykrywania, reagowania i przywracania. Framework NIST CSF pomaga organizacjom określić, ocenić i doskonalić swoje podejścia do cyberbezpieczeństwa.
- **ISO/IEC 27001.** Standard opracowany przez Międzynarodową Organizację Normalizacyjną (ISO) i Międzynarodową Elektrotechniczną Komisję

(IEC). Jest oparty na podejściu zarządzania ryzykiem i definiuje wymagania dla systemu zarządzania bezpieczeństwem informacji (ISMS). Pomaga organizacjom w identyfikacji, zarządzaniu i minimalizacji ryzyka związanego z bezpieczeństwem informacji.

CIS Controls. Center for Internet Security (CIS) opracowało 20 podstawowych kontroli bezpieczeństwa, które stanowią jednocześnie zbiór zaleceń w zakresie cyberbezpieczeństwa. Kontrole CIS pomagają organizacjom w skutecznym zabezpieczaniu systemów informatycznych przed najważniejszymi zagrożeniami.

MITRE ATT&CK. Jest to framework opisujący techniki i procedury używane przez atakujących w różnych fazach kampanii cybernetycznych. Framework ATT&CK firmy MITRE umożliwia organizacjom lepsze zrozumienie sposobów działania potencjalnych zagrożeń i dostosowanie swoich środków obronnych.

SANS Critical Security Controls (CSC). SANS Institute opracował 20 kontroli bezpieczeństwa, które pomagają organizacjom w ochronie przed zaawansowanymi zagrożeniami. Kontrole SANS CSC są oparte na praktycznych doświadczeniach i wiedzy ekspertów branżowych.

Cybersecurity Capability Maturity Model (C2M2). Jest to model oceny dojrzałości systemu cyberbezpieczeństwa opracowany przez Departament Energii Stanów Zjednoczonych. Pomaga organizacjom ocenić swoje zdolności w zakresie cyberbezpieczeństwa i zaplanować kolejne ulepszenia.

NIST Risk Management Framework (RMF). To podejście do zarządzania ryzykiem oparte na cyklu życia, które pomaga organizacjom w identyfikacji, ocenie, wybieraniu i monitorowaniu kontroli bezpieczeństwa informacji. Jest stosowane głównie w sektorze rządowym i organizacjach z nim związanych, gdzie ochrona informacji i danych jest krytycznym aspektem działalności.

Dokumenty te stanowią tylko wycinek dostępnych rozwiązań w zakresie cyberbezpieczeństwa. Wybór odpowiedniego standardu zależy od specyficznych potrzeb, rodzaju działalności i wymogów regulacyjnych, które organizacja musi spełnić. Decyzję o wyborze tych, na których będzie się opierać, powinien podjąć zarząd na podstawie rekomendacji CISO. Często wybór może być podyktowany specyfiką obszaru działalności czy regulacji prawnych.

Przykładowy program poprawy cyberbezpieczeństwa

Każda firma, niezależnie od swojej wielkości, powinna zdefiniować i wdrożyć program poprawy bezpieczeństwa. Taki program poprawy to zestaw działań i inicjatyw mających na celu wzmocnienie poziomu bezpieczeństwa informacji i ochronę przed zagrożeniami związanymi z cyberprzestępczością. Może on być skonstruowany w odpowiedzi na wykryte luki w zabezpieczeniach, bieżące zagrożenia oraz potrzeby organizacji w zakresie ochrony poufności, integralności i dostępności danych. Obejmuje różnorodne działania, które mogą być wdrażane etapami, aby osiągnąć coraz wyższy poziom cyberbezpieczeństwa.

Konstrukcja programów bezpieczeństwa opisana jest w wymienionych w tym opracowaniu frameworkach i standardach. Istotne jest, aby to Zarząd podjął decyzję o rozpoczęciu programu poprawy bezpieczeństwa, zaplanował budżet na te działania i w miarę możliwości wybrał jeden z dostępnych frameworków.

Niezależnie od powyższego, każdy z frameworków zawiera kluczowe elementy, które muszą wystąpić, aby zapewnić minimum skuteczności działań. I tak, kluczowe elementy każdego programu poprawy cyberbezpieczeństwa w firmie to:

OCENA RYZYKA I AUDYT BEZPIECZEŃSTWA

- Przeprowadzenie analizy ryzyka, aby zidentyfikować potencjalne zagrożenia i słabe punkty w infrastrukturze i procesach.
- Przeprowadzenie audytów bezpieczeństwa w celu zrozumienia bieżącej sytuacji i identyfikacji obszarów wymagających ulepszenia.

POLITYKI I PROCEDURY BEZPIECZEŃSTWA

- Wprowadzenie i wdrożenie spójnych polityk i procedur dotyczących cyberbezpieczeństwa w całej organizacji.
- Zapewnienie, że pracowniczki i pracownicy są ich świadomi i przestrzegają zasad bezpieczeństwa.

SZKOLENIA I EDUKACJA PRACOWNIKÓW

- Stałe organizowanie szkoleń i sesji edukacyjnych, aby podnieść świadomość pracowniczek i pracowników w zakresie cyberbezpieczeństwa i zwiększyć ich zdolność rozpoznawania zagrożeń.

ZABEZPIECZENIA TECHNICZNE

- Wdrożenie rozwiązań technologicznych, takich jak zapory sieciowe, antywirusy, systemy wykrywania intruzów (IDPS) czy też szyfrowanie danych.
- Aktualizacja i łatanie oprogramowania w celu wyeliminowania znanych podatności.

ZARZĄDZANIE TOŻSAMOŚCIĄ I DOSTĘPEM

- Wprowadzenie mechanizmów zarządzania tożsamością i dostępem, takich jak jednokrotne logowanie (SSO) i wieloskładnikowe uwierzytelnianie.

MONITOROWANIE I ANALIZA ZDARZEŃ BEZPIECZEŃSTWA

- Wdrożenie systemów monitorowania zdarzeń, które pozwalają na wykrywanie podejrzanych aktywności i reagowanie na nie.

PLANOWANIE CIĄGŁOŚCI DZIAŁANIA

- Opracowanie planów ciągłości działania i odzyskiwania danych po awariach czy incydentach związanych z cyberbezpieczeństwem.

TESTY I ĆWICZENIA

- Regularne przeprowadzanie testów penetracyjnych oraz ćwiczeń na wypadek wystąpienia incydentu, aby ocenić skuteczność zabezpieczeń i procedur reagowania.

MONITORING I DOSKONALENIE

- Ciągłe monitorowanie efektywności programu poprawy cyberbezpieczeństwa i wprowadzanie ulepszeń w miarę zdobywania nowych doświadczeń i informacji o zagrożeniach.

ROLA OSÓB ZATRUDNIONYCH W ORGANIZACJI W POPRAWIE JEJ CYBERBEZPIECZEŃSTWA

Zarząd firmy, wdrażając procesy bezpieczeństwa danych w firmie, musi zdawać sobie sprawę, że z tej perspektywy najsłabszym, ale jednocześnie najważniejszym ogniwem w organizacji jest załoga. Pracowniczki i pracownicy odpowiadają za realizację wszystkich procesów, dysponują dostępem do zasobów informatycznych firmy, a także mają przypisany większy lub mniejszy poziom decyzyjności.

Zatrudnieni mający dostęp do zasobów informacyjnych stanowią potencjalne „słabe ogniwo" w procesie zapewnienia bezpieczeństwa. Wśród najważniejszych przyczyn można wymienić:

Brak świadomości zagrożeń. Wielu zatrudnionych może nie być świadomych zagrożeń związanych z obszarem ani tego, jakie praktyki bezpieczeństwa powinni stosować w swojej pracy. To może prowadzić do nieostrożnych działań, które ułatwiają cyberprzestępcom włamanie się do systemów.

Społeczny inżyniering. Atakujący często wykorzystują techniki społecznego inżynieringu, aby oszukać pracowniczki i pracowników i zdobyć dostęp do poufnych informacji. Może to obejmować phishing (przesyłanie fałszywych e-maili), podszywanie się pod zaufane osoby lub firmy oraz manipulowanie zatrudnionymi w celu ujawnienia poufnych danych.

Brak zabezpieczeń wewnętrznych. Załoga może nie być wystarczająco odpowiedzialna w zakresie zabezpieczeń wewnętrznych, takich jak utrzymywanie silnych haseł, zamykanie sesji, unikanie korzystania z niezaufanych urządzeń itp.

Ryzykowne zachowania online. Niektórzy z zatrudnionych mogą podejmować ryzykowne działania online, takie jak korzystanie z niezaufanych stron internetowych, pobieranie podejrzanych plików lub klikanie w podejrzane linki, co może prowadzić do infekcji złośliwym oprogramowaniem.

Utrata lub kradzież urządzeń. Pracowniczki i pracownicy mogą być podatni na utratę urządzeń przenośnych, takich jak telefony komórkowe lub laptopy, które mogą zawierać poufne dane. W przypadku kradzieży lub utraty tych urządzeń, dane mogą wpaść w niepowołane ręce.

Przywileje dostępu. Pracowniczki i pracownicy z wysokimi przywilejami dostępu do systemów i danych są bardziej narażeni na wykorzystanie przez cyberprzestępców do celów włamania się i kradzieży poufnych informacji.

Ważne jest, aby organizacje inwestowały w edukację zatrudnionych w zakresie świadomości cyberbezpieczeństwa oraz wdrażały odpowiednie procedury i polityki, aby zminimalizować ryzyko, jakie mogą stanowić pracowniczki i pracownicy dla bezpieczeństwa informacji w firmie. Regularne szkolenia, monitorowanie aktywności i egzekwowanie zasad bezpieczeństwa są podstawą w ochronie przed zagrożeniami związanymi z czynnikiem ludzkim. Całość działań opisanych powyżej określa się mianem „poprawy świadomości pracowniczek i pracowników".

Poprawa świadomości pracowników w zakresie cyberbezpieczeństwa

Świadomi zagrożeń zatrudnieni są bardziej zdolni do rozpoznawania i unikania zagrożeń związanych z cyberprzestępczością, co może znacznie zmniejszyć ryzyko wystąpienia incydentów w tym obszarze. Oto kilka kroków, które można podjąć w celu poprawy świadomości pracowników w zakresie cyberbezpieczeństwa:

Szkolenia w zakresie cyberbezpieczeństwa. Ważne jest organizowanie regularnych kursów, warsztatów i sesji edukacyjnych dotyczące cyberbezpieczeństwa z udziałem wszystkich zatrudnionych. Szkolenia powinny skupiać się na zagrożeniach takich jak phishing, ransomware, hasła, zasady bezpiecznego korzystania z urządzeń itp.

Polityki i procedury. Istotne jest, aby upewnić się, że w firmie istnieją jasne i zrozumiałe polityki bezpieczeństwa informacji oraz procedury postępowania w przypadku wystąpienia zagrożeń. Pracowniczki i powinni dobrze znać te polityki i procedury.

Egzekwowanie zasad bezpieczeństwa. Ważne jest wprowadzenie systemu egzekwowania zasad bezpieczeństwa i odpowiedzialności za nieprzestrzeganie zasad. Pracowniczki i pracownicy powinni rozumieć, że bezpieczeństwo informacji jest wspólnym obowiązkiem i każdy musi brać w nim udział.

Testy wewnętrzne. Konieczne jest przeprowadzanie regularnych testów wewnętrznych, takich jak symulacje phishingu, aby ocenić poziom świadomości załogi i zidentyfikować obszary wymagające dodatkowej edukacji.

Powiadomienia o zagrożeniach. Trzeba informować pracowniczki i pracowników o aktualnych zagrożeniach i ostrzeżeniach związanych z cyberbezpieczeństwem. Powiadomienia powinny być skuteczne i trafiać do adresatów w odpowiednim czasie.

Nagrody i uznania. Wskazane jest motywowanie zespołów pracowniczych do przestrzegania zasad bezpieczeństwa poprzez wprowadzenie programu nagradzania za bezpieczne zachowania i reagowanie na zagrożenia.

Partnerstwo z pracowniczkami i pracownikami. Bardzo przydaje się zaangażowanie załóg w proces poprawy świadomości cyberbezpieczeństwa, zachęcanie zatrudnionych do zgłaszania podejrzanych aktywności i pomysłów na zwiększenie bezpieczeństwa.

Poprawa świadomości zespołów pracowniczych w zakresie cyberbezpieczeństwa wymaga systematycznego i konsekwentnego podejścia. Wprowadzenie odpowiednich działań edukacyjnych i zabezpieczeń może znacznie zmniejszyć ryzyko wystąpienia incydentów i wzmocnić cyberbezpieczeństwo całej firmy.

Ścieżki szkoleniowe z cyberbezpieczeństwa

Szkolenie z cyberbezpieczeństwa dla zatrudnionych może obejmować kilka etapów, które pozwalają stopniowo zwiększać ich świadomość i umiejętności w tym zakresie. Oto przykładowa ścieżka szkolenia:

PODSTAWY CYBERBEZPIECZEŃSTWA

- wstępne wprowadzenie do zagadnień związanych z cyberbezpieczeństwem,
- znaczenie bezpieczeństwa informacji dla organizacji,
- rozpoznawanie podstawowych zagrożeń, takich jak phishing i malware.

BEZPIECZNE PRAKTYKI W KORZYSTANIU Z URZĄDZEŃ I KONT

- zasady tworzenia silnych haseł i zarządzania nimi,
- bezpieczne logowanie i wylogowywanie się z kont i systemów,
- bezpieczne korzystanie z urządzeń mobilnych i publicznych sieci Wi-Fi.

ROZPOZNAWANIE ZAGROŻEŃ ONLINE

- rozpoznawanie prób phishingu i oszustw w e-mailach i wiadomościach,
- rozpoznawanie podejrzanych linków i załączników,
- zasady bezpiecznego pobierania plików i oprogramowania.

BEZPIECZNE PRAKTYKI W PRACY ZDALNEJ

- zasady związane z bezpiecznym korzystaniem z VPN (wirtualnych sieci prywatnych) i zdalnego dostępu,
- bezpieczeństwo pracy w miejscach publicznych i poza biurem.

OCHRONA DANYCH I POUFNOŚĆ INFORMACJI

- zasady ochrony poufnych informacji i danych klientek i klientów,
- bezpieczne przechowywanie i przesyłanie poufnych danych.

ZARZĄDZANIE INCYDENTAMI

- procedury raportowania i reagowania na podejrzane aktywności,
- jak zgłaszać incydenty bezpieczeństwa w organizacji.

OCHRONA PRZED ZAGROŻENIAMI SPECYFICZNYMI DLA BRANŻY

- Dodatkowe zagrożenia i wyzwania związane z bezpieczeństwem w konkretnej branży.

KONTYNUACJA EDUKACJI I AKTUALIZACJE

- regularne szkolenia i uzupełnianie wiedzy na temat nowych zagrożeń i technik cyberataków,
- dostęp do aktualnych materiałów i źródeł informacji na temat cyberbezpieczeństwa.

Ważne jest, aby szkolenia były regularne i dostosowane do potrzeb firmy. Tylko wtedy zatrudnieni będą mogli doskonalić swoje umiejętności. Dodatkowo organizacja może wykorzystać testy wewnętrzne i symulacje, takie jak symulacje phishingu, aby ocenić skuteczność szkoleń i poziom świadomości swoich zespołów pracowniczych..

Przykładowa ścieżka szkoleniowa dla administrujących systemami pod kątem cyberbezpieczeństwa

PODSTAWY CYBERBEZPIECZEŃSTWA

- wprowadzenie do podstawowych pojęć i terminów związanych z cyberbezpieczeństwem,
- znaczenie roli administratora w ochronie infrastruktury IT.

BEZPIECZEŃSTWO SYSTEMÓW OPERACYJNYCH

- zasady bezpiecznej konfiguracji systemów operacyjnych (np. Windows, Linux),
- zarządzanie kontami i uprawnieniami oraz zdalnym dostępem do serwerów.

OCHRONA SIECI

- bezpieczna konfiguracja urządzeń sieciowych, takich jak routery i firewalle,
- monitorowanie ruchu sieciowego w celu wykrywania nieprawidłowości,
- zastosowanie zabezpieczeń przeciwko atakom typu DDoS.

ZARZĄDZANIE INCYDENTAMI I LOGAMI

- procedury reagowania na incydenty bezpieczeństwa,
- analiza logów w celu wykrywania podejrzanych aktywności i audyty bezpieczeństwa.

ZABEZPIECZANIE APLIKACJI

- zapewnienie bezpieczeństwa aplikacji, takich jak serwery WWW i bazy danych,
- zarządzanie podatnościami aplikacji i ich łatanie,
- wdrażanie zasad związanych z bezpiecznym programowaniem,
- ochrona poufności danych i zarządzanie kluczami szyfrującymi,
- zabezpieczenie danych w przechowywaniu i przesyłaniu,
- planowanie i testowanie kopii zapasowych danych.

ZABEZPIECZANIE URZĄDZEŃ MOBILNYCH

- bezpieczeństwo urządzeń mobilnych używanych przez pracowniczki i pracowników,
- polityki BYOD (Bring Your Own Device) i zabezpieczenie danych firmowych.

CERTYFIKACJE BRANŻOWE

- zdobycie certyfikacji związanych z cyberbezpieczeństwem, takich jak CompTIA Security+, Certified Information Systems Security Professional (CISSP) lub Certified Ethical Hacker (CEH).

Ważne jest, aby szkolenie administratorek i administratorów było odpowiednio zaawansowane i zgodne z wymaganiami branżowymi i regulacjami. Osoby te odgrywają kluczową rolę w ochronie infrastruktury IT i danych organizacji. Dlatego konieczne jest, aby byli odpowiednio przeszkoleni i świadomi najnowszych zagrożeń i praktyk bezpieczeństwa.

Przykładowa ścieżka szkoleniowa dla audytora cyberbezpieczeństwa

Taka ścieżka skupiałaby się na umiejętnościach i wiedzy potrzebnych do przeprowadzania audytów związanych z bezpieczeństwem informacji i cyberbezpieczeństwem.

PODSTAWY CYBERBEZPIECZEŃSTWA

- wprowadzenie do podstawowych pojęć i terminów związanych z cyberbezpieczeństwem,
- zrozumienie podstawowych zagrożeń i wyzwań związanych z bezpieczeństwem informacji.

STANDARDY I REGULACJE ZWIĄZANE Z CYBERBEZPIECZEŃSTWEM

- zapoznanie się z międzynarodowymi standardami i regulacjami dotyczącymi cyberbezpieczeństwa, takimi jak ISO/IEC 27001, NIST Cybersecurity Framework, GDPR itp.

PROCESY I PROCEDURY AUDYTU

- zrozumienie procesów audytu i metodologii oceny ryzyka,
- wykorzystanie narzędzi i technik audytorskich w kontekście cyberbezpieczeństwa.

AUDYT INFRASTRUKTURY IT I ARCHITEKTURY

- przeglądanie i ocena infrastruktury IT, w tym sieci, serwerów, urządzeń mobilnych i urządzeń końcowych,
- ocena zabezpieczeń fizycznych i logicznych.

AUDYT APLIKACJI I SYSTEMÓW

- analiza i ocena zabezpieczeń aplikacji, w tym aplikacji internetowych i baz danych,
- ocena bezpieczeństwa systemów operacyjnych i oprogramowania.

ZARZĄDZANIE RYZYKIEM I PLANOWANIE CIĄGŁOŚCI DZIAŁANIA

- ocena procedur zarządzania ryzykiem organizacji,
- planowanie i testowanie planów ciągłości działania w razie incydentu.

AUDYT ZGODNOŚCI I POLITYK BEZPIECZEŃSTWA

- ocena zgodności organizacji z odpowiednimi standardami, regulacjami i politykami bezpieczeństwa,
- weryfikacja czy polityki bezpieczeństwa są odpowiednio wdrożone i przestrzegane.

ZARZĄDZANIE INCYDENTAMI I REAGOWANIE NA NARUSZENIA

- zapoznanie się z procedurami reagowania na incydenty bezpieczeństwa,
- ocena jak organizacja reaguje na wystąpienie naruszeń i próby włamań.

PRAKTYCZNE ĆWICZENIA AUDYTORSKIE

- praktyczne szkolenia i ćwiczenia audytorskie, które pozwalają praktykować umiejętności zdobyte podczas szkolenia.

CERTYFIKACJE AUDYTORSKIE

- ukończenie odpowiednich certyfikacji branżowych z zakresu audytu, takich jak Certified Information Systems Auditor (CISA) bądź uzyskanie certyfikacji Audytora Wiodącego ISO 27001 lub ISO 22301.

Aby zapewnić audytorkom i audytorom odpowiednie umiejętności i wiedzę potrzebną do oceny i analizy poziomu bezpieczeństwa organizacji, szkolenie dla nich powinno uwzględniać zarówno teorię, jak i praktykę. Świadomość zagrożeń i bieżących trendów w cyberbezpieczeństwie jest kluczowym elementem skutecznych audytów w zakresie bezpieczeństwa informacji.

OPIS RÓL I KOMPETENCJI CYBERBEZPIECZEŃSTWA W ORGANIZACJI

Istnieje wiele ról i funkcji w dziedzinie cyberbezpieczeństwa, które są niezbędne w celu zapewnienia ochrony przedsiębiorstwa przed zagrożeniami cybernetycznymi, utrzymania ciągłości działania i zabezpieczenia wrażliwych danych klientów i pracowników. W miarę jak zagrożenia cybernetyczne ewoluują, także role i funkcje w dziedzinie cyberbezpieczeństwa ciągle się rozwijają, aby dostosować się do nowych wyzwań.

Dominującym obecnie trendem w zarządzaniu cyberbezpieczeństwem jest podejście polegające na określeniu ról w organizacji, zakresu ich obowiązków i wymaganych przez te role kompetencji. Ma ono swoje odzwierciedlenie w dominujących standardach, normach oraz w tzw. frameworkach, m.in. we wskazywanym tu kilkakrotnie Workforce Framework for Cybersecurity (NICE Framework) czy European Cybersecurity Skills Framework (ECSF) – promowanym przez organizację unijną ENISA.

W ramach dobrych praktyk warto, aby podmioty zatrudniające więcej niż 50 osób powołały przynajmniej funkcję CISO (opisana poniżej). To pozwoli w sposób zorganizowany kreować i koordynować politykę bezpieczeństwa informacji w firmie.

Katalog ról podstawowych dla cyberbezpieczeństwa

Administrator bezpieczeństwa to specjalistka lub specjalista (administrator) ds. utrzymania infrastruktury oraz zabezpieczeń informatycznych w organizacjach, w tym w przedsiębiorstwach. Ich obowiązki mogą obejmować konfigurację, zarządzanie i monitorowanie systemów bezpieczeństwa, takich jak zapory ogniowe, systemy wykrywania intruzów (IDS) i systemy zapobiegania włamaniom (IPS); instalację i aktualizację oprogramowania antywirusowego oraz innych narzędzi zabezpieczających; regularne tworzenie kopii zapasowych danych w celu zapewnienia ochrony przed ich utratą. W większym przedsiębiorstwie zadania te mogą zostać podzielone na role o szczególnych kompetencjach, w tym:

- **Inżynier ds. bezpieczeństwa sieci** (network security engineer) to specjalistka lub specjalista, który projektuje, implementuje i zarządza zabezpieczeniami sieciowymi, w tym zaporami sieciowymi, detekcją intruzów, kontrolą dostępu itp.
- **Inżynier ds. bezpieczeństwa aplikacji** (application security engineer) zajmuje się zapewnieniem bezpieczeństwa aplikacji i oprogramowania organizacji. Przeprowadza audyty kodu, testy penetracyjne i wprowadza środki bezpieczeństwa w procesie tworzenia oprogramowania.

Specjalista pierwszej linii wsparcia SOC (L1) to ekspertka lub ekspert ds. bezpieczeństwa obserwujący alerty i określający poziom krytyczności każdego z nich (kategoryzuje je), a kiedy zachodzi taka potrzeba, to dokonuje eskalacji do poziomu drugiego. Personel poziomu L1 może również zarządzać narzędziami bezpieczeństwa (np. firewallami) i generować regularne raporty. Specjalistka lub specjalista pierwszej linii wsparcia SOC może pełnić funkcję administratora bezpieczeństwa, czyli zarządzać i konfigurować zapory ogniowe, systemy IDS, IPS, DLP, aktualizować oprogramowanie antywirusowe czy wykonywać lub kontrolować wykonanie kopii bezpieczeństwa.

Specjalista drugiej linii SOC (L2), często nazywany z angielskiego „Incident Responder", to osoba mająca zwykle większą wiedzę niż specjalista poziomu L1. Dzięki temu może szybko dotrzeć do źródła problemu (incydentu) i ocenić, które systemy zostały dotknięte atakiem oraz jego zakres (skalę). Specjalista L2 śledzi zewnętrzne źródła informacji o zagrożeniach i podatnościach.

Specjalista trzeciej linii SOC, często nazywany z angielskiego „Threat Hunter", to wysokiej klasy ekspertka lub ekspert – analityk bezpieczeństwa. Wyszukuje aktywnie podejrzane zachowania oraz testuje i dokonuje oceny bezpieczeństwa sieci w celu wykrywania zaawansowanych zagrożeń, a także identyfikuje słabe punkty i niewystarczająco chronione zasoby. W tej grupie można znaleźć również specjalistów takich jak śledczy, audytorzy zgodności czy analitycy cyberbezpieczeństwa. Dodatkowo w Linii L3 mogą pracować architekci bezpieczeństwa, którzy projektują cały system bezpieczeństwa i jego procesy oraz integrują różne komponenty technologiczne i zasoby ludzkie.

Audytor wewnętrzny cyberbezpieczeństwa. Jej lub jego głównym zadaniem jest ocena i analiza skuteczności systemów bezpieczeństwa informacji, polityk, procedur oraz praktyk w zakresie ochrony danych i zasobów cyfrowych. Główne role i odpowiedzialność audytora wewnętrznego cyberbezpieczeństwa obejmują:

- **Przeprowadzanie audytów bezpieczeństwa.** Audytorzy wewnętrzni cyberbezpieczeństwa wykonują niezależne oceny systemów informatycznych, infrastruktury sieciowej i innych aspektów związanych z bezpieczeństwem danych. Oceny te mają na celu identyfikację potencjalnych zagrożeń i luk w zabezpieczeniach.
- **Monitorowanie zgodności.** Audytorzy sprawdzają, czy organizacja przestrzega obowiązujących standardów i przepisów dotyczących bezpieczeństwa informacji, takich jak RODO, ISO 27001 czy inne odpowiednie regulacje.
- **Ocenianie polityk i procedur.** Audytorzy analizują i oceniają skuteczność polityk bezpieczeństwa i procedur w organizacji sprawdzając, czy są odpowiednio dostosowane do bieżących zagrożeń i potrzeb organizacji.
- **Identyfikacja ryzyka.** Audytorzy identyfikują potencjalne ryzyka związane z cyberbezpieczeństwem oraz rekomendują odpowiednie środki zaradcze w celu minimalizacji tych zagrożeń.
- **Raportowanie i rekomendacje.** Po przeprowadzeniu audytu audytorzy przygotowują raporty, które zawierają wnioski i zalecenia dotyczące poprawy bezpieczeństwa informacji w organizacji. Raporty te przekazywane są zwykle kierownictwu, aby podjęto działania naprawcze.
- **Edukacja i szkolenia.** Audytorzy wewnętrzni mogą również prowadzić szkolenia dla pracowników organizacji w zakresie bezpiecznych praktyk w obszarze cyberbezpieczeństwa.

CISO (Chief Information Security Officer) to w organizacji najwyższa rangą specjalistka lub specjalista ds. bezpieczeństwa informacji. CISO pełni kluczową rolę w zarządzaniu i zapewnianiu ochrony danych, zasobów i infrastruktury organizacji przed zagrożeniami związanymi z bezpieczeństwem informacji, w tym atakami cybernetycznymi. CISO ma sprawić, że organizacja jest odpowiednio chroniona przed zagrożeniami związanymi z cyberbezpieczeństwem i że stosowane są odpowiednie środki zaradcze w celu minimalizacji ryzyka. Jest to stanowisko wymagające szerokiej wiedzy z zakresu technologii, bezpieczeństwa informatycznego oraz umiejętności zarządzania ryzykiem i ludźmi. Główne pola odpowiedzialności CISO to:

- **Zarządzanie strategią bezpieczeństwa informacji.** CISO jest odpowiedzialny za opracowywanie i wdrażanie strategii oraz polityk bezpieczeństwa informacji w organizacji. Współpracuje z kierownictwem w celu zapewnienia, że polityki bezpieczeństwa odpowiadają celom biznesowym i uwzględniają obowiązujące przepisy.
- **Ochrona przed zagrożeniami.** CISO identyfikuje, analizuje i ocenia potencjalne zagrożenia dla bezpieczeństwa informacji w organizacji. Tworzy plany zarządzania ryzykiem oraz wdraża odpowiednie rozwiązania techniczne i proceduralne w celu minimalizacji ryzyka.
- **Zarządzanie programem bezpieczeństwa.** CISO nadzoruje i koordynuje program bezpieczeństwa informacji w organizacji. Obejmuje to zarządzanie zespołem bezpieczeństwa, wdrażanie technologii zabezpieczających i innych środków bezpieczeństwa, a także organizację szkoleń dla pracowników.
- **Reagowanie na incydenty.** CISO jest odpowiedzialny za koordynowanie procesu reagowania na incydenty bezpieczeństwa, takie jak ataki hakerskie, wycieki danych czy naruszenia zabezpieczeń. Jeśli jest to możliwe, CISO dysponuje zespołem SOC obejmującym pierwszą (L1), drugą (L2) i trzecią (L3) linię wsparcia.
- **Monitorowanie i analiza.** CISO nadzoruje monitorowanie aktywności sieciowej i systemów w celu wykrywania podejrzanych lub nietypowych zachowań. Analizuje dane dotyczące bezpieczeństwa, aby identyfikować trendy i wzorce, które mogą wskazywać na potencjalne zagrożenia.
- **Zgodność i audyty.** CISO dba o spełnienie wymagań dotyczących bezpieczeństwa informacji, takich jak standardy branżowe i przepisy prawne. Przeprowadza audyty wewnętrzne i współpracuje z audytorami zewnętrznymi, aby ocenić i potwierdzić zgodność z wytycznymi bezpieczeństwa.
- **Komunikacja i świadomość.** CISO jest odpowiedzialny za komunikację z kierownictwem i pracownikami organizacji w sprawach związanych z bezpieczeństwem informacji. Wspiera działania edukacyjne mające na celu zwiększenie świadomości pracowników na temat bezpiecznych praktyk w zakresie cyberbezpieczeństwa.

Inspektor Ochrony Danych Osobowych to osoba powoływana przez administratora lub podmiot przetwarzający do pomocy przy przestrzeganiu w firmie lub organizacji przepisów o ochronie danych osobowych. IODO pełni rolę pośrednika pomiędzy zainteresowanymi podmiotami (Urzędem Ochrony Danych Osobowych, podmiotem przetwarzającym dane oraz osobą, której dane są przetwarzane). Ponadto Inspektor zapewnia realizację zasady rozliczalności. Pomaga przy sporządzaniu oceny ryzyka czy oceny skutku ochrony danych osobowych.

Główne odpowiedzialności IODO to:

- informowanie administratora, podmiotu przetwarzającego oraz pracowników o obowiązkach w zakresie ochrony danych osobowych wynikających z RODO,
- doradzanie zarządowi i kadrze kierowniczej, jak przestrzegać przepisów o ochronie danych osobowych,

- monitorowanie przestrzegania przepisów, polityk w zakresie ochrony danych osobowych,
- wsparcie przy sporządzaniu oceny ryzyka lub oceny skutków dla ochrony danych osobowych,
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego. Na terenie Rzeczypospolitej Polskiej organem nadzorczym, którego kompetencje określa RODO oraz krajowa Ustawa o ochronie danych osobowych, jest Prezes Urzędu Ochrony Danych Osobowych.

Łączenie ról cyberbezpieczeństwa i obszaru IT

Role w obszarze cyberbezpieczeństwa zasadniczo nie powinny być łączone z rolami odpowiedzialnymi za obszar IT. W szczególności dyskusyjną kwestią jest łączenie roli CISO i dyrektorki / dyrektora obszaru IT.

Tylko w niektórych sytuacjach można dopuścić pełnienie roli CISO (Chief Information Security Officer) i Dyrektora IT (IT Director) przez jedną osobę. Decyzja o połączeniu tych dwóch ról zależy od wielu czynników, takich jak wielkość organizacji, budżet, złożoność infrastruktury IT, wymagania dotyczące bezpieczeństwa, dostępność odpowiednich zasobów ludzkich itp.

W mniejszych przedsiębiorstwach lub organizacjach, które nie dysponują dużymi zespołami i budżetami na dział IT i cyberbezpieczeństwo, połączenie tych ról może być nieuniknione. Osoba pełniąca funkcję CISO i Dyrektora IT ma szerszy zakres odpowiedzialności, zarządzając zarówno aspektami bezpieczeństwa, jak i infrastrukturą techniczną organizacji.

Jednak połączenie ról CISO i dyrektorki / dyrektora IT może być trudne w większych organizacjach lub w tych, które mają bardziej skomplikowaną infrastrukturę i zaawansowane wymagania w zakresie cyberbezpieczeństwa. W takich przypadkach posiadanie oddzielnych osób na stanowisku CISO i szefa IT zapewni lepszą specjalizację, głębszą wiedzę branżową i skuteczniejsze zarządzanie.

Warto również zauważyć, że rolą CISO jest skuteczna ochrona cyberbezpieczeństwa organizacji, podczas gdy Dyrektorka / Dyrektor IT jest odpowiedzialny za zarządzanie jej technologią informatyczną. Czasami te dwie funkcje mogą mieć nieco inne cele i priorytety, a to jest trudne do zrealizowania przez jedną osobę.

Ostateczna decyzja o łączeniu obu tych ról powinna być podjęta na podstawie unikalnych potrzeb i wymagań każdej organizacji oraz dostępności odpowiednich zasobów. W większych przedsiębiorstwach bardziej korzystne będzie posiadanie oddzielnych osób na tych stanowiskach. Ostateczną decyzję w tej sprawie powinien podjąć Zarząd firmy.

TECHNOLOGIE W ARCHITEKTURZE BEZPIECZEŃSTWA ORGANIZACJI

W ramach budowy bezpiecznej architektury w organizacji warto rozważyć zastosowanie przynajmniej wybranych technologii opisanych poniżej. Jest to zestaw niezbędny, choć może okazać się niewystarczający do zapewniania podstawowego poziomu bezpieczeństwa.

Docelowa architektura bezpieczeństwa powinna być odzwierciedleniem wyników analizy ryzyka wykonanej w przedsiębiorstwie, choć zdajemy sobie sprawę, że większość mniejszych podmiotów gospodarczych nie podejmuje takiego wysiłku.

Separacja sieci, zwana również izolacją sieci lub sieciowym podziałem na segmenty, oznacza praktyki fizycznego lub logicznego dzielenia sieci komputerowych na mniejsze, odizolowane podsieci. Celem takiej separacji jest ograniczenie dostępu do zasobów i danych tylko dla wybranych użytkowników lub urządzeń, a także minimalizacja ryzyka ataków na całą sieć w przypadku kompromitacji jednego z segmentów.

Istnieje kilka powodów, dla których organizacje stosują separację sieci:

- **Bezpieczeństwo.** Separacja sieci jest jednym z kluczowych środków zapewniania bezpieczeństwa w środowiskach informatycznych. Poprzez izolację różnych segmentów, ogranicza się możliwość ruchu sieciowego między nimi, co utrudnia niepowołany dostęp do wrażliwych danych lub zasobów.
- **Kontrola dostępu.** Podział sieci pozwala na precyzyjne zarządzanie dostępem do różnych części infrastruktury. Pozwala nadawać odpowiednie uprawnienia wybranym użytkownikom i urządzeniom, zgodnie z ich funkcją i potrzebami.
- **Ograniczenie rozprzestrzeniania** się zagrożeń. W przypadku ataku lub infekcji złośliwym oprogramowaniem separacja sieci może pomóc w ograniczeniu rozprzestrzeniania się tego zagrożenia na inne części infrastruktury.
- **Wymagania regulacyjne.** W niektórych branżach, takich jak opieka zdrowotna czy finanse, istnieją regulacje wymagające fizycznego rozdzielenia danych, np. między sieciami obsługującymi pacjentów a administracyjnymi.

W zależności od wielkości i złożoności organizacji separacja sieci może być wdrażana w różny sposób. Może obejmować podział sieci na fizyczne podsieci, wirtualne sieci LAN (VLAN) czy też stosowanie specjalnych urządzeń, takich jak firewalle, które kontrolują przepływ ruchu między segmentami.

Warto podkreślić, że separacja sieci jest tylko jednym ze środków zabezpieczających i nie gwarantuje pełnego bezpieczeństwa. Dla zapewnienia kompleksowego bezpieczeństwa sieci niezbędne są również dobre praktyki w zakresie zarządzania dostępem, monitorowania ruchu sieciowego i wdrażania aktualizacji.

Zasada minimalnych uprawnień, znana również jako zasada najmniejszych przywilejów (ang. *principle of least privilege*) mówi, że każdy użytkownik lub proces powinien mieć przyznane jedynie te uprawnienia i dostęp do zasobów, które są niezbędne do wykonywania jego określonych zadań. I nic ponadto.

Główne zalety zasady minimalnych uprawnień to:

- **Ograniczenie ryzyka.** Poprzez przyznawanie minimalnych uprawnień ogranicza się możliwość nieautoryzowanego dostępu do systemu lub danych. W przypadku ataku czy kompromitacji jednego użytkownika potencjalne szkody są ograniczone do jego pola odpowiedzialności.
- **Zwiększenie bezpieczeństwa.** Zasada ta pomaga zminimalizować możliwość popełnienia błędów przez użytkowników lub procesy mające dostęp do funkcji lub danych, których nie potrzebują.

Ułatwienie audytu. Dzięki minimalnym uprawnieniom łatwiej jest śledzić, kto ma dostęp do jakich zasobów i jakie operacje są wykonywane. A to ułatwia audyt i identyfikację potencjalnych zagrożeń.

Wspieranie zasady „need-to-know". Zasada minimalnych uprawnień jest związana z zasadą „need-to-know", która mówi, że użytkownicy powinni mieć dostęp tylko do informacji, które są niezbędne do wykonywania ich pracy.

Wdrożenie zasady minimalnych uprawnień jest więc ważnym elementem strategii bezpieczeństwa informatycznego i pomaga zminimalizować potencjalne ryzyko związane z nieautoryzowanym dostępem do danych czy naruszeniem bezpieczeństwa systemu. Administratorki i administratorzy systemów powinni dbać o regularne przeglądy i analizy uprawnień, aby upewnić się, że są one nadane zgodnie z zasadą „need-to-know".

Zapora sieciowa (ang. *firewall*) to element infrastruktury sieciowej lub oprogramowania, który służy do monitorowania i kontrolowania ruchu sieciowego między różnymi sieciami, na przykład między siecią lokalną (LAN) a Internetem. Celem zapór sieciowych jest zabezpieczenie sieci przed nieautoryzowanym dostępem, atakami oraz niepożądanym ruchem sieciowym.

Zapory sieciowe działają na zasadzie analizy pakietów danych, które przesyłane są przez sieć. Gdy pakiet danych przechodzi przez zaporę, są one analizowane w oparciu o zestaw reguł zdefiniowanych przez administratora. Te reguły określają, które rodzaje ruchu są dozwolone, a które powinny być odrzucone lub zablokowane.

Główne typy zapór sieciowych to:

Zapora sieciowa typu pakiety (ang. *packet filtering firewall*). Analizuje ona poszczególne pakiety danych w oparciu o adresy źródłowe i docelowe, porty, protokoły itp. I decyduje, czy przepuścić, odrzucić lub zablokować pakiet na podstawie zdefiniowanych reguł.

Zapora sieciowa typu stanowa (ang. *stateful firewall*). Oprócz analizy pojedynczych pakietów śledzi ona stan połączenia, pamiętając wcześniej przepuszczone pakiety. Pozwala to na bardziej inteligentne decyzje w odniesieniu do ruchu, ponieważ może rozróżnić prawidłowe połączenia od prób ataku.

Zapora sieciowa na poziomie aplikacji (ang. *application-layer firewall*). Ta zaawansowana zapora operuje na poziomie aplikacji i może dokładniej analizować i kontrolować ruch sieciowy na podstawie konkretnych protokołów, co pozwala na bardziej precyzyjne zarządzanie dostępem.

Zapory sieciowe są jednym z podstawowych narzędzi w zabezpieczaniu sieci przed atakami z zewnątrz. Ważne jest, aby były one konfigurowane i zarządzane zgodnie z najlepszymi praktykami w zakresie bezpieczeństwa, co zapewni odpowiednią ochronę sieci przed zagrożeniami.

IDPS (*Intrusion Detection and Prevention System*) wykrywa i zapobiega włamaniom. Jest to zaawansowane narzędzie w dziedzinie bezpieczeństwa sieci, które ma wykrywać próby nieautoryzowanego dostępu, ataków i działań podejrzanych w infrastrukturze sieciowej.

Główne funkcje systemu IDPS to:

Wykrywanie ataków. IDPS analizuje ruch sieciowy w czasie rzeczywistym, poszukując wzorców charakterystycznych dla różnych typów ataków, takich jak próby włamań, ataki złożone, oprogramowanie szpiegujące itp.

Zapobieganie atakom. Oprócz wykrywania, niektóre systemy IDPS mają również zdolność do automatycznego reagowania i blokowania podejrzanych aktywności, aby zapobiec powodzeniu ataków.

Reagowanie na incydenty. IDPS generuje alerty i powiadomienia, gdy wykryje podejrzane zachowania lub ataki. Te alerty pomagają administratorom sieci w podjęciu szybkich działań i odpowiedzi na incydenty.

Monitorowanie i analiza. System IDPS gromadzi dane dotyczące aktywności sieciowej, co umożliwia analizę zdarzeń, wykrycie trendów i identyfikację potencjalnych zagrożeń.

Integracja z innymi narzędziami bezpieczeństwa. Systemy IDPS mogą być zintegrowane z innymi rozwiązaniami bezpieczeństwa, takimi jak firewalle, systemy zarządzania dostępem i systemy audytu. Zapewnia to bardziej kompleksową ochronę sieci.

Systemy IDPS działają na różnych poziomach sieci, takich jak poziom pakietu (analizując poszczególne pakiety danych), poziom sesji (śledząc aktywność między hostami) lub poziom aplikacji (analizując ruch w oparciu o specyficzne protokoły i aplikacje).

DMZ (ang. *Demilitarized Zone*) to pojęcie z dziedziny bezpieczeństwa sieciowego, które odnosi się do specjalnego segmentu sieci znajdującego się pomiędzy siecią wewnętrzną (np. sieć firmową) a siecią zewnętrzną (np. Internetem). DMZ jest wykorzystywana do zwiększenia bezpieczeństwa sieci poprzez izolację niektórych zasobów i usług od bezpośredniego dostępu do sieci wewnętrznej.

Główne cechy DMZ:

Izolacja zasobów. W DMZ umieszcza się publicznie dostępne zasoby i usługi, takie jak serwery WWW, serwery poczty elektronicznej, serwery VPN czy serwery proxy. Te zasoby są dostępne dla użytkowników z sieci zewnętrznej, ale nie mają bezpośredniego dostępu do zasobów w sieci wewnętrznej.

Dodatkowa warstwa zabezpieczeń. DMZ działa jako dodatkowa warstwa zabezpieczeń między siecią wewnętrzną a siecią zewnętrzną. Ma na celu ograniczenie potencjalnych ataków na wewnętrzne zasoby sieciowe poprzez dostęp z sieci zewnętrznej.

Redukcja ryzyka. Przez umieszczenie publicznie dostępnych usług i zasobów w DMZ, organizacja minimalizuje ryzyko ataku bezpośrednio na wewnętrzną sieć. W przypadku kompromitacji serwera w DMZ, dostęp do kluczowych zasobów w sieci wewnętrznej jest nadal utrudniony.

Konfiguracja zapór sieciowych. DMZ jest zazwyczaj wspierana przez zapory sieciowe, które kontrolują ruch między sieciami wewnętrznymi i zewnętrznymi oraz przez wewnętrzne zapory kontrolujące ruch między DMZ a siecią wewnętrzną.

DMZ wymaga starannego zaprojektowania, uwzględniającego rodzaje zasobów dostępnych w tej strefie oraz odpowiednich zasad zarządzania dostępem, aby zminimalizować ryzyko ataków i naruszeń bezpieczeństwa.

Antywirusy (ang. *antivirus software lub AV*) to programy komputerowe, które służą do wykrywania, blokowania i usuwania złośliwego oprogramowania, takiego jak wirusy, trojany, robaki, ransomware, keyloggery i inne szkodliwe aplikacje. Ich głównym celem jest ochrona systemów komputerowych przed infekcjami i zagrożeniami związanymi z cyberprzestępczością.

Działanie antywirusów opiera się na takich j technikach, jak:

Skanowanie plików. Antywirusy skanują pliki na dysku twardym i w pamięci komputera w poszukiwaniu charakterystycznych wzorców kodu, które mogą wskazywać na obecność złośliwego oprogramowania.

Bazy sygnatur. Antywirusy używają baz sygnatur, które zawierają znane wzorce kodu złośliwego oprogramowania. Jeśli wykryją pasującą sygnaturę w skanowanym pliku, oznacza to, że plik jest potencjalnie zainfekowany.

Wykrywanie behawioralne. Niektóre antywirusy analizują zachowanie działających programów w czasie rzeczywistym, szukając podejrzanych aktywności mogących wskazywać na złośliwe działanie.

Heurystyka. Antywirusy stosują heurystykę, czyli technikę opartą na regułach i algorytmach, aby rozpoznać nowe i nieznane zagrożenia, które nie znajdują się jeszcze w bazach sygnatur.

Ochrona w czasie rzeczywistym. Wiele antywirusów oferuje ochronę w czasie rzeczywistym, co oznacza, że skanują aktywnie działające procesy i pliki podczas korzystania z komputera, aby natychmiast reagować na potencjalne zagrożenia.

Antywirusy są niezbędnym elementem bezpieczeństwa komputerowego, ponieważ pomagają zapobiegać infekcjom i minimalizują ryzyko utraty danych czy szkód wynikających z działalności złośliwego oprogramowania.

Szyfrowanie danych to proces konwersji czytelnych danych (takich jak tekst, pliki, dane transakcyjne) na nieczytelny format za pomocą specjalnego algorytmu matematycznego, aby zabezpieczyć je przed nieautoryzowanym dostępem. Szyfrowanie jest kluczowym narzędziem w dziedzinie cyberbezpieczeństwa, pozwalającym na ochronę poufności informacji, integralności i poufności danych w przypadku utraty kontroli nad nimi lub ich nieautoryzowanego ujawnienia.

Rodzaje szyfrowania danych to:

Szyfrowanie w ruchu (ang. *in motion*). Zabezpiecza dane w trakcie ich przesyłania pomiędzy urządzeniami lub sieciami. Celem tego rodzaju szyfrowania jest ochrona danych wrażliwych podczas ich transmisji przez sieć, aby nie były podatne na przechwycenie lub podsłuchanie przez nieautoryzowane osoby. Najczęściej stosuje się je w komunikacji internetowej, takiej jak przeglądanie stron internetowych przez protokół HTTPS, wymiana poczty elektronicznej przez protokół SSL/TLS czy korzystanie z bezpiecznych sieci VPN (Virtual Private Network).

Szyfrowanie w spoczynku (ang. *at rest*). Dotyczy zabezpieczania danych, które są przechowywane i pozostają w nieaktywnym stanie na urządzeniach pamięci masowej, takich jak dyski twarde, pamięć USB, karty pamięci itp. Celem tego rodzaju szyfrowania jest ochrona danych przed nieautoryzowanym dostępem, gdy znajdują się na nośnikach fizycznych. Szyfrowanie w spoczynku jest szczególnie ważne w przypadku zagubienia lub kradzieży urządzeń, aby dane na nich nie były dostępne dla osób nieupoważnionych.

Ważnym aspektem szyfrowania danych jest wykorzystanie odpowiednich kluczy szyfrujących, które są używane do kodowania i dekodowania danych. Klucz szyfrujący jest jak klucz do zamka – osoba, która posiada odpowiedni klucz, może odczytać i odszyfrować dane. Bez klucza dane pozostają nieczytelne.

Szyfrowanie danych jest skutecznym środkiem ochrony poufności informacji w środowisku online i offline.

Dodatkowo szyfrowanie danych może znacznie wspomóc organizacje w spełnieniu wymogów Rozporządzenia Ogólnego o Ochronie Danych Osobowych (RODO):

Ochrona poufności danych osobowych. Szyfrowanie danych osobowych zapewnia dodatkową warstwę ochrony, dzięki której stają się one nieczytelne dla osób nieupoważnionych. W przypadku naruszenia bezpieczeństwa i dostania się do zaszyfrowanych danych, atakujący nie będzie w stanie odczytać ich treści.

Zasada integralności i pouczania. Szyfrowanie zapobiega modyfikacji danych w nieuprawniony sposób, ponieważ nawet w przypadku nieautoryzowanego dostępu do zaszyfrowanych danych osoba trzecia nie będzie w stanie zmieniać ich zawartości bez odpowiednich kluczy szyfrujących.

Obowiązek zapewnienia odpowiedniego poziomu bezpieczeństwa. RODO wymaga od firm stosowania odpowiednich środków technicznych i organizacyjnych, aby chronić dane osobowe przed nieuprawnionym dostępem, utratą czy uszkodzeniem. Szyfrowanie danych jest uznawane za zaawansowaną technicznie metodę zabezpieczania informacji.

Powiadamianie o naruszeniach danych. Szyfrowanie danych może pomóc organizacjom uniknąć obowiązku powiadamiania o naruszeniach danych, jeśli dane były odpowiednio zaszyfrowane i dostęp do kluczy szyfrujących był kontrolowany.

PROCES OBSŁUGI INCYDENTÓW

Podstawy obsługi incydentów w organizacji

Proces obsługi incydentu cyberbezpieczeństwa to strukturalny i skoordynowany sposób reagowania na podejrzane lub potwierdzone wydarzenia związane z bezpieczeństwem informacji. Proces ten składa się z kilku kluczowych etapów:

Wykrycie incydentu. Pierwszym krokiem jest wykrycie możliwego incydentu cyberbezpieczeństwa. Może to nastąpić poprzez automatyczne systemy monitorujące lub raportowanie przez pracowniczki i pracowników o podejrzanych zdarzeniach.

Ocena i klasyfikacja. Zespół odpowiedzialny za obsługę incydentu (powołany ad hoc albo istniejący już w ramach systemu zarządzania bezpieczeństwem) przeprowadza wstępną ocenę i klasyfikację zdarzenia, aby określić jego charakter i potencjalne zagrożenia. To pozwala na przypisanie odpowiedniego priorytetu oraz skoncentrowanie wysiłków na najbardziej krytycznych incydentach.

Izolacja i ograniczenie. W tym etapie zespół podejmuje działania mające na celu izolację i ograniczenie skutków incydentu. Może to oznaczać odłączenie zainfekowanego urządzenia od sieci, wyłączenie uszkodzonego systemu czy zablokowanie atakującego adresu IP.

Eliminacja incydentu. Następnym krokiem jest eliminacja przyczyn incydentu oraz usunięcie złośliwego oprogramowania czy nieautoryzowanych dostępów.

Przywracanie normalnego działania. Po usunięciu zagrożenia zespół pracuje nad przywróceniem normalnego działania systemów i usług.

Śledzenie i analiza. Po zakończeniu obsługi incydentu zespół przeprowadza szczegółową analizę zdarzenia, aby zrozumieć przyczyny i sposób działania atakującego. Analiza ta ma również pomóc w wyciągnięciu wniosków i zastosowaniu działań zapobiegawczych na przyszłość.

Dokumentacja. Ważne jest, aby cały proces obsłu-

gi incydentu został dokładnie udokumentowany, w tym działania podjęte podczas reakcji, wnioski z analizy oraz wykorzystane zasoby.

Raportowanie. Na koniec zespół powinien przygotować raport na temat obsługi incydentu, który będzie zawierał opis zdarzenia, działania podjęte w celu jego rozwiązania oraz wnioski i zalecenia na przyszłość.

JAK ZGŁASZAĆ INCYDENTY?

Jeśli osoby odpowiedzialne za bezpieczeństwo firmy zidentyfikowały, że doszło do skutecznego ataku, w wyniku którego ucierpiały dane, powinny zgłosić taki incydent do właściwych podmiotów. Jeśli jest to incydent związany z danymi osobowymi, należy zgłosić go do Urzędu Ochrony Danych Osobowych. W pozostałych przypadkach warto zgłosić taki incydent do CSIRT NASK. W przypadku, kiedy podmiot podlega pod reżim Ustawy o Krajowym Systemie Cyberbezpieczeństwa, takie zgłoszenie może być obowiązkiem ustawowym.

Zgłaszanie incydentów do CSIRT NASK

CSIRT NASK to inaczej Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego – CERT Polska. CERT Polska to zespół ekspertów, którzy na bieżąco monitorują bezpieczeństwo sieci i analizują wszelkie niepokojące zachowania, aby ostrzegać o cyberzagrożeniach.

Zgłaszanie incydentów do CSIRT NASK odbywa się przez stronę https://incydent.cert.pl/

Proces zgłaszania incydentu polega na wyborze rodzaju incydentu jak poniżej:

Kolejnym etapem jest podanie danych zgłaszającego oraz wprowadzenie opisu incydentu.

W przypadku zgłaszania podejrzanego oprogramowania należy spakować podejrzane pliki do archiwum, np. w formacie .rar, .zip, .7z, i użyć w nazwie słowa infected.

Jeżeli zgłoszenie dotyczy oprogramowania, które w wyniku użycia doprowadziło do zaszyfrowania plików na urządzeniu, należy opisać, w jaki sposób doszło do infekcji, a także załączyć plik tekstowy z żądaniem okupu lub przykładowego zaszyfrowanego pliku.

Zgłoszenie naruszenia ochrony danych

Organem właściwym do zgłaszania naruszeń ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO).

Jeżeli naruszenie dotyczy danych osób w różnych krajach UE, Prezes UODO może być, ale nie musi być wiodącym (czyli właściwym dla administratora lub podmiotu przetwarzającego) organem nadzorczym. W przypadku transgranicznego naruszenia danych administrator powinien dokonać analizy, czy wiodącym organem nadzorczym w odniesieniu do czynności przetwarzania, które zostały objęte naruszeniem, jest Prezes UODO, czy też może inny europejski organ nadzorczy.

SEKTOROWA RADA DS. KOMPETENCJI TELEKOMUNIKACJA I CYBERBEZPIECZEŃSTWO

Rada inicjuje i uczestniczy w przedsięwzięciach związanych z potrzebami kompetencyjnymi w obszarach telekomunikacji i cyberbezpieczeństwa, pomagając dostosować ofertę edukacyjną do wymagań rynku pracy w tym sektorze.

Rada pomaga dostosowywać ofertę edukacyjną do obecnych wymagań rynku pracy w sektorach telekomunikacji i cyberbezpieczeństwa m.in. poprzez:

- rekomendowanie rozwiązań /zmian legislacyjnych w edukacji i jej dostosowania do potrzeb rynku pracy w sektorze
- wskazywanie obszarów badawczych dotyczących kompetencji w sektorach oraz zlecanie tego rodzaju badań
- identyfikację potrzeb w zakresie aktualizacji Sektorowej Ramy Kwalifikacji oraz definiowanie poszczególnych kwalifikacji
- przekazywanie informacji nt. zapotrzebowania na kompetencje pracowników do instytucji edukacyjnych i rynku pracy, aby wpłynąć na poprawę ich skuteczności
- obsługę działania 2.21 typ 4 POWER (szkolenia lub doradztwo wynikające z rekomendacji Sektorowych Rad ds. Kompetencji), w szczególności opracowanie oraz aktualizacja rekomendacji dotyczących zapotrzebowania na kompetencje w sektorze.

Rada wydała dotychczas dwie rekomendacje rozwojowe – nadzwyczajną, tzw. antycovidową, oraz zwyczajną. Ich celem było wskazanie najpilniejszych potrzeb kompetencyjnych w sektorze telekomunikacji i cyberbezpieczeństwa.

Działając na styku edukacji z biznesem, Rada współorganizuje coroczne Forum Współpracy Edukacji i Biznesu EDUMIXER. Jego celem jest wypracowanie propozycji zmian w programach kształcenia przyszłych pracobiorców, które będą uwzględniały rozwój technologiczny oraz potrzeby rynku pracy.

e-mail: rada.telekomunikacja@pti.org.pl

www.srtcb.radasektorowa.pl

Projekt „Utworzenie i funkcjonowanie Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo" jest realizowany w ramach Osi priorytetowej II: Efektywne polityki publiczne dla rynku pracy, gospodarki i edukacji oraz Działania 2.12 Zwiększenie wiedzy o potrzebach kwalifikacyjno-zawodowych w poszczególnych sektorach gospodarki.

Projekt nr UDA-POWR.02.12.00- 00-SR03/18 jest współfinansowany z Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014–2020.

PARP
Grupa PFR

Sektorowa Rada
ds. Kompetencji
Telekomunikacja
i Cyberbezpieczeństwo

www.srtcb.radasektorowa.pl

Partnerzy projektu:

PTI
POLSKIE TOWARZYSTWO INFORMATYCZNE

PIIT

Fundusze
Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz Społeczny

Warszawa, wrzesień 2023