Cyberbezpieczny samorząd

PORADNIK

NASK

Ministerstwo Cyfryzacji

OPRACOWANIE

NASK

Warszawa 2023

NASK – Państwowy Instytut Badawczy

ul. Kolska 12
01–045 Warszawa

Ministerstwo Cyfryzacji

Fundusze Europejskie na Rozwój Cyfrowy

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

01

Wstęp

1.1 O projekcie „Cyberbezpieczny Samorząd”

Projekt grantowy pn. „Cyberbezpieczny Samorząd” realizowany jest w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC) Działanie 2.2. pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa”.

Operacyjne zarządzanie projektem powierzono Centrum Projektów Polska Cyfrowa (CPPC) – państwowej jednostce budżetowej podległej ministrowi właściwemu do spraw informatyzacji – oraz Państwowemu Instytutowi Badawczemu NASK (NASK-PIB). Projekt jest odpowiedzią na potrzeby jednostek samorządu terytorialnego (dalej JST) wyłaniające się z „Diagnozy cyberbezpieczeństwa” przeprowadzonej w ramach projektów „Cyfrowa Gmina”, „Cyfrowy Powiat” i „Cyfrowe Województwo”, realizowanych przez CPPC we współpracy z NASK-PIB w poprzednich latach.

Celem Projektu grantowego pn. „Cyberbezpieczny Samorząd” jest zwiększenie bezpieczeństwa informacji poprzez wzmacnianie odporności jednostek samorządu terytorialnego oraz ich zdolności do skutecznego zapobiegania incydentom bezpieczeństwa teleinformatycznego, wykrywania ich i reagowania na nie.

Tak postawiony cel jest szczególnie ważny w kontekście potencjalnych konsekwencji dla kierownictwa jednostki, dotyczących zaniechań w tym obszarze – wynikających m.in. z przepisów Ogólnego rozporządzenia o ochronie danych osobowych (RODO), narażania instytucji na szkody, wstrzymania pracy urzędów, utraty danych czy mienia, ujawnienia wrażliwych danych osobom nieuprawnionym albo umożliwienia atakującym zniszczenia dokumentów lub danych.

1.2 Cel Poradnika

Niniejszy Poradnik jest skierowany do podmiotów uprawnionych – jednostek samorządu terytorialnego (JST), zainteresowanych podniesieniem poziomu cyberbezpieczeństwa.

Głównym celem Poradnika jest ułatwienie każdej jednostce samorządu terytorialnego identyfikacji aktualnego stanu cyberbezpieczeństwa i rzeczywistych potrzeb jednostki w tym zakresie oraz określenie realnych możliwości podniesienia przez JST poziomu cyberbezpieczeństwa. Równocześnie w Poradniku przedstawione zostały podstawowe zagadnienia formalne, prawne, organizacyjne i techniczne, umożliwiające analizę stanu rozwoju JST w obszarze cyberbezpieczeństwa. Wskazano również przykłady przedsięwzięć, jakie mogą podjąć JST w celu zwiększenia bezpieczeństwa informacji przez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania incydentom, wykrywania ich i reagowania na nie.

W Poradniku wskazano również wybrane aspekty prawne wynikające z przepisów Ustawy o krajowym systemie cyberbezpieczeństwa (uoKSC), Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (KRI) oraz Ogólnego rozporządzenia o ochronie danych osobowych (RODO).

Poradnik składa się łącznie z ośmiu rozdziałów, przybliżających m.in. aspekty prawne czy planowanie rozwoju JST w obszarze cyberbezpieczeństwa. Nawigację w publikacji ułatwia interaktywny spis treści na dole każdej strony – klikając w kolejne cyfry, można wygodnie przenosić się pomiędzy rozdziałami.

Opracowany przez ekspertów wykaz pojęć i skrótów używanych w dokumencie został zebrany i umieszczony w rozdziale 2. Poradnika. Wskazówki zawarte w publikacji powinny umożliwić JST zrównoważony rozwój cyberbezpieczeństwa, co w praktyce może przełożyć się na realną poprawę cyberbezpieczeństwa w obszarach związanych z regulacjami i procedurami, środkami technicznymi i kompetencjami personelu. Dodatkowo Poradnik omawia zagadnienia dotyczące zarządzania bezpieczeństwem w jednostce w kontekście budowy Systemu Zarządzania Bezpieczeństwem Informacji oraz szkoleń pracowników.

W Poradniku zaproponowano również przykłady działań, które mogą wesprzeć jednostkę w wypełnianiu wymagań, ale nie są zindywidualizowanymi zaleceniami dla danej JST. Poradnik nie zastępuje profesjonalnego doradztwa w zakresie cyberbezpieczeństwa.

Cyberbezpieczeństwo to zagadnienie szerokie i dynamiczne, obejmujące wiele aspektów: od technicznych, po prawne i społeczne. Poradnik nie jest pełnym kompendium wiedzy o cyberbezpieczeństwie. Zagadnienia są przedstawione w sposób uproszczony, stanowią podstawę do dalszych analiz. Intencją autorów było przedstawienie różnych, często skomplikowanych zagadnień w sposób przystępny również dla osób, które nie są ekspertami w dziedzinie cyberbezpieczeństwa. Publikacja będzie aktualizowana, aby zapewnić czytelnikom dostęp do najnowszych informacji i trendów w tej dziedzinie.

02

Wykaz skrótów i pojęć

Skróty używane w Poradniku

CPPC	Centrum Projektów Polska Cyfrowa
CSIRT	(ang. *Computer Security Incident Response Team*) – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego
IOD	Inspektor Ochrony Danych
JST	Jednostki Samorządu Terytorialnego
MC	Ministerstwo Cyfryzacji
NASK-PIB	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy
KRI	Rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247.)
RODO	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 oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
UOKSC	ustawa z 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. z 2023 r. poz.1863)

Pojęcia używane w Poradniku

A
B

Administrator Systemu Informatycznego (ASI)
osoba zarządzająca systemem informatycznym, odpowiedzialna za jego eksploatację, konserwację, działanie, bezpieczeństwo przechowywanych w systemie danych oraz realizację przypisanych użytkownikom uprawnień. ASI jest zazwyczaj powoływany zgodnie z wewnętrznymi zasadami ujętymi w Politykach Bezpieczeństwa Informacji (PBI).

Adres IP
(ang. *IP address*)
identyfikator (numer identyfikacyjny) nadawany urządzeniom podłączonym do sieci (np. komputerom, tabletom, urządzeniom sieciowym), służący do identyfikacji urządzeń podczas pracy w sieci.

Aktywa
wszystkie elementy w organizacji, które mają dla niej jakąś wartość: procesy biznesowe, w których przetwarzane są informacje (np. dane osobowe), pracownicy, sprzęt, odbiorcy usług publicznych czy mechanizmy działania w ramach jednostki. Wszystkie aktywa związane z przetwarzaniem danych powinny zostać ujęte w analizie ryzyka.

Anty-DDoS
(ang. *Anti-Distributed Denial of Service*)
środki, techniki i rozwiązania (sprzętowe, programowe lub usługi), realizujące ochronę przed atakami typu DDoS na systemy komputerowe lub usługi sieciowe. Zapobiegają przeciążeniu infrastruktury IT alokacją dużej ilości jej zasobów przez czynniki zewnętrzne, niezależne od organizacji, mające na celu zakłócenie dostępności docelowego systemu, sieci lub usługi przez przytłoczenie ich zalewem złośliwego ruchu z wielu źródeł.

Aplikacja
program komputerowy, wykonujący określone czynności i zadania (np. program obsługi magazynu, edytor tekstu lub arkusz kalkulacyjny).

Aplikacja mobilna
program, który działa na urządzeniach przenośnych (smartfon, tablet), posiadający często podobne funkcje do programu instalowanego na komputerze, ale dostosowany do specyficznego sposobu obsługi z wykorzystaniem ekranów dotykowych.

Atak „brute-force”
atak polegający na próbach złamania haseł lub kluczy kryptograficznych w celu uzyskania dostępu do zasobów informatycznych. Ta technika charakteryzuje się sprawdzaniem różnych kombinacji popularnych haseł, liczb czy znaków specjalnych w celu odnalezienia prawidłowego klucza.

BDR
(ang. *Backup & Disaster Recovery*)
proces kopiowania i przechowywania plików (ich kopii zapasowych) w określonej lokalizacji oraz odzyskiwania lub przywracania tych danych w przypadku wystąpienia sytuacji awaryjnych, takich jak utrata lub uszkodzenie danych (np. przez ich niekontrolowane zaszyfrowanie).

Bot

program komputerowy lub skrypt, którego zadaniem jest uruchomienie się na określonej grupie komputerów i wykonanie na nich zleconych przez agresorów zautomatyzowanych, niepożądanych działań bez wiedzy użytkownika komputera.

Botnet

grupa komputerów (botów) zainfekowanych szkodliwym oprogramowaniem, często należących do nieświadomych tego faktu organizacji. Takie zainfekowane komputery wykorzystują moc obliczeniową, energię elektryczną i sieć komputerową właścicieli tych urządzeń bez ich wiedzy, najczęściej do niepożądanych celów, związanych z przeprowadzaniem zaplanowanych ataków, do których jest potrzebna duża moc obliczeniowa rozproszonej sieci urządzeń.

BYOD

(ang. *Bring Your Own Device*)

polityka zezwalania pracownikom na legalne wykorzystywanie do celów służbowych ich prywatnych urządzeń przenośnych (laptopów, tabletów i smartfonów) w miejscach pracy i w sieci organizacji, w zgodzie z jej politykami i zasadami dostępu do informacji.

Chmura obliczeniowa

(ang. *Cloud Computing*)

model przetwarzania danych oparty na wykorzystywaniu usług dostarczonych spoza organizacji. Chmura to usługa oferowana przez zewnętrznego dostawcę, wykorzystująca konieczną infrastrukturę fizyczną, niebędącą własnością organizacji i nieznajdującą się na jej terenie. Eliminuje to konieczność utrzymywania przez organizację własnej infrastruktury informatycznej oraz instalowania i administrowania oprogramowaniem udostępnianym organizacji z zewnątrz chmury.

CMDB

(ang. *Configuration Management DataBase*)

baza danych, zawierająca dwa typy informacji: szczegóły każdego komponentu infrastruktury IT i jego konfiguracji (ang. *Configuration Item*, *CI*)oraz bazę relacji między elementami CI. Baza CI mówi o sprzęcie i komponentach oprogramowania, wykorzystywanych w usługach IT, którymi można zarządzać, a także o samych usługach. CMDB pozwala na wykrywanie i odnotowywanie zmian inwentaryzacyjnych oraz szybką ocenę wpływu tych zmian na inne usługi i elementy lub obszary infrastruktury IT. CMDB może także wspomagać automatyczną inwentaryzację zasobów IT organizacji oraz wspierać procesem zmian.

CSINT

(ang. *Closed-Source Intelligence* lub *Confidential Source Intelligence*)

zbieranie i analiza informacji ze źródeł zamkniętych lub niejawnych, sklasyfikowanych lub poufnych, tajnych, niepublicznych lub zastrzeżonych, które nie są łatwo dostępne dla społeczeństwa.

CSIRT

(ang. *Computer Security Incident Response Team*)

Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego. UoKSC ustanowiła trzy zespoły CSIRT na poziomie krajowym: CSIRT NASK, CSIRT GOV oraz CSIRT MON. Każdy z CSIRT odpowiedzialny jest za koordynację incydentów zgłaszanych przez przyporządkowane zgodnie z ustawą podmioty.

CTI

(ang. *Cyber Threat Inteligence*)

analiza zagrożeń cyberbezpieczeństwa. Dotyczy informacji o potencjalnych i istniejących zagrożeniach dla systemów, sieci, aplikacji i zasobów cyfrowych organizacji. CTI obejmuje gromadzenie, przetwarzanie, analizę i rozpowszechnianie danych związanych z cyberzagrożeniami, w tym uczestników, metod, motywów i wskaźników kompromitacji. Głównym celem CTI jest zapewnienie organizacjom przydatnych informacji, które

mogą im pomóc w proaktywnym wykrywaniu cyberzagrożeń, zapobieganiu im oraz skutecznemu reagowaniu na nie. CTI wykorzystuje różne źródła, w tym informacje ogólnie dostępne (OSINT), informacje ze źródeł zamkniętych lub zastrzeżonych (CSINT), platform udostępniania informacji o zagrożeniach oraz ze współpracy z zaufanymi partnerami i agencjami rządowymi.

Cyberbezpieczeństwo

dziedzina wiedzy zajmująca się zapewnieniem odporności: systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność posiadanych i przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

Zapewnienie **poufności** to zabezpieczenie przed ujawnieniem danych osobom niepowołanym, zwykle realizowane poprzez mechanizmy kontroli dostępu i szyfrowania, w spoczynku, podczas ich przesyłania i przetwarzania.

Dbałość o **integralność** danych oznacza dążenie do zapewnienia, że dane pozostają niezmienione, tzn. zabezpieczone przed nieautoryzowanymi zmianami.

Dostępność informacji to możliwość korzystania z nich w dowolnym czasie i bez żadnych utrudnień. Zapewnienie **autentyczności** to możliwość pewnego potwierdzenia pochodzenia danych.

DAM
(ang. *Database Access Management*)

rozwiązanie bezpieczeństwa pozwalające na zarządzanie dostępami do baz danych. Określa ono: jakie konta mogą mieć dostęp do jakich obszarów baz i ich elementów oraz jakie prawa dostępu do zawartości baz danych mają te konta. Rozwiązanie zapewnia także monitorowanie i rozliczalność takich dostępów

Dane osobowe

zgodnie z definicją z RODO dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania żyjącej osoby fizycznej. Poszczególne informacje, które w połączeniu ze sobą mogą prowadzić do zidentyfikowania tożsamości danej osoby, także stanowią dane osobowe.

DDoS
(ang. *Distributed Denial of Service*)

atak na systemy komputerowe lub usługi sieciowe w celu uniemożliwienia ich działania przez przeciążenie infrastruktury alokacją dużej ilości jej zasobów – przeprowadzany równocześnie z wielu komputerów.

DLP
(ang. *Data Leak / Loss Prevention*)

rozwiązania służące zabezpieczeniu przed wyciekami informacji z organizacji.

DNS
(ang. *Domain Name System*)

protokół i oprogramowanie, które sprawia, że nazwa strony internetowej jest przekształcana na adres IP. DNS wyszukuje adres IP danej witryny na podstawie adresu, jaki użytkownik wpisał np. w swojej przeglądarce.

EDR
(ang. *Endpoint Detection and Response*)

zintegrowane rozwiązanie bezpieczeństwa, którego główne funkcje to: monitorowanie i gromadzenie danych o aktywnościach użytkowników i oprogramowania na urządzeniach końcowych, analiza tych danych w celu identyfikacji wzorców zagrożeń, automatyczne reagowanie na zidentyfikowane zagrożenia w celu ich usunięcia lub powstrzymania, powiadamianie personelu bezpieczeństwa o zidentyfikowanych anomaliach.

Firewall

zapora sieciowa, urządzenie (fizyczne lub wirtualne), które zapewnia filtrację lub separację ruchu pomiędzy kilkoma sieciami i znajdującymi się w nich urządzeniami.

GovPress

panel redakcyjny portalu dla JST (redakcja.samorzad.gov.pl).

GRC
(ang. *Governance, Risk management and Compliance*)

indywidualne podejście organizacji do współistnienia i wzajemnego działania w niej trzech grup procesów: zarządczych, zarządzania ryzykiem w skali organizacji oraz zarządzania zgodnością z wewnętrznymi i zewnętrznymi normami, regulacjami branżowymi i prawnymi. GRC pomaga instytucjom w identyfikacji, zarządzaniu i kontrolowaniu różnych rodzajów ryzyka związanego z działalnością oraz zapewnia, że organizacja działa zgodnie z wymaganiami i regulacjami otoczenia.

HSM
(ang. *Hardware Security Module*)

rozwiązanie sprzętowe, służące do bezpiecznego przechowywania i ochrony kluczy kryptograficznych oraz zarządzania nimi, używane przede wszystkim jako procesor kryptograficzny do efektywnego i szybkiego szyfrowania i deszyfrowania informacji z użyciem kluczy, które przechowuje i udostępnia.

IAM / IDM
(ang. *Identity Access Management / Identity Management*)

rozwiązanie ułatwiające zarządzanie tożsamościami cyfrowymi użytkowników oraz ich dostępami do systemów i zasobów w infrastrukturze IT organizacji. Dzięki wdrożeniu IAM / IDM można centralizować kontrolę dostępu użytkowników do zasobów organizacji.

ICT
(ang. *Information and Communication Technology*)

technologie informacyjne i komunikacyjne, które zamiennie nazywane są technologiami informacyjno-komunikacyjnymi (TIK), teleinformatycznymi lub cyfrowymi. Pojęcie odnosi się do rodziny technologii, które przetwarzają, gromadzą i przesyłają informacje w postaci elektronicznej.

Interesariusz
(strona zainteresowana)

jednostka (osoba, grupa lub organizacja), która może wpływać, na którą może wpływać lub która postrzega siebie samą jako zależną od określonych aktów prawnych lub normatywnych, określonych organizacji, decyzji lub działań.

IDS
(ang. *Intrusion Detection System*)

rozwiązanie służące do wykrywania niepożądanych aktywności w infrastrukturze organizacji oraz informowania o ich wystąpieniu odpowiednich funkcji lub osób. Bardziej zaawansowaną formą IDS są rozwiązania **IPS**.

IPS
(ang. *Intrusion Prevention System*)

rozwiązanie służące do zapobiegania wystąpieniom niepożądanych aktywności w infrastrukturze organizacji, takich jak np. próby włamań czy przełamania zabezpieczeń. Zadaniem IPS jest także wykrywanie takich działań w sieci organizacji, podejmowanie prób zapobiegania ich skutkom i informowanie o ich wystąpieniu odpowiednich funkcji lub osób.

Kontrola dostępu

podstawowy element zabezpieczeń, który formalizuje zasady uzyskiwania dostępu do określonych zasobów oraz określa warunki wymagane do uzyskania tego dostępu, zasady i procedury nadawania użytkownikom uprawnień i dostępów do zasobów niezbędnych do pełnienia ich funkcji czy realizowania zadań.

Malware

złośliwe oprogramowanie (ang. ***Mal****icious Soft****ware***), które prowadzi szkodliwe działania, np. przejmuje kontrolę nad urządzeniami, kradnie dane, hasła, pliki, np. wirus, trojan, rootkit, oprogramowanie szyfrujące, ransomware, worm, keylogger itp.

MDM
(ang. *Mobile Device Management*)

oprogramowanie, które umożliwia administratorom IT monitorowanie, zarządzanie i zabezpieczanie służbowych urządzeń mobilnych, takich jak smartfon czy tablet. MDM pozwala zespołom IT na zdalną aktualizację i zabezpieczanie urządzeń mobilnych za pośrednictwem centralnej konsoli zarządzania. W zakres tego zarządzania może wchodzić: zarządzanie aplikacjami, wymuszanie zmian haseł, wymuszanie aktualizacji urządzeń, definiowanie polityk ściśle określających zakres działań użytkowników na urządzeniach mobilnych w celu zapewnienia im systemowych mechanizmów bezpieczeństwa.

MDR
(ang. *Managed Detection and Response*)

usługa wykrywania i reagowania na zagrożenia, która powinna znajdować się w katalogu usług SOC. W jej zakresie mieści się m.in.: prewencja, neutralizacja zagrożeń i reagowanie na nietypowe aktywności w sieciach, a także rozpoznawanie ataków na wczesnym etapie i podejmowanie działań zaradczych.

MFA
(ang. *Multi-Factor Authentication*)

uwierzytelnianie wieloskładnikowe. To metoda uwierzytelniania, w której użytkownik, aby dostać się do zasobów (np. aplikacji mobilnej, konta online lub sieci VPN), musi uwierzytelnić się na co najmniej dwa różne sposoby (np. hasło i kod z aplikacji, użycie klucza, karty zbliżeniowej lub mikroprocesorowej). W przypadku zaawansowanych systemów tych elementów weryfikacji może być więcej. Najprostszym rodzajem MFA jest weryfikacja dwuetapowa (2FA), która wykorzystuje przy uwierzytelnieniu dwa czynniki różnych kategorii (np. hasło i kod z aplikacji online lub tokena).

N6

platforma stworzona przez CERT Polska, służąca do gromadzenia, przetwarzania i przekazywania informacji o zdarzeniach bezpieczeństwa w sieci. W ciągu każdego roku przez platformę przetwarzane są dziesiątki milionów zdarzeń bezpieczeństwa z Polski i całego świata. N6 funkcjonuje w pełni automatycznie.

NAC
(ang. *Network Access Control*)

rozwiązanie zapewniające kontrolę dostępu do sieci przez weryfikację bezpieczeństwa i uprawnień urządzenia końcowego ubiegającego się o dostęp do sieci, uwierzytelnienie stacji lub użytkownika, warunkowe przydzielenie dostępu do określonej sieci.

Oprogramowanie

obejmuje systemy operacyjne, aplikacje komercyjne i udostępniane nieodpłatnie, narzędzia i biblioteki programistyczne, oprogramowanie sieciowe oraz oprogramowanie sprzętowe urządzeń infrastruktury sieciowej, serwerów i stacji roboczych.

Oprogramowanie antywirusowe

oprogramowanie, którego celem jest skanowanie, wykrywanie, rozpoznawanie oraz usuwanie złośliwego oprogramowania (**malware**) z komputera lub innego urządzenia, na którym zostało zainstalowane.

OSINT
(ang. *Open-Source Intelligence*)

gromadzenie i analiza informacji ze źródeł publicznych, ogólnie dostępnych.

PAM
(ang. *Privileged Access Management*)

rozwiązanie, które koncentruje się na scentralizowaniu zarządzania poświadczeniami wszelkich kont z wysokimi uprawnieniami do różnych systemów w infrastrukturze organizacji. PAM zarządza bezpiecznym przechowywaniem poświadczeń (patrz: **HSM**), ich zmianami, rotacją i dostępem uprawnionych użytkowników, co bardzo upraszcza zarządzanie dostępem do kluczowych zasobów oraz istotnie podnosi ich bezpieczeństwo (patrz także: **DAM**).

Plan postępowania z ryzykiem
(ang. *Risk Management Plan, RMP*)

dokument, w którym znajduje się zbiór zaplanowanych czynności niezbędnych do stworzenia i zorganizowania procesu zarządzania ryzykiem. Plan powinien zawierać analizę prawdopodobnych zagrożeń o dużym, średnim lub niskim wpływie na organizację i jej poprawne funkcjonowanie. Powinien zawierać także strategie i mechanizmy, które pomogą uniknąć utraty ciągłości działania na wypadek pojawienia się określonych typów przewidywalnych incydentów.

Pojedyncze logowanie
(ang. *Single Sign-On – SSO*)

metoda stosowania pojedynczego procesu podawania poświadczeń przez użytkownika w celu potwierdzenia swojej tożsamości oraz uzyskania dostępu do usług i zasobów w obrębie danej organizacji. Metoda wymaga istnienia scentralizowanej bazy użytkowników w domenie organizacji. SSO ułatwia użytkownikom dostęp do zasobów organizacji i podnosi efektywność zarządzania i utrzymania środowiska IT w skali całej organizacji.

Polityka Bezpieczeństwa Informacji (PBI)

dokument określający metody, narzędzia, praktyki i zasady, których należy używać i przestrzegać w celu zapewnienia bezpieczeństwa informacji danej organizacji.

Polityka haseł

jeden z dokumentów **SZBI**, który opisuje zasady tworzenia, przechowywania oraz posługiwania się hasłami jako środkami bezpieczeństwa danych osobowych.

RAID
(ang. *Redundant Array of Independent Disks*)

macierz lub grupa dysków fizycznych, które stanowią jeden dysk logiczny, zabezpieczając w ten sposób dane tam zapisywane przed ich bezpowrotną utratą w przypadku awarii dowolnego pojedynczego dysku. W zależności od przyjętego typu rozwiązania RAID i liczby dysków może zapewniać także szybszy dostęp do danych oraz większą przestrzeń widoczną jako jeden dysk logiczny.

Ransomware	jeden z rodzajów złośliwego oprogramowania, które powoduje zablokowanie lub zaszyfrowanie zasobów czy systemów danej organizacji. Za przywrócenie dostępu do nich żąda okupu, jednak jego wpłacenie nie gwarantuje odzyskania zasobów.
Robak komputerowy	szkodliwe oprogramowanie, które uruchamia się bez wiedzy użytkowników z wysłanego pliku lub linku strony internetowej. Robaki komputerowe zwykle mają zdolność samoistnego powielania i rozprzestrzenia się w sieci organizacji.
Ryzyko	wpływ niepewności na cele (zgodnie z PN-ISO/IEC 27005:2014-01).
S46	system teleinformatyczny, który wspiera zgłaszanie i obsługę incydentów, wymianę informacji, współpracę pomiędzy uczestnikami Krajowego Systemu Cyberbezpieczeństwa (KSC) oraz zapewnia szacowanie ryzyka i ostrzeganie o zagrożeniach cyberbezpieczeństwa na poziomie krajowym.
Serwer	fizyczny, logiczny lub wirtualny komputer, który dostarcza dane lub usługi do innych komputerów w ramach infrastruktury IT oraz działalności organizacji.
SIEM (ang. *Security Information and Event Management*)	rozwiązanie służące do wykrywania, korelacji oraz analizy zdarzeń bezpieczeństwa, występujących w systemach i sieciach teleinformatycznych.
SOAR (ang. *Security Orchestration, Automation and Response*)	rozwiązanie rozszerzające zakres funkcjonalności rozwiązań klasy **SIEM**. Pozwala automatyzować działania administracyjne SIEM oraz tworzyć schematy czynności, które są skutecznymi procedurami zaradczymi lub naprawczymi po identyfikacji określonych typów incydentów lub wystąpieniach znanych zagrożeń, a także wykonywać je bez interwencji administratorów SIEM / SOAR. Zaawansowane i na ogół drogie narzędzie dla jednostek **SOC**.
SOC (ang. *Security Operations Center*)	jednostka odpowiedzialna za bieżące monitorowanie i analizę stanu cyberbezpieczeństwa organizacji. Celem SOC jest wykrywanie incydentów związanych z cyberbezpieczeństwem, analizowanie ich i reagowanie na nie z wykorzystaniem trzech rodzajów zasobów: ludzi i ich kompetencji, wypracowanych procesów i procedur oraz narzędz i rozwiązań technicznych.
SOCaaS (ang. *SOC as a Service*)	usługa polegająca na zleceniu zewnętrznemu podmiotowi obsługi i utrzymania w pełni zarządzanego SOC. SOCaaS zapewnia w modelu usługowym wszystkie funkcje bezpieczeństwa realizowane przez tradycyjny, wewnętrzny SOC, w tym: monitorowanie, analizę dzienników zdarzeń, wykrywanie zagrożeń i ich analizę, identyfikację i reagowanie na incydenty, raportowanie. Dostawca usługi SOCaaS przyjmuje odpowiedzialność za ludzi, procesy i technologie potrzebne do świadczenia usługi i zapewnia wsparcie w określonym wymiarze.

SYSLOG

narzędzie systemu operacyjnego, które umożliwia centralną rejestrację wszystkich zdarzeń w systemie, uwzględniając także priorytety zdarzeń oraz ich źródła.

System informacyjny

system teleinformatyczny, o którym mowa w art. 3 pkt 3 Ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2023 r. poz. 57) wraz z przetwarzanymi w nim danymi w postaci elektronicznej.

System informatyczny/ teleinfomatyczny

zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów Ustawy z 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. z 2022 r. poz. 1648 i 1933).

SZBI

System Zarządzania Bezpieczeństwem Informacji to zestaw polityk (patrz: **PBI**), procesów, procedur, kompetencji i narzędzi, który powinien być opracowany i zatwierdzony przez kierownictwo, opublikowany, zakomunikowany pracownikom i właściwym stronom zewnętrznym oraz na bieżąco aktualizowany zgodnie z wymaganiami.

UEBA

(ang. *User and Entity Behavior Analytics*)

analityka zachowań użytkowników i podmiotów. Metoda lub typ rozwiązania dla cyberbezpieczeństwa, które koncentruje się na wykrywaniu i zapobieganiu zagrożeniom wewnętrznym. Polega na wykrywaniu i analizie nietypowych zachowań w sieci i systemach organizacji. UEBA wykorzystuje techniki uczenia maszynowego, analizy statystycznej i korelacji danych do analizy i monitorowania wzorców zachowań użytkowników i podmiotów (takich jak aplikacje, urządzenia i serwery) w celu identyfikacji potencjalnych zagrożeń bezpieczeństwa i anomalii.

UPS

(ang. Uninterruptable Power Supply)

zapasowe zasilanie baterynje

Urządzenia sieciowe

grupa urządzeń, które pozwalają na przesyłanie danych przez sieć komputerową, takich jak przełączniki sieciowe, rutery itp.

Urządzenia końcowe

wszystkie urządzenia przeznaczone do podłączenia do sieci, które komunikują się z urządzeniami sieciowymi, korzystają z sieci lub udostępniają usługi innym urządzeniom końcowym. Do tej grupy należą komputery przenośne (notebooki, laptopy, netbooki), oraz stacjonarne (komputery, serwery, konsole do gier, smartfony, inteligentne telewizory, drukarki itp.).

UTM

(ang. *Unified Threat Management*)

urządzenia sieciowe, odpowiadające za kompleksową ochronę, nadzorowanie ruchu w sieci lokalnej oraz styk / dostęp do internetu. Zamiast wielu rozwiązań typu: zapory sieciowe, IPS, filtry antyspamowe, routery itp. – jedno rozwiązanie, łączące wszystkie te funkcje.

Uwierzytelnienie
(ang. *Authentication*)

proces polegający na potwierdzeniu zadeklarowanej tożsamości osoby lub podmiotu biorącego udział w komunikacji. Celem uwierzytelniania jest uzyskanie określonego poziomu pewności, że dana osoba lub podmiot jest w rzeczywistości tym, za kogo się podaje.

VPN
(ang. *Virtual Private Network*)

wirtualna sieć prywatna lub rozwiązanie, które umożliwia zdalne, bezpieczne (szyfrowane) połączenie z siecią komputerową organizacji i jej zasobami przez niechronione i niezaufane sieci publiczne.

WAF
(ang. *Web Application Firewall*)

programowe rozwiązanie bezpieczeństwa, pełniące funkcję firewalla aplikacyjnego, przeznaczone do ochrony aplikacji internetowych przed atakami, lukami w zabezpieczeniach aplikacji i złośliwymi działaniami. Funkcjonuje jako filtr między aplikacją a siecią, monitorując i analizując przychodzący i wychodzący ruch w celu identyfikacji i blokowania potencjalnych zagrożeń.

Wirusy komputerowe

szkodliwe oprogramowanie, które może przedostać się do komputerów w organizacji bez wiedzy i pozwolenia użytkowników czy administratorów oraz wyrządzić szkody. Ten rodzaj złośliwego oprogramowania ma zdolność powielania się w danej sieci i infekowania innych komputerów.

Złośliwe oprogramowanie

patrz: **Malware**.

03

Aspekty prawne

Wraz ze wzrostem popularności usług cyfrowych i pojawianiem się nowych technologii rośnie także cyberprzestępczość, co jest wyraźnie widoczne w statystykach zespołów zajmujących się reagowaniem na incydenty bezpieczeństwa komputerowego. Dodatkowo sytuacja międzynarodowa sprawia, że systematycznie rośnie liczba ataków na instytucje publiczne. W takich okolicznościach ważne jest – jak nigdy przedtem – zadbanie o cyberbezpieczeństwo podmiotów świadczących usługi publiczne i przetwarzających dane obywateli.

Cyberbezpieczeństwo, według definicji z uoKSC, to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Warto dodać, że odporność systemów informacyjnych buduje się wielopoziomowo: od zapewnienia bezpieczeństwa sieci teleinformatycznej, poprzez bezpieczeństwo komputerów i innych urządzeń oraz oprogramowania, aż po procedury i praktyki obowiązujące w danej organizacji. Zbudowanie odpowiedniego poziomu odporności nie jest łatwe i wymaga odpowiedniego przygotowania organizacyjnego, właściwie dobranych narzędzi i systematycznie podnoszonych kompetencji, zarówno użytkowników, jak i specjalistów zajmujących się utrzymaniem IT i bezpieczeństwem podmiotu publicznego.

Polski ustawodawca przygotował szereg regulacji, które obligują podmioty publiczne do utrzymania minimalnego poziomu bezpieczeństwa w sferze cyfrowej. Niniejszy Poradnik skupia się na trzech z nich:

[KRI] Rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;

[UOKSC] Ustawa z 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa;

[RODO] 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 oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Zaleca się stały monitoring postępu prac legislacyjnych związanych z nowelizacją ww. regulacji.

Zastosowanie odpowiednich środków we wszystkich trzech obszarach zmniejsza ryzyko wystąpienia szkód spowodowanych atakiem, zarówno w postaci ograniczenia świadczonych usług publicznych, jak i potencjalnych szkód dla obywateli, których dane nie powinny trafić w niepowołane ręce (lub zostać w sposób nieautoryzowany zmienione, uszkodzone lub zniszczone).

Jednostki samorządu terytorialnego, w tym ich związki i organy, podlegają ww. regulacjom, odpowiednio jako:

- podmiot publiczny, w przypadku rozporządzenia KRI (§ 3 ust. 1, w związku z art. 2 ust. 1 pkt 1) ustawy z 17 lutego 2005 r. o informatyzacji podmiotów państwowych (Dz.U. z 2023 r. poz. 57) oraz uoKSC (art. 4 pkt 7);
- administrator danych w rozumieniu RODO.

Do najistotniejszych zobowiązań w zakresie powiązanym z zapewnieniem cyberbezpieczeństwa dla JST zdaniem autorów Poradnika należą opisane niżej wymogi wynikające z KRI, uoKSC i RODO.

I. Wymogi wynikające z Rozporządzenia Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

Zgodnie z art. 13 ust. 1 ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne podmiot publiczny używa do realizacji zadań publicznych systemów teleinformatycznych spełniających minimalne wymagania dla systemów teleinformatycznych oraz zapewniających interoperacyjność systemów na zasadach określonych w Krajowych Ramach Interoperacyjności (KRI).

Podstawowe zobowiązania dla podmiotu publicznego w zakresie rozporządzenia KRI określa z kolei jego § 20 – zobowiązuje do „opracowania i ustanowienia, wdrożenia i eksploatacji, monitorowania i przeglądania oraz utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji zapewniającego poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność". W doktrynie wskazuje się, że przepis ten „ustanawia – jako podstawę funkcjonowania tego systemu – model procesu zarządzania oparty na tzw. cyklu Deminga (planuj – wykonuj – sprawdzaj – działaj, ang. *Plan – Do – Check – Act*)". Jest to zbieżne z podejściem zaprezentowanym również w normie ISO 27001. Istotą tego podejścia jest ciągłe testowanie wprowadzonych środków organizacyjnych i technicznych oraz wprowadzanie na tej podstawie niezbędnych zmian.

Dodatkowo należy zwrócić szczególną uwagę na § 21 rozporządzenia KRI, w którym uregulowano wymogi techniczne związane z zapewnianiem rozliczalności, będącej jednym z atrybutów bezpieczeństwa informacji.

II. Wymogi wynikające z ustawy z 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa

Jednostki samorządu terytorialnego wchodzą w skład krajowego systemu cyberbezpieczeństwa, którego skład podmiotowy określa art. 4 uoKSC. Pamiętać należy, że obok JST podmiotami krajowego systemu cyberbezpieczeństwa są również spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z 20 grudnia 1996 r. o gospodarce komunalnej (Dz.U. z 2021 r. poz. 679).

Obowiązki podmiotu publicznego realizującego zadania publiczne zależne od systemu informacyjnego określają art. 21, art. 22 i art. 23 uoKSC:

„Podmiot publiczny, aby mieć obowiązek stosowania przewidzianych w rozdziale III obowiązków, musi wykonywać przynajmniej jedno zadanie publiczne zależne od systemu informacyjnego. Nieważne jest tu zatem samo organizacyjne funkcjonowanie urzędu (np. wdrożenie EZD) – jego zależność bądź brak takiej zależności od systemu informacyjnego, a realizacja zadania publicznego. W obecnych czasach, przy wdrożeniu m.in. systemu ePUAP, Obywatel.gov.pl, gov.pl, większość podmiotów publicznych realizuje przynajmniej jedno zadanie publiczne zależne od systemu informacyjnego”.

Podstawowym obowiązkiem podmiotów publicznych jest wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa (tzw. osoby kontaktowej). Osoba ta będzie kontaktować się z właściwymi organami w przypadku wystąpienia incydentu, powinna więc posiadać dokładną wiedzę o systemach teleinformatycznych wykorzystywanych w danym urzędzie. Warto wskazać, że wyznaczając osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami KSC, jednostka samorządu terytorialnego może wskazać jedną osobę odpowiedzialną za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych również przez jej jednostki organizacyjne.

Zgodnie z art. 22 ust. 1 pkt 5 podmioty publiczne zobowiązane do wyznaczenia osoby do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa muszą przekazać właściwemu CSIRT w terminie 14 dni od wyznaczenia tej osoby następujące dane: jej imię, nazwisko, numer telefonu oraz adres poczty elektronicznej. W przypadku zmiany danych lub wyznaczenia innej osoby podmiot publiczny również ma 14 dni na poinformowanie o tym właściwego CSIRT.

Właściwości CSIRT określa art. 26 ustawy o KSC. Jednostki samorządu terytorialnego zgłaszają incydenty do CSIRT NASK za pośrednictwem formularza dostępnego na stronie incydent.cert.pl.

Art. 22 reguluje kwestie związane z incydentem w podmiocie publicznym, w tym w szczególności jego zgłoszenie i obsługę. Zgodnie z art. 2 pkt 9 uoKSC incydent w podmiocie publicznym to „incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny”. W doktrynie wskazuje się, że obowiązkiem nałożonym na podmioty publiczne, choć niewyartykułowanym wprost w art. 22, jest prowadzenie dokumentacji (rejestracji) wszystkich incydentów w podmiocie publicznym. Obowiązek ten wynika z definicji zarządzania incydentem oraz jego obsługi.

Art. 23 określa minimalny zakres danych przesyłanych w ramach zgłoszenia incydentu w podmiocie publicznym.

Art. 24 przyznaje pomiotom publicznym realizującym zadanie publiczne zależne od systemu informacyjnego uprawnienie analogiczne do operatorów usługi kluczowej.

Polega ono na przekazywaniu do właściwego CSIRT informacji: o innych incydentach, o zagrożeniu cyberbezpieczeństwa, dotyczących szacowania ryzyka, o podatnościach, a także o wykorzystanych technologiach.

Art. 25. UOKSC – należy mieć na uwadze, że zgodnie z art. 5 ust. 2 UOKSC wobec podmiotu publicznego może zostać również wydana decyzja o uznaniu tego podmiotu za operatora usługi kluczowej (OUK). Podmioty te muszą stosować dodatkowo przepisy rozdziału 3 UOKSC „Obowiązki operatorów usług kluczowych" (art. 8–16 UOKSC). Podmiot taki stosuje przepisy rozdziału 3 wyłącznie w zakresie realizacji usługi, w związku z którą został uznany za operatora usługi kluczowej. Jeżeli podmiot publiczny świadczy różne usługi, w tym również usługę kluczową, tzn. usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych, to przepisy rozdziału 3 mają zastosowanie wyłącznie do tej usługi.

Warto również zwrócić uwagę na rekomendacje dotyczące stosowania urządzeń informatycznych lub oprogramowania, które może wydawać Pełnomocnik Rządu do spraw Cyberbezpieczeństwa na podstawie art. 33 UOKSC. Rekomendacje te wydawane są po przebadaniu danego urządzenia lub oprogramowania przez jeden z zespołów CSIRT. Pełnomocnik może następnie zwrócić się do podmiotów krajowego systemu cyberbezpieczeństwa, w tym podmiotów publicznych, o informacje o sposobie i zakresie ich uwzględnienia.

Podmioty krajowego systemu cyberbezpieczeństwa, w tym podmioty publiczne, informują Pełnomocnika (na jego wniosek) o sposobie i zakresie uwzględnienia rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania.

W przypadku nieuwzględnienia tych rekomendacji Pełnomocnik informuje o tym organ nadzorujący daną jednostkę.

Informacje o wydanych rekomendacjach będzie można znaleźć na stronie gov.pl/web/cyfryzacja.

III. Wymogi wynikające z Rozporządzenia 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 oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

Jednostka samorządu terytorialnego, w świetle przepisów obowiązującego prawa, podlega takim samym obowiązkom administratora danych osobowych osób fizycznych, jakim podlega każdy inny administrator danych osobowych osób fizycznych[1].

Wykonywanie przez JST zadań własnych oraz zleconych wiąże się z potrzebą przetwarzania danych osobowych ich mieszkańców. Za przetwarzanie danych osobowych, zgodnie z RODO, uważa się operację/zestaw operacji wykonywanych na danych osobowych albo zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany.

Reguły przetwarzania danych osobowych określa art. 5 RODO. Z punktu widzenia cyberbezpieczeństwa szczególnie istotny jest obowiązek określony w lit. f), tj. obowiązek przetwarzania „w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (*integralność i poufność*)".

1 Odpowiedzi na kluczowe pytania związane z RODO znajdują się w publikacji „RODO dla administracji".

Podstawy prawne przetwarzania danych osobowych, z których dla działalności JST zastosowanie może znaleźć co najmniej kilka, określa art. 6 RODO. JST jako administrator danych osobowych w większości przypadków przetwarza dane osobowe w oparciu o kryterium wypełniania obowiązków prawnych na niej ciążących bądź kryterium niezbędności przetwarzania takich danych do wykonania zadań realizowanych w interesie publicznym lub w ramach sprawowania władzy publicznej.

Jednostka samorządu terytorialnego jako administrator jest zobowiązana do wykonywania wobec osób fizycznych, których dane przetwarza, ich praw, wskazanych w art. 12–22 RODO, z wyjątkami ustanowionymi w ustawie z 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781).

Zgodnie z art. 24 i 25 RODO (w związku z art. 32) JST, aby przetwarzanie przez nie danych osobowych odbywało się zgodnie z przepisami RODO i aby mogły to wykazać, muszą opracować i wprowadzić do stosowania odpowiednie środki techniczne i organizacyjne. Środki te powinny być opracowane przy uwzględnieniu charakteru, zakresu, kontekstu i celów przetwarzania danych osobowych, a także ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia.

Zgodnie z art. 28 RODO jednostka samorządu terytorialnego w przypadku powierzania innym podmiotom przetwarzania w swoim imieniu danych osobowych, którymi administruje, „korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą".

Zgodnie z art. 30 RODO każdy administrator prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada.

Zgodnie z art. 33 RODO obowiązek zgłaszania naruszenia bezpieczeństwa ochrony danych osobowych prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, spoczywa na administratorze, który bez zbędnej zwłoki, w terminie nie dłuższym niż 72 godziny po stwierdzeniu naruszenia, zgłasza naruszenie ochrony danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych (PUODO). Pozostałe obowiązki w przypadku naruszenia bezpieczeństwa określa art. 34 RODO.

Zgodnie z art. 35 RODO jednostka samorządu terytorialnego jako administrator danych ma obowiązek przed rozpoczęciem przetwarzania dokonać oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Zgodnie z art. 37 RODO jednostka samorządu terytorialnego ma obowiązek wyznaczyć inspektora ochrony danych.

Należy pamiętać, że wystąpienie niektórych incydentów będzie prowadzić do naruszenia różnych aktów prawnych, np. UOKSC i RODO. Niewykluczone, że w znacznej części incydenty będą dotyczyć naruszenia dostępu, autentyczności, integralności lub poufności danych osobowych zawartych w systemach teleinformatycznych. Podmiot publiczny będzie wówczas musiał zgłosić taki incydent zarówno do właściwego CSIRT (niezwłocznie, nie później niż 24 godziny od stwierdzenia naruszenia), jak i do Prezesa Urzędu Ochrony Danych Osobowych (w ciągu 72 godzin). W takim przypadku zgłoszenie incydentu do właściwego CSIRT nie będzie zwalniało z obowiązku wynikającego z przepisów RODO.

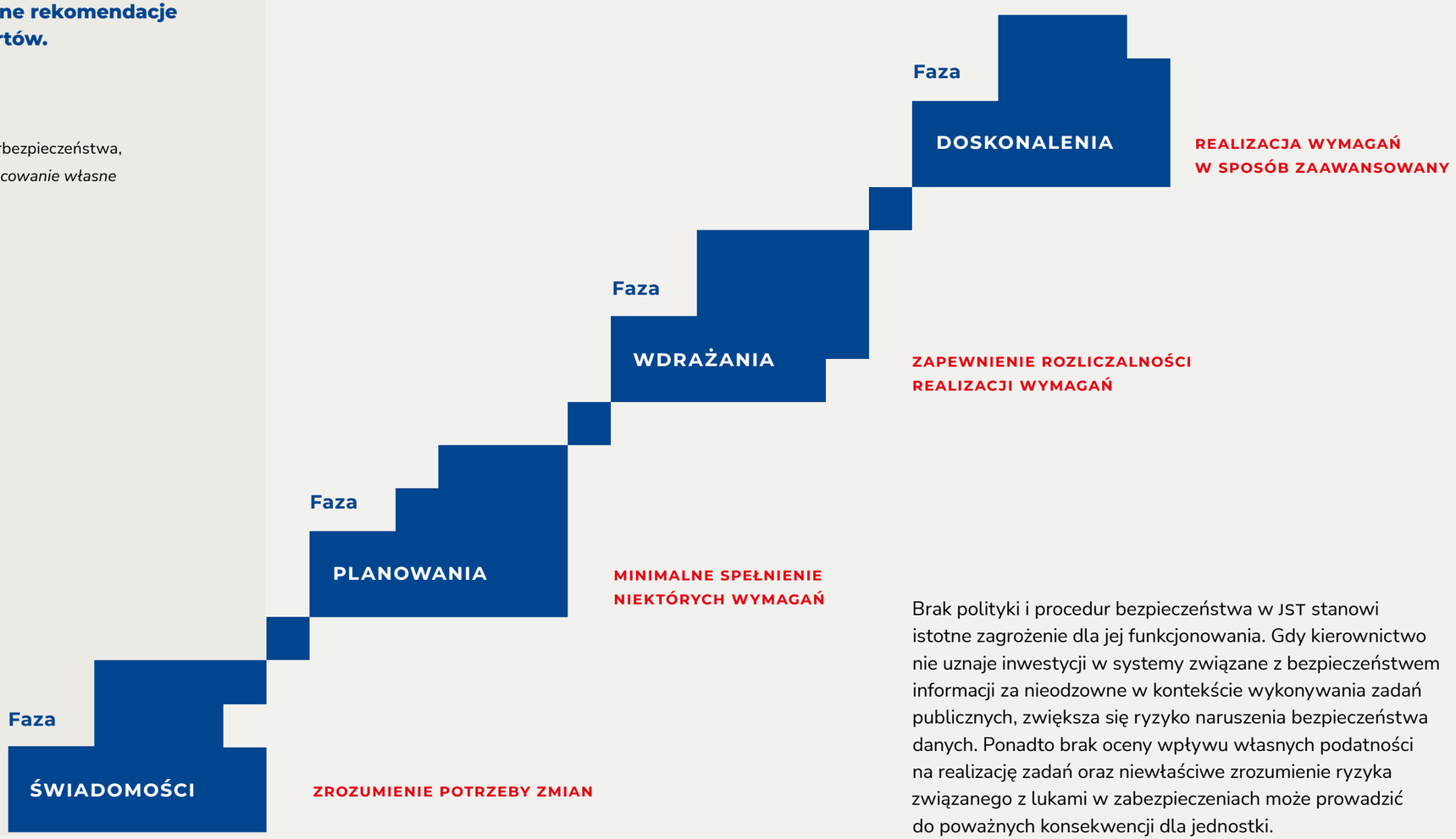
04

Planowanie rozwoju jednostki w obszarze cyberbezpieczeństwa

W ramach realizacji projektów „Cyfrowa Gmina”, „Cyfrowy Powiat” i „Cyfrowe Województwo” przeprowadzone zostały badania mające na celu ocenę stanu przygotowania JST do wypełniania minimalnych obowiązków w zakresie zapewnienia bezpieczeństwa teleinformatycznego. Wyniki tego badania (nazywanego „Diagnozą Cyberbezpieczeństwa”) wskazują na duże zróżnicowanie poziomu dojrzałości cyberbezpieczeństwa podmiotów. U dużego odsetka JST występują nawet problemy ze spełnieniem minimalnych wymogów bezpieczeństwa zdefiniowanych w obowiązujących przepisach prawa. Dlatego w niniejszym rozdziale zaprezentowano ścieżkę budowania odporności podmiotu na zagrożenia płynące z cyberprzestrzeni, która może ułatwić zaplanowanie działań w ramach projektu „Cyberbezpieczny Samorząd”.

Przygotowana na potrzeby tego Poradnika 4-fazowa ścieżka rozwoju JST w obszarze cyberbezpieczeństwa pokazuje, w jaki sposób stopniowo można podnosić zdolności jednostki, wdrażając kolejne rekomendacje przygotowane przez naszych ekspertów.

Rysunek 1. Poziomy rozwoju JST w obszarze cyberbezpieczeństwa, na podstawie RODO, uoKSC i KRI. *Opracowanie własne*



Brak polityki i procedur bezpieczeństwa w JST stanowi istotne zagrożenie dla jej funkcjonowania. Gdy kierownictwo nie uznaje inwestycji w systemy związane z bezpieczeństwem informacji za nieodzowne w kontekście wykonywania zadań publicznych, zwiększa się ryzyko naruszenia bezpieczeństwa danych. Ponadto brak oceny wpływu własnych podatności na realizację zadań oraz niewłaściwe zrozumienie ryzyka związanego z lukami w zabezpieczeniach może prowadzić do poważnych konsekwencji dla jednostki.

I. Faza świadomości

ZROZUMIENIE POTRZEBY ZMIAN

To początkowy etap ścieżki rozwoju cyberbezpieczeństwa. W tej fazie znajdują się jednostki, które dopiero nabierają świadomości istnienia zagrożeń cyberbezpieczeństwa i działają intuicyjnie, niespójnie, *ad hoc* oraz wyłącznie reaktywnie odpowiadają na wykryte incydenty lub w ogóle nie są ich świadome. Zaczynają rozpoznawać ryzyko dla realizacji zadań publicznych wynikające ze słabości zabezpieczeń. Nie mają zdefiniowanych zasad, procedur, polityk ani SZBI chroniących informacje oraz dysponują tylko niezbędnymi dla funkcjonowania wdrożeniami technicznymi, które nie uwzględniają wielu zagadnień cyberbezpieczeństwa.

II. Faza planowania

MINIMALNE SPEŁNIENIE NIEKTÓRYCH WYMAGAŃ

Ta faza charakteryzuje jednostkę, która chroni swoją infrastrukturę i zapewnia jej częściową ciągłość realizowania zadań publicznych (przynajmniej w minimalnym stopniu). JST w tej fazie jest świadoma zagrożeń i konieczności zapobiegania im oraz w pewnym stopniu podejmuje takie działania, wykorzystując kompetencje specjalistów, własne procedury i posiadane narzędzia. Wdrożone są mechanizmy bezpieczeństwa używanych aplikacji i sieci, ale zmiany w tym zakresie nie są zarządzane centralnie – powszechne są działania *ad hoc*. W tym stanie przeważa model, w którym instytucja ufa interakcji między użytkownikiem a systemami. Programy budowania świadomości na temat cyberzagrożeń są rozważne tylko w przypadku kluczowych pracowników, procedury bezpieczeństwa informacji są zdefiniowane nieformalnie, a analizę ryzyka przeprowadza się jedynie w ograniczonym zakresie.

III. Faza wdrażania

ZAPEWNIENIE ROZLICZALNOŚCI REALIZACJI WYMAGAŃ

W tej fazie JST posiadają wybrane polityki związane z bezpieczeństwem informacji. Niektóre aspekty interakcji użytkowników z systemami informacyjnymi są postrzegane ako potencjalne ryzyka. Tutaj nie podejmuje się już działań *ad hoc* – praca oparta jest na planowaniu lub wykorzystywaniu istniejących polityk, procedur, udokumentowanych procesów. Modele konfiguracji są wdrażane centralnie, stosowane są zasady bezpieczeństwa i procedury postępowania, stale rozwijana jest świadomość użytkowników, a zgodność JST z regulacjami wzrasta. Kontrole dostępu do informacji są obowiązkowe i ściśle monitorowane. Środki bezpieczeństwa wprowadza się na zasadzie oceny kosztu i korzyści chronionych informacji.

IV. Faza doskonalenia

REALIZACJA WYMAGAŃ W SPOSÓB ZAAWANSOWANY

Ta faza charakteryzuje się najogólniej zgodnością z wymaganiami KRI oraz uoKSC. Oznacza m.in. posiadanie kontroli nad bezpieczeństwem informacji w obrębie jednostki, monitorowaniem systemów, utrzymywaniem wysokiej świadomości zagrożeń i zdolności do reagowania na nie lub zapobiegania im. W JST w tej fazie istnieje kompleksowy plan utworzony na podstawie formalnych zasad i procedur operacyjnych, mających na celu zapobieganie, wykrywanie i korygowanie wykrytych problemów bezpieczeństwa. Aby jednostka miała pełną zgodność, zarządzanie bezpieczeństwem musi polegać na identyfikowaniu wszelkich symptomów związanych z naruszeniem bezpieczeństwa, a wykryte incydenty muszą być obsługiwane w zorganizowany sposób. Zaawansowany poziom dotyczy również architektury bezpieczeństwa informacji w jednostce. Istnieje system zapewniający identyfikowalność zbiorów informacji, użytkowników, systemów, urządzeń i oprogramowania.

Aby rozwój jednostki był zrównoważony konieczne jest prowadzenie działań jednocześnie w następujących trzech kierunkach:

O — ORGANIZACYJNE ŚRODKI

obejmujące działania doskonalące jednostkę w zakresie regulacji wewnętrznych, polityk i procedur ich wypełniania.

T — TECHNICZNE ŚRODKI

obejmujące wdrażanie i modernizowanie narzędzi.

K — KOMPETENCJE

obejmujące działania zmierzające do podniesienia świadomości na temat zagrożeń i metod ochrony oraz kompetencji specjalistycznych pracowników odpowiedzialnych za utrzymanie i rozwój obszaru cyberbezpieczeństwa.

05

Zarządzanie bezpieczeństwem informacji w JST

Nieodzowne dla ochrony przed cyberzagrożeniami oraz skutecznego działania w sytuacjach wystąpienia incydentu bezpieczeństwa jest wieloaspektowe podejście do zarządzania bezpieczeństwem. Wymaga to pełnego zrozumienia potencjalnych zagrożeń oraz zapewnienia skutecznych środków ochronnych. Zarządzanie bezpieczeństwem informacji w jednostce obejmuje szeroki zakres działań związanych zarówno z opracowaniem i wdrażaniem regulacji, polityk czy procedur, jak i budowaniem świadomości oraz podnoszeniem poziomu kompetencji pracowników. Jednym z pierwszych, podstawowych działań jest budowa Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

5.1 —— System Zarządzania Bezpieczeństwem Informacji

System Zarządzania Bezpieczeństwem Informacji stanowi niezwykle istotny aspekt w dzisiejszym środowisku informacyjnym. SZBI jest kompleksowym ramowym podejściem do identyfikacji, zarządzania i ochrony informacji w jednostki.

Zgodnie z § 20 ust. 1 rozporządzeniem KRI podmiot realizujący zadania publiczne:

- opracowuje i ustanawia,
- wdraża i eksploatuje,
- monitoruje i przegląda,
- oraz utrzymuje i doskonali

system zarządzania bezpieczeństwem informacji.

System zarządzania bezpieczeństwem informacji

zapewnia:

POUFNOŚĆ
ochronę informacji przed dostępem przez osoby nieupoważnione,

DOSTĘPNOŚĆ
zapewnienie możliwości osiągalności informacji „na żądanie”,

INTEGRALNOŚĆ
zabezpieczenie przed niewłaściwym (również przypadkowym) modyfikowaniem informacji lub ich zniszczeniem.

SZBI dotyczy takich atrybutów, jak:

- **autentyczność**
  możliwość zweryfikowania prawdziwości informacji;
- **rozliczalność**
  możliwość określenia osób mających dostęp do informacji oraz zapis procesów, jakim podlegała od ostatniego sprawdzania;
- **niezaprzeczalność**
  brak możliwości zanegowania swojego uczestnictwa w wymianie lub przetwarzaniu informacji;
- **niezawodność**
  zapewnienie bezawaryjnego systemu umożliwiającego dostęp i przetwarzanie informacji.

System Zarządzania Bezpieczeństwem Informacji (ang. *Information Security Management System* – ISMS) to kompleksowa i sformalizowana strategia zarządzania bezpieczeństwem przetwarzanych informacji w organizacji. Powinien być oparty na rzetelnie przeprowadzonej analizie ryzyka, uwzględniającej m.in. kontekst jednostki, wymagania prawe oraz wymagania interesariuszy.

Nie ma jednej, uniwersalnej strategii funkcjonowania SZBI odpowiadającej na potrzeby różnych organizacji. Uniwersalność SZBI zbudowanego w odniesieniu do wymagań PN-EN ISO/IEC 27001 pozwala zarządzać bezpieczeństwem informacji z uwzględnieniem procesów bezpieczeństwa i kolejności podejmowanych działań związanych z projektowanie, wdrożeniem oraz późniejszą eksploatacją i doskonaleniem systemu.

Tworząc i wdrażając SZBI, warto pamiętać o kilku istotnych aspektach:

- Bez wsparcia kierownictwa, zapewnienia budżetów oraz szkoleń podnoszących świadomość i kompetencje pracowników wdrożenie SZBI nie będzie możliwe.

- Opracowanie i ogłoszenie dokumentacji SZBI, często nazywane przez firmy zewnętrzne „wdrożeniem SZBI", nie jest gwarantem utrzymania deklarowanego początkowo poziomu bezpieczeństwa.

- SZBI bywa często utożsamiane z certyfikacją na zgodność z normą PN-EN ISO/IEC 27001, co jednak nie zawsze musi być konieczne. Takie wymaganie nie pojawia się w żadnym akcie prawnym opisującym obowiązki podmiotów publicznych.

- Realizacja SZBI odbywa się w tzw. cyklu ciągłego doskonalenia, znanego pod nazwą cyklu Deminga lub pętli PDCA – **P**lan (zaplanuj), **D**o (wykonaj), **C**heck (sprawdź), **A**ct (działaj). Nie jest to zatem proces jednorazowy, a cykliczny – wdrożenie to dopiero pierwszy krok.

- Przy definiowaniu i wdrażaniu SZBI potrzebne są odpowiednie kompetencje i umiejętności. Jeżeli jednostka nie jest w stanie ich zapewnić wewnętrznie – należy skorzystać ze wsparcia ekspertów zewnętrznych z zakresu bezpieczeństwa informacji i dzięki tej współpracy budować kompetencje w JST.

5.1.1 Podstawowe etapy budowania SZBI

Poniżej przedstawione korki i etapy budowania SZBI w JST stanowią jedynie zalecenia przykładowe. Każda jednostka jest inna, ma różne doświadczenia, kompetencje i potrzeby.

Informacje

Zarządzanie bezpieczeństwem informacji wymaga wcześniejszego zrozumienia, które informacje są najcenniejsze dla JST i najbardziej narażone na ryzyko naruszenia. Następnym krokiem jest zastosowanie odpowiednich środków ochrony – zarówno z poziomu proceduralnego, jak i środków technicznych. Często „informacje" są rozumiane przez pryzmat ochrony danych osobowych, a tymczasem jest to niewystarczające podejście. W jednostkach przetwarza się znacznie więcej informacji. Wśród informacji podlegających ochronie będą m.in. wszelkiego rodzaju dane, raporty, notatki służbowe, a także dokumentacja wewnętrzna.

Wsparcia kierownictwa

Przy podejmowaniu decyzji o wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji kluczowym krokiem powinno być potwierdzenie zaangażowania ze strony najwyższego kierownictwa JST. To właśnie ta grupa decyzyjna ma najistotniejsze znaczenie dla sukcesu takiego przedsięwzięcia, ponieważ decyduje o przydzielaniu niezbędnych zasobów i budżetu potrzebnych do utrzymania systemu zarządzania.

Na szczeblu kierownictwa wyznacza się cele dla SZBI, które są potem komunikowane i monitorowane w całej JST. Bez właściwego zaangażowania i zrozumienia ze strony kierownictwa wszelkie próby wdrożenia systemu zarządzania bezpieczeństwem informacji mogą spotkać się z niezrozumieniem, oporem, a nawet niepowodzeniem. Dlatego zawsze warto rozpocząć od zapewnienia, że najwyższe kierownictwo jest w pełni zaangażowane i świadome swojej roli w tym procesie.

Zasoby i ich wartość

Kolejnym krokiem jest inwentaryzacja zasobów (aktywów) związanych z przetwarzaniem informacji. Taka inwentaryzacja wykracza poza „spis z natury". Jest to systematyczny przegląd wszystkich zasobów JST, które są związane z opracowaniem, przechowywaniem i przetwarzaniem informacji. Warto zaznaczyć, że zasoby danych osobowych prawdopodobnie zostały już zidentyfikowane zgodnie z wymaganiami określonymi w Rozporządzeniu o Ochronie Danych Osobowych (UE) 2016/679.

Przykładowymi zasobami podlegającym inwentaryzacji będą:

- SPRZĘT INFORMATYCZNY – komputery, telefony, tablety, fizyczne nośniki danych;
- SERWERY I INFRASTRUKTURA SIECIOWA;
- ZASOBY LUDZKIE – kadra kierownicza, kluczowy informatyk, pracownicy oraz dostawcy;
- USŁUGI W CHMURZE;
- INFORMACJE POWIERZONE PRZEZ KLIENTÓW;
- POMIESZCZENIA I LOKALIZACJE;
- INNE, np. papierowe nośniki informacji.

Dla każdego wskazanego zasobu lub ich kategorii ustala się właściciela – czyli osobę odpowiedzialną.

Warto też dodać, że zgormadzone dane o zasobach uczestniczących w przetwarzaniu informacji w JST (aktywach) są kluczowym elementem zarządzania bezpieczeństwem. Wykorzystuje się je w wielu procesach bezpieczeństwa, np. są podstawowym elementem analizy ryzyka, pozwalają na zarządzanie podatnościami technicznymi czy zarządzanie aktualizacją.

Analiza ryzyka

Po zgromadzeniu danych z poprzedniego kroku należy przeprowadzić analizę ryzyka, czyli ocenić faktyczną możliwość wystąpienia negatywnego wpływu na dane zasoby. Trzeba przy tym uwzględnić cały kontekst JST, zakres przetwarzanych informacji oraz zasoby – od lokalizacji i związanych z nią zagrożeń (np. możliwość zalania, pożar czy włamanie) po ocenę prawdopodobieństwa ataku cyberprzestępców.

Prowadząc analizę ryzyka, warto wziąć pod uwagę aspekty wpływające na prawdopodobieństwo jego wystąpienia, np.

- atrakcyjność informacji przetwarzanych przez JST,
- motywację agresora i korzyści jakie może osiągnąć,
- popularność stosowanych przez JST technologii i dostępność narzędzi pozwalających na skuteczne przeprowadzenie ataku.

Należy uwzględnić także:

- zastosowane zabezpieczenia fizyczne, organizacyjne i techniczne;
- lokalizacje budynków i możliwość wystąpienia katastrof naturalnych, pożaru czy zalania;
- przerwy w dostawie prądu i dostępu do sieci/internetu oraz wpływ na realizowanie zadań i świadczone usługi;
- naruszenia prawa – wynikające z zaniedbania lub nieetycznego działania pracowników lub osób trzecich, ataków, jak i działalności cyberprzestępców.

Analiza ryzyka może zostać przeprowadzana w różny sposób, z zastosowaniem różnych metodyk. Może również bazować na wiedzy eksperckiej pracowników odpowiedzialnych za ten obszar. Ważne, aby była wykonywana cyklicznie w sposób udokumentowany i powtarzalny.

Poprawnie wykonana analiza ryzyka dostarcza informacji o istniejących zagrożeniach, potencjalnych skutkach materializacji ryzyka. Pozwala dopasować odpowiednie zabezpieczenia do chronionych zasobów, a kadrze kierowniczej ułatwia podejmowanie świadomych decyzji.

Wskazanie sposobu ochrony i ograniczenie skutków materializacji ryzyka to inaczej elementy planu przeciwdziałania ryzykom (planu postepowania z ryzykiem). Analiza ryzyka wspomaga proces decyzyjny oraz określenie narzędzi i mechanizmów bezpieczeństwa, a także definiuje niezbędne zakupy realizowane w procesie zakupowym. Innego rodzaju zabezpieczeń będzie potrzebować jednostka na poziomie miasta wojewódzkiego, zatrudniająca kilkaset osób, innych – JST na poziomie gminy wiejskiej. Istotne są również możliwości budżetowe. Wszystkie rodzaje zabezpieczeń powinny podlegać inwentaryzacji, ze szczególnym uwzględnieniem czasu przewidzianego przez producenta na wspieranie danego produktu lub usługi. Nieaktualizowane i niewspierane zabezpieczenia stają się zagrożeniem dla bezpieczeństwa JST.

Analiza ryzyka powinna być regularnie powtarzana – zasoby informacyjne oraz technologie nieustannie się zmieniają, co będzie wymagało okresowego dopasowania sytuacji do nowych okoliczności.

Role

Pojęcie roli w kontekście Systemu Zarządzania Bezpieczeństwem Informacji jest istotne ze względu na prawidłowe przypisane zadań i odpowiedzialności, a także określenie potrzeb szkoleniowych.

Należy określić następujące role w jednostce:

- PRACOWNIK – każda osoba zatrudniona w JST.
- AUDYTOR WEWNĘTRZNY – rola odpowiedzialna za przeprowadzenie audytów systemów zarządzania.
- ADMINISTRATOR IT – rola reprezentująca osoby odpowiedzialne za zarządzanie infrastrukturą IT JST.
- NAJWYŻSZE KIEROWNICTWO – rola reprezentująca grupę odpowiedzialną za wytyczanie kierunków i kontrolę JST na najwyższym szczeblu.
- IOD – Inspektor Ochrony Danych, który sprawuje pieczę nad ochroną danych osobowych w JST.
- DOSTAWCY I PODWYKONAWCY, odpowiedzialni za dostarczenie lub utrzymanie usług, narzędzi oprogramowania uczestniczących lub wpływających na bezpieczeństwo przetwarzanych informacji.

W zależności od JST niektóre z tych ról można łączyć, przy czym warto mieć na uwadze, że nałożenie zbyt dużej odpowiedzialności na jedną osobę może mieć negatywny wpływ na jakość wykonywanych działań.

Na tym etapie jednostka powinna określić kompetencje oraz umiejętności wymagane do wypełnienia określonych ról. Warto zdefiniować na tym etapie rodzaje potrzebnych szkoleń.

Dokumentacja

Zarządzanie bezpieczeństwem informacji w jednostce to zadanie wymagające precyzyjnego przygotowania i wdrożenia zestawu regulacji wewnętrznych. Udokumentują one wszystkie kroki i uregulują postępowanie pracowników zapewniające zachowanie odpowiedniego poziomu bezpieczeństwa informacji. Takie regulacje to np. polityki, schematy organizacyjne, regulaminy i zasady, procedury i instrukcje, oraz nadrzędna wobec nich – polityka bezpieczeństwa.

Polityka Bezpieczeństwa Informacji (PBI) to podstawowy zestaw dokumentów, który odgrywa kluczową rolę w zarządzaniu bezpieczeństwem. Ten dokument – jeśli zostanie prawidłowo przygotowany, zaakceptowany i zaimplementowany – stanowi podstawę Systemu Zarządzania Bezpieczeństwem Informacji dla środków technicznych, proceduralnych i personalnych wykorzystywanych do ochrony informacji w jednostce.

Należy pamiętać, że PBI powinno definiować cele oraz zakres systemu zarządzania bezpieczeństwem informacji, a także zawierać deklarację wsparcia zarządzania bezpieczeństwem przez kierownictwo jednostki.

Dokumentację systemu należy opracować w odniesieniu do wymagań jednostki, z uwzględnieniem obszarów, których dotyczy, oraz możliwości prezentowania poszczególnych dokumentów różnym grupom odbiorców.

- Jednym z powielanych błędów jest tworzenie dokumentacji SZBI jako jednego dużego dokumentu (PBI), zawierającego wszystkie aspekty bezpieczeństwa.
- Często dokumentacja SZBI mylnie jest utożsamiana z polityką przetwarzania danych osobowych oraz instrukcją zarządzania systemem

teleinformatycznym w odniesieniu do wymagań ustawy o ochronie danych osobowych z 1997 r. Dobrą praktyką jest łączenie obu obszarów, gdyż ochrona informacji i zapewnienie bezpieczeństwa przetwarzaniem danych osobowych wykorzystuje te same procesy bezpieczeństwa, np. zarządzanie ryzykiem w obszarze informacji i obszarze technicznym, zarządzanie podatnościami technicznymi, zarządzanie aktualizacją czy zarządzanie incydentami bezpieczeństwa.

Aby mieć pewność, że wymagania bezpieczeństwa informacji będą odpowiednio realizowane, Politykę Bezpieczeństwa Informacji należy odpowiednio ogłosić, formalnie zatwierdzić i przeszkolić pracowników w tym zakresie.

Podsumowanie

System Zarządzania Bezpieczeństwem Informacji (SZBI) to kompleksowa, sformalizowana strategia bezpieczeństwa informacji, bazująca na analizie ryzyka, dostosowana do specyfiki danej jednostki. Opracowanie i publikacja dokumentacji SZBI nie jest jednak gwarancją utrzymania bezpieczeństwa. Od JST wymaga się ciągłego monitoringu i doskonalenia modelu PDCA (Planuj – Wdrażaj – Sprawdzaj – Działaj). Dla skutecznego wdrożenia SZBI kluczowe jest zaangażowanie i zrozumienie ze strony kierownictwa, które określa cele i przekazuje je jednostce.

5.2 Podnoszenie poziomu świadomości cyberbezpieczeństwa

W obliczu dynamicznego rozwoju technologicznego i digitalizacji rola technologii informacyjno-komunikacyjnych w sektorze publicznym znacznie wzrosła. W celu zapewnienia skutecznej i efektywnej realizacji swoich zadań jednostki sektora publicznego, w tym samorządowego, wykorzystują różne platformy i narzędzia elektroniczne. Umożliwiają one szybki dostęp do informacji, usprawniają procesy administracyjne oraz zwiększają transparentność działań.

Wykorzystywanie narzędzi informatycznych w codziennej pracy staje się normą, a wraz z tym rośnie potrzeba świadomości i kompetencji z zakresu bezpieczeństwa dla wszystkich pracowników. Ciągłe podnoszenie poziomu kompetencji cyfrowych pracowników jest w tej sytuacji niezbędne. Kompetencje cyfrowe obejmują m.in. umiejętność korzystania z oprogramowania, rozumienie zasad bezpieczeństwa cyfrowego, efektywne wyszukiwanie i przetwarzanie informacji, a także umiejętność komunikacji online. Niezwykle ważne są kompetencje w obszarze szeroko pojętego bezpieczeństwa ze szczególnym uwzględnieniem (cyber)bezpieczeństwa. Wszyscy pracownicy, a w szczególności pracownicy wykorzystujący w swej codziennej pracy narzędzia informatyczne, powinni znać podstawowe zasady i politykę bezpieczeństwa, a także swoją rolę i odpowiedzialność w systemie bezpieczeństwa jednostki.

Cyberprzestępcy wykorzystują nieświadomość użytkowników jako metodę ataku na instytucje publiczne.

MANIPULACJE

Szczególnie popularnym sposobem są strategie oparte na manipulacji i ludzkich błędach, zachęcające do kliknięcia w linki zawarte w wiadomościach e-mail. Umożliwia to pozyskanie poufnych danych użytkownika, naruszenie sieci wewnętrznej jednostki lub zainfekowanie komputera złośliwym oprogramowaniem. Potencjalne konsekwencje mogą być bardzo poważne dla JST. W zależności od działań poszczególnych pracowników mogą prowadzić do ujawnienia danych logowania do systemów wewnętrznych (efekt skutecznej kampanii phishingowej) czy też zaszyfrowania danych przez oprogramowanie typu ransomware. Ostatecznie wpływa to na możliwość świadczenia usług i realizacji zadań przez JST oraz może powodować skutki prawne, finansowe lub utratę wizerunku jednostki.

PHISHING

RANSOMWARE

SZKOLENIA

Aby sprostać rosnącym wymaganiom, jednostki sektora publicznego powinny zapewnić swoim pracownikom odpowiednie szkolenia i możliwości rozwoju kompetencji cyfrowych. Warto inwestować w programy szkoleniowe, które obejmują zarówno podstawowe umiejętności obsługi technologii, jak i bardziej zaawansowane zagadnienia związane z analizą danych, programowaniem czy wykorzystaniem narzędzi analitycznych, a także poruszające kwestie prawne oraz psychospołeczne aspekty cyberzagrożeń.

UŚWIADAMIANIE

Warto również zauważyć, że oprócz kształtowania typowych kompetencji o charakterze technicznym, należy prowadzić działania uświadamiające pracowników, gdyż sama świadomość o bieżących zagrożeniach związana z użytkowaniem nowych technologii zdecydowanie zmniejsza poziom ekspozycji na ataki. Pozwala m.in. na odróżnienie typowego błędu technicznego od potencjalnego ataku, pomaga uniknąć potencjalnego zagrożenia, a w przypadku wystąpienia naruszenia – sprzyja podjęciu podstawowych działań ograniczających skutki wystąpienia incydentu oraz zgłoszeniu incydentu do odpowiednich komórek.

Działania edukacyjne są kluczowym elementem w podnoszeniu świadomości pracowników w zakresie cyberbezpieczeństwa.

KULTURA BEZPIECZEŃSTWA

Informowanie pracowników o zagrożeniach, organizowanie szkoleń dotyczących praktyk bezpieczeństwa oraz regularne przypomnienia o zasadach bezpiecznego korzystania z narzędzi informatycznych mają istotny wpływ na redukcję ryzyka ataków cyberprzestępczych. Zaplanowane działania na rzecz podnoszenia poziomu cyber-bezpieczeństwa dla całego personelu danej JST budują kulturę bezpieczeństwa jednostki, zapewniają spójność sposobów przeciwdziałania atakom oraz skutecznych metod reagowania. Odpowiednio przeszkolony i świadomy personel jest ważnym elementem systemu bezpieczeństwa i uzupełnia działanie zabezpieczeń technologicznych oraz realizuje wewnętrzną politykę bezpieczeństwa. Świadomy użytkownik rozumie istotę nakładanych przez jednostkę procedur, które często odbierane są jako zbędne ograniczenia i utrudnienia w realizacji bieżących zadań.

ZRÓŻNICOWANY PROGRAM SZKOLEŃ

Specyfika pracy oraz rola pracownika w systemie cyberbezpieczeń-stwa jednostki mają wpływ na typ oddziaływań szkoleniowych oraz ich zakres tematyczny. Szkolenia powinny różnić się w zależności od konkretnej grupy docelowej. Istotna jest tutaj identyfikacja potrzeb poszczególnych grup na podstawie ich roli zawodowej, poziomu wiedzy, dostępu do danych i innych czynników mających wpływ na ich zaangażowanie w zagadnienia związane z cyberbezpieczeństwem. Podstawowe szkolenia z zakresu cyberbezpieczeństwa powinny obejmować wszystkich pracowników, natomiast kadra kierownicza oraz personel IT wymagają bardziej specjalistycznej wiedzy i umiejętności, aby efektywnie zarządzać i chronić infrastrukturę informatyczną jednostki. W uzasadnionych przypadkach pracownicy IT powinni uczestniczyć w szkoleniach certyfikowanych przez renomowane instytucje, które dostarczą im zaawansowanych technik i strategii ochrony cyberbezpieczeństwa. Proponowany podział tematyczny szkoleń został zaproponowany w tabeli poniżej.

ROZWÓJ

Ponadto jednostki sektora publicznego powinny promować atmosferę ciągłego uczenia się i innowacyjności. Można to osiągnąć poprzez podejmowanie innych działań (newslettery, plakaty informacyjne, konkursy) czy organizowanie warsztatów i konferencji, które umożliwią pracownikom wymianę wiedzy i doświadczeń z innymi specjalistami. Ważne jest również zachęcanie do korzystania z zasobów edukacyjnych dostępnych online, takich jak kursy internetowe, webinaria czy platformy e-learningowe.

Tabela 1 zawiera przykłady tematów, które mogą zostać wykorzystane w zakresie podnoszenia kompetencji i świadomości pracowników w obszarze bezpieczeństwa informacji i cyberbezpieczeństwa.

METODY I NARZĘDZIA

Skuteczna realizacja programu szkoleniowego dla pracowników w zakresie cyberbezpieczeństwa powinna zakładać opracowanie sposobów i narzędzi ewaluacji. Pozwolą one na zdiagnozowanie potrzeb szkoleniowych, wiedzy i umiejętności czy poznanie opinii i poziomu satysfakcji. Sprawdzanie wiedzy po szkoleniu umożliwi ocenę skuteczności szkolenia i zidentyfikowanie obszarów, które wymagają dalszej pracy, oraz wpłynie na motywację pracowników. Należy pamiętać, że pomiary mają stanowić wartość dodaną i służyć wzmacnianiu pracownika, a nie być elementem oceny w karierze zawodowej.

Podnoszenie poziomu świadomości cyberbezpieczeństwa

Tabela 1. Podnoszenie świadomości cyberbezpieczeństwa w jednostce

Szkolenia

	WSZYSCY PRACOWNICY	KADRA KIEROWNICZA	SPECJALIŚCI IT
1.	**Bezpieczeństwo informacji – podstawowe wiadomości, z uwzględnieniem regulacji wewnętrznych oraz wymagań rozporządzenia KRI** ■ Wewnętrzne procedury w obszarze bezpieczeństwa informacji cyberbezpieczeństwa ■ Wymagania dla pracowników wynikające z KRI, UOKSC oraz RODO ■ System Zarządzania Bezpieczeństwem Informacji w praktyce	■ Podstawy prawne cyberbezpieczeństwa ■ Wymogi wynikające z KRI, UOKSC i RODO ■ Przegląd znanych typów ataków na JST ■ Przegląd nowoczesnych narzędzi i usług cyberbezpieczeństwa (jako wsparcie procesu zakupowego) ■ Zarządzanie ryzykiem w bezpieczeństwie informacji i obszarach technicznych. ■ System Zarzadzania Bezpieczeństwem Informacji – jak skutecznie wdrożyć SZBI ■ Ciągłość działania – dlaczego jest istotna i jak ją wdrożyć ■ Współpraca w ramach s46 ■ Identyfikowanie zagrożeń – jak wdrożyć odpowiednie zabezpieczenia	■ Podstawy bezpieczeństwa sieci ■ Aspekty techniczne najpopularniejszych ataków i metody reagowania ■ Zabezpieczanie poczty elektronicznej ■ Zabezpieczanie serwisów www ■ Ochrona przed atakami DDoS ■ Profilaktyka cyberzagrożeń ze szczególnym uwzględnieniem zarządzania kopiami zapasowymi ■ Przegląd źródeł wiedzy o zagrożeniach ■ Podstawy zabezpieczenia ciągłości działania ■ Identyfikacja podatności i aktualizacja oprogramowania ■ Zarządzanie incydentem
2.	**Przegląd najpopularniejszych zagrożeń i zasady bezpiecznego korzystania z internetu** ■ Ochrona informacji i prywatność w internecie ■ Ransomware jako poważne zagrożenie dla JST ■ Phishing, oszustwa i wyłudzenia z uwzględnieniem oszustwa typu BEC (Business E-mail Compromise) ■ Cyberhigiena, w tym bezpieczeństwo urządzeń i bezpieczeństwo fizyczne ■ Bezpieczne hasła i uwierzytelnienie dwuskładnikowe ■ Wewnętrzne zalecenia i rekomendacje, w tym sposoby reakcji na incydenty bezpieczeństwa		

Inne oddziaływania edukacyjne

Newslettery, wewnętrzne webinary, plakaty w ogólnodostępnych miejscach, komunikaty i ostrzeżenia, podcasty, konkursy, quizy

Ważne!

Jednostka powinna zadbać o sformułowanie planu budowania świadomości cyberbezpieczeństwa w instytucji, rozumianego jako wielowymiarowy, zaplanowany zestaw działań mających na celu zwiększenie wiedzy i umiejętności pracowników związanych z cyberbezpieczeństwem. Plan ten obejmuje szereg elementów, tj. identyfikację kluczowych obszarów tematycznych, zdefiniowanie celów i efektów, wyznaczenie osoby/zespołu odpowiedzialnego za jego przygotowanie, realizację, aktualizację, a także zaplanowanie potencjalnych ryzyk i metod pomiaru wskaźników sukcesu.

Treść szkoleń obejmujących wszystkich pracowników powinna być **spójna z zaleceniami jednostki** (polityką bezpieczeństwa oraz podrzędnymi wobec niej procesami i procedurami). Warto ustalić z organizatorem szkoleń, w jaki sposób będzie się odnosić do dokumentacji wewnętrznej.

Szkolenia z zakresu cyberbezpieczeństwa mogą przyjmować **różną formę**. Mogą to być prowadzone przez ekspertów szkolenia stacjonarne lub online, a także różne formy e-learningu czy blended learningu. Istotne jest, aby szkolenia były dostosowane do konkretnych potrzeb i stanowisk pracy pracowników. W ten sposób możliwe będzie skuteczne poszerzanie wiedzy i umiejętności cyfrowych. Należy pamiętać, że wiedza o cyberbezpieczeństwie ewoluuje, a zalecania sprzed kliku lat mogą być już nieaktualne. Te zmiany najszybciej będą wprowadzane do szkoleń prowadzonych przez ekspertów.

Ewaluacja szkoleń jest bardzo istotnym czynnikiem zarówno pod względem oceny konkretnego produktu szkoleniowego, jak i efektów szkolenia dla podniesienia poziomu świadomości cyberbezpieczeństwa.

Ważne jest, aby program szkoleniowy z zakresu cyberbezpieczeństwa dla pracowników uwzględniał także opracowanie metod i narzędzi do pomiaru jego skuteczności. Przeprowadzenie różnorodnych badań pozwoli na identyfikację potrzeb szkoleniowych, ocenę poziomu wiedzy i umiejętności, a także poznanie opinii i poziomu zadowolenia pracowników z programu. Dzięki temu można dokonać diagnozy i dostosować program, aby był jak najbardziej efektywny.

Ciekawą formą sprawdzania wiedzy nabytej po szkoleniu jest próbna **symulacja ataku phishingowego** z oceną skuteczności. Należy pamiętać, że jest to element podnoszenia świadomości polecany zaawansowanym organizacjom z ustanowionym programem szkoleń i procedurą/procesem zgłaszania podejrzanych wiadomości elektronicznych.

Podnoszenie poziomu świadomości cyberbezpieczeństwa to **nie tylko szkolenia**. Odpowiednie informacje w skrótowej formie powinny być zamieszczane też w intranecie lub innej przestrzeni wspólnej dla pracowników. Ostrzeżenia i inne komunikaty bezpieczeństwa mogą pojawiać się także w formie mailowej.

Szkolenia i inne oddziaływania edukacyjne z zakresu cyberbezpieczeństwa powinny towarzyszyć pracownikom przez **cały okres zatrudnienia** w placówce i być regularnie powtarzane. Warto przygotować plany szkoleniowe.

Pamiętaj!

Sprawdź ofertę **darmowych szkoleń** dla podmiotów KSC oferowanych przez instytucje publiczne, np. Ministerstwo Cyfryzacji. Traktuj je jednak jako uzupełnienie i odświeżenie wiedzy.

Bądź świadom, że szkolenia oferowane przez firmy sprzedające produkty i rozwiązania komercyjne mogą zawierać głównie **lokowanie produktu** i nie będą realizować założonych celów edukacyjnych.

Przed podjęciem decyzji o zakupie szkolenia warto przeprowadzić **dokładną analizę produktów** dostępnych na rynku i dobrać produkt najbardziej odpowiadający potrzebom jednostki. Cena nie może być ostatecznym kryterium.

Zadbaj o **podnoszenie świadomości interesariuszy jednostki**. Możesz utworzyć odpowiednią zakładkę na stronie internetowej JST. Skorzystaj z materiałów opracowanych przez ekspertów NASK-PIB (CERT Polska, ECSM – Europejski Miesiąc Cyberbezpieczeństwa) czy informacji zawartych w Bazie Wiedzy w serwisie gov.pl

Szkolenia specjalistyczne

W wybranych przypadkach, na podstawie przeprowadzonej analizy ryzyka, jednostka może zidentyfikować potrzebę podniesienia kwalifikacji personelu zajmującego się kwestiami cyberbezpieczeństwa lub konieczność zatrudnienia osób o odpowiedniej, udokumentowanej wiedzy specjalistycznej. Pomocne mogą być wtedy szkolenia certyfikowane. Obszerną listę certyfikatów z zakresu cyberbezpieczeństwa można znaleźć m.in. w Rozporządzeniu Rady Ministrów z 19 stycznia 2022 r. w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa. Ponadto szkolenia specjalistyczne powinny towarzyszyć również wdrożeniom systemów operacyjnych oraz innych usług i produktów, podnoszących poziom cyberbezpieczeństwa.

Specjalistyczne szkolenia certyfikowane przez renomowane instytucje mogą być bardzo kosztowne. Należy zweryfikować, czy pracownicy będą w stanie wykorzystać zdobytą wiedzę i umiejętności w swojej pracy w JST. Można rozważyć podpisywanie umów lojalnościowych.

W związku ze zwiększającym się zapotrzebowaniem na specjalistów cyberbezpieczeństwa – zarówno w sektorze publicznym, jak i prywatnym – aktualnie trwają prace nad przygotowaniem sektorowej ramy kwalifikacji, zgodnej z ustawą o ZSK (Zintegrowany System Kwalifikacji). Zostaną tam opisane i uporządkowane kwalifikacje wymagane od pracowników odpowiedzialnych za bezpieczeństwo w sieci, a także propozycje ścieżek rozwoju i podnoszenia kwalifikacji.

06

Wykaz wymagań bezpieczeństwa dla podmiotów publicznych

Podmioty publiczne w Polsce podlegają różnorodnym obowiązkom prawnym, które regulują ich działalność. W poprzednim rozdziale zostały przedstawione przepisy prawne dotyczące obowiązków, które obligują podmioty publiczne do utrzymania minimalnego poziomu bezpieczeństwa w sferze cyfrowej.

Niniejszy rozdział zawiera szczegółowy wykaz wymagań wynikających z rozporządzenia KRI oraz uoKSC wraz z obszernymi opisami, mającymi na celu ułatwienie zrozumienia oczekiwań ustawodawcy.

Przedstawione poniżej przykłady rekomendowanych działań są zbiorem propozycji wynikających z dobrych praktyk. Mogą wesprzeć jednostkę w realizacji wypełnienia wymagań, ale nie powinny być traktowane jak zindywidualizowane zalecenia dla jednostki, ze względu na zróżnicowanie sytuacji wyjściowej, potrzeby i uwarunkowania organizacyjne.

W — WYMAGANIA
oznaczenia wymagań dla podmiotów publicznych wynikających z rozporządzenia KRI oraz uoKSC

O — ORGANIZACYJNE ŚRODKI
obejmujące działania doskonalące jednostkę w zakresie regulacji wewnętrznych, polityk i procedur ich wypełniania.

T — TECHNICZNE ŚRODKI
obejmujące wdrażanie i modernizowanie narzędzi.

K — KOMPETENCJE
obejmujące działania zmierzające do podniesienia świadomości na temat zagrożeń i metod ochrony oraz kompetencji specjalistycznych pracowników odpowiedzialnych za utrzymanie i rozwój obszaru cyberbezpieczeństwa.

01

Wdrożenie systemu zarządzania bezpieczeństwem informacji (SZBI)

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §20 UST. 1**

TREŚĆ PODSTAWY

Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Opis wymagania

System Zarządzania Bezpieczeństwem Informacji (SZBI) – czyli zestaw polityk, procesów, procedur, kompetencji i narzędzi – powinien być opracowany, zatwierdzony przez kierownictwo, opublikowany, zakomunikowany pracownikom i właściwym stronom zewnętrznym oraz na bieżąco aktualizowany zgodnie z zewnętrznymi wymaganiami. W wielu organizacjach stosuje się także obowiązkowe szkolenia dotyczące SZBI (interaktywne lub online) oraz zbierane są oświadczenia o zapoznaniu się z nimi zarówno przez wszystkich pracowników, jak i podmioty zewnętrzne (które muszą zapoznać się z wybranymi fragmentami Polityki Bezpieczeństwa Informacji, np. z polityką obowiązującą dostawców usług zewnętrznych). Ponieważ samorząd realizuje zadania publiczne przy pomocy wielu jednostek organizacyjnych, wymogu wdrożenia Systemu Zarządzania Polityki Bezpieczeństwa nie należy ograniczać tylko do procedur obowiązujących w urzędzie gminy, starostowie powiatowym czy urzędzie marszałkowskim.

Rekomendowane działania – przykłady

Wdrożenie wymagań § 20 i § 21 rozporządzenia KRI

- Projekt Systemu Zarządzania Bezpieczeństwem Informacji.
- Opracowanie dokumentacji SZBI.
- Przeprowadzenie audytu otwarcia GAP Analysis.

Realizacja rekomendacji z raportu po audycie zgodności z rozporządzeniem KRI

02

PBI zgodne z aktualnymi, zewnętrznymi wymaganiami

KIERUNEK ROZWOJU: 

PODSTAWA: **KRI §20 UST. 2 PKT 1**

TREŚĆ PODSTAWY

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

Opis wymagania

Polityka Bezpieczeństwa Informacji musi być zgodna z innymi regulacjami zewnętrznymi oraz wewnętrznymi, a zgodność ta powinna być monitorowana w trybie ciągłym lub cyklicznie. W razie potrzeby PBI powinna być uaktualniana lub tworzona nowa – np. dotyczące nowych obszarów, nieuwzględnionych dotąd w PBI.

Rekomendowane działania – przykłady

1. Utworzenie system monitorowania zmian w otoczeniu

Należy utworzyć system monitorowania zmian w otoczeniu, takich jak zmiany w technologii, zagrożeniach, przepisach i regulacjach dotyczących bezpieczeństwa informacji. Trzeba ustalić odpowiednie kanały informacyjne, aby być na bieżąco z nowymi wydarzeniami i trendami w dziedzinie cyberbezpieczeństwa.

2. Przeprowadzanie regularnej analizy ryzyka

Należy przeprowadzać regularne analizy ryzyka, aby ocenić potencjalne zagrożenia i słabości w związku z aktualnym otoczeniem, a także zidentyfikować obszary, w których regulacje wewnętrzne mogą wymagać aktualizacji, aby dostosować się do zmieniających się warunków. Należy skoncentrować się na nowych technologiach, rozwijających się zagrożeniach i zmieniających się przepisach prawnych.

3. Aktualizowanie polityk i procedur

Na podstawie wyników analizy ryzyka należy dokonać aktualizacji polityk i procedur wewnętrznych dotyczących bezpieczeństwa informacji oraz wprowadzać zmiany, które uwzględniają nowe wymogi dotyczące aktualnego otoczenia. Polityki powinny być jasne, zrozumiałe i dostępne dla wszystkich pracowników. Należy upewnić się, że wszyscy pracownicy są świadomi zmian i przestrzegają nowych zasad.

4. Szkolenie pracowników

Należy organizować regularne szkolenia dla pracowników, aby poinformować ich o nowych zagrożeniach i zmianach w przepisach dotyczących bezpieczeństwa informacji. Warto skoncentrować się na aktualnym otoczeniu i związanych z nim regulacjach. Szkolenia powinny obejmować zagrożenia wynikające z nowych technologii, odpowiedzialności prawnej – związanej z naruszeniem zasad bezpieczeństwa informacji – oraz sposobami zapewnienia bezpieczeństwa w nowym otoczeniu.

5. Współpraca z zewnętrznymi ekspertami

Należy nawiązać współpracę z zewnętrznymi ekspertami w dziedzinie cyberbezpieczeństwa i regulacji, korzystać z ich wiedzy i doświadczenia w celu oceny aktualnych zasad wewnętrznych i wprowadzenia niezbędnych aktualizacji. Zewnętrzne audyty i oceny mogą również pomóc w identyfikacji obszarów wymagających ulepszeń.

6. Przeprowadzanie testów i oceny zgodności

Należy regularnie przeprowadzać testy i oceny zgodności w celu sprawdzenia, czy aktualizacje regulacji wewnętrznych są skutecznie wdrażane i przestrzegane. Należy weryfikować, czy nowe zasady są odpowiednio stosowane i przynoszą oczekiwane rezultaty, oraz identyfikować obszary wymagające dalszych ulepszeń i podejmować odpowiednie działania naprawcze.

03

Inwentaryzacja aktywów i ich konfiguracji

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §20 UST. 2 PKT 2**

TREŚĆ PODSTAWY

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

Opis wymagania

Utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania to proces monitorowania i aktualizowania informacji dotyczących wykorzystywanego sprzętu i oprogramowania w celu lepszego zarządzania, zabezpieczania i kontrolowania kosztów. Proces ten polega na regularnym monitorowaniu i aktualizowaniu informacji dotyczących rodzaju i konfiguracji używanego sprzętu i oprogramowania – na utrzymaniu szczegółowej listy wszystkich urządzeń komputerowych i oprogramowania, które są wykorzystywane do przetwarzania informacji w organizacji. Na tej liście powinny znajdować się takie informacje, jak: rodzaj komputerów, laptopów, drukarek, serwerów i innych urządzeń, zainstalowane na nich oprogramowanie i jego wersje. Aby utrzymać aktualność inwentaryzacji, konieczne jest regularne sprawdzanie i uaktualnianie informacji na liście. Nowe urządzenia lub oprogramowanie należy dodać do inwentarza. W przypadku, gdy istniejące urządzenia lub oprogramowanie zostają zastąpione lub usunięte, należy odpowiednio zaktualizować listę. Pomaga to w zarządzaniu sprzętem i oprogramowaniem, ułatwia planowanie zakupów i aktualizacji oraz przewidywanie potrzeb i unikanie nieoczekiwanych problemów.

Dzięki aktualnym informacjom można lepiej monitorować potencjalne zagrożenia bezpieczeństwa i łatwiej zidentyfikować słabe punkty, które mogą wymagać wzmocnienia.

Utrzymywanie aktualności inwentaryzacji ułatwia śledzenie kosztów związanych z utrzymaniem sprzętu i oprogramowania. Pozwala na kontrolowanie wydatków na zakupy, naprawy i aktualizacje.

Prowadzona na bieżąco baza aktywów jest podstawą do prawidłowej realizacji wielu procesów, m.in. zarządzania ryzykiem, zarządzania podatnościami technicznymi, incydentami czy aktualizacji oprogramowania.

Rekomendowane działania – przykłady

1. Regularne aktualizacje inwentaryzacji

Należy cyklicznie robić przeglądy i aktualizacje inwentaryzacji sprzętu i oprogramowania, dodawać nowe elementy, usuwać przestarzałe, a także aktualizować informacje dotyczące rodzaju i konfiguracji. Warto wprowadzać procedury i harmonogramy, które zapewnią regularne i systematyczne przeglądy inwentaryzacji.

2. Automatyzacja inwentaryzacji

Należy wprowadzić narzędzia i systemy automatyzujące proces inwentaryzacji. Można wykorzystać narzędzia do skanowania sieci i oprogramowania, które mogą identyfikować i monitorować urządzenia i oprogramowanie w czasie rzeczywistym. Automatyzacja ułatwi utrzymanie aktualności inwentaryzacji i umożliwi szybkie wykrycie niezidentyfikowanych urządzeń lub oprogramowania.

3. Polityki i procedury zarządzania inwentaryzacją

Należy opracować jasne polityki i procedury zarządzania inwentaryzacją sprzętu i oprogramowania oraz określić odpowiedzialności za utrzymanie aktualności inwentaryzacji, wymagania dotyczące raportowania zmian oraz procedury audytowe. Trzeba się także upewnić, że wszyscy pracownicy są świadomi istnienia polityk i procedur oraz ich przestrzegają.

4. Monitorowanie i wykrywanie nieautoryzowanego sprzętu lub oprogramowania

Należy wdrożyć mechanizmy monitorowania sieci i systemów, które umożliwią wykrycie nieautoryzowanego sprzętu lub oprogramowania. Można wykorzystać narzędzia, takie jak systemy wykrywania intruzów (IDS/IPS) lub systemy zarządzania zdarzeniami bezpieczeństwa (SIEM), aby monitorować i alarmować w przypadku wykrycia nieznanych lub nieautoryzowanych urządzeń lub oprogramowania.

5. Szkolenia pracowników

Należy organizować regularne szkolenia dla pracowników, aby podnieść poziom ich świadomości na temat znaczenia utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania. Szkolenia powinny obejmować edukację na temat zagrożeń wynikających z nieaktualnych inwentaryzacji, jak również zasady i procedury dotyczące utrzymywania ich aktualności.

6. Audyty inwentaryzacyjne

Należy regularnie przeprowadzać audyty inwentaryzacyjne, aby sprawdzić zgodność z politykami i procedurami zarządzania inwentaryzacją. Audyty pomogą w identyfikacji ewentualnych braków lub niezgodności w aktualizacji inwentaryzacji, umożliwiając podjęcie odpowiednich działań naprawczych.

04

Zarządzanie ryzykiem

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §20 UST. 2 PKT 3**

TREŚĆ PODSTAWY

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.

Opis wymagania

Spełnienie wymagania można osiągnąć w kilku krokach:

1. **Przeprowadzenie analizy ryzyka** – dokonanie przeglądu systemu, procesów i zasobów informacyjnych w organizacji, identyfikacja potencjalnych zagrożeń, które mogą wpływać na integralność, dostępność lub poufność informacji.

2. **Ocena ryzyka**, czyli prawdopodobieństwa wystąpienia zagrożeń oraz konsekwencji, jakie mogą one mieć dla integralności, dostępności lub poufności informacji. Przydzielanie ryzyka do kategorii, np. wysokie, średnie lub niskie, aby lepiej zrozumieć priorytety i skalę zagrożeń.

3. **Opracowanie planu działania** na podstawie wyników analizy ryzyka, określającego konkretne kroki prowadzące do minimalizacji ryzyka. Wprowadzenie odpowiednich kontroli, procedur i zabezpieczeń, które będą chronić informacje i zapewnią ich integralność, dostępność i poufność.

4. **Wdrażanie środków ochrony** i upewnienie się, że środki te są zgodne z wynikami analizy ryzyka oraz przyczynią się do minimalizacji ryzyka utraty integralności, dostępności lub poufności informacji.

5. **Regularne, okresowe przeglądy analizy ryzyka** w celu sprawdzenia, czy istnieją nowe zagrożenia lub zmiany, które mogą wymagać aktualizacji planu działania. Monitorowanie środowiska i wprowadzanie niezbędnych zmian dla utrzymania lub podniesienia poziomu bezpieczeństwa informacji.

6. **Zapewnienie pracownikom szkoleń**, aby podnieść ich świadomość na temat zagrożeń dla integralności, dostępności i poufności informacji oraz poziomu wiedzy dotyczącej postępowania w przypadku wystąpienia takich zagrożeń. Edukowanie ich na temat istniejących procedur i postępowań, które minimalizują ryzyko.

Istotne są także regularnie przeprowadzane analizy ryzyka i aktualizacja działań zapobiegawczych, aby utrzymać odpowiedni poziom bezpieczeństwa informacji, minimalizować ryzyko utraty integralności, dostępności lub poufności.

Rekomendowane działania – przykłady

Przy poprawnym prowadzeniu cyklicznej analizy ryzyka jej wyniki powinny być oceniane. Stosownie do ocen należy podejmować odpowiednie działania mające na celu minimalizowanie tych ryzyk. Działania te mogą obejmować wdrożenie dodatkowych zabezpieczeń, takich jak np. zapory sieciowe, systemy antywirusowe, systemy monitorowania i zarządzania zdarzeniami, procedury zabezpieczeń fizycznych czy szyfrowanie danych itd. Dla lepszej ochrony informacji mogą również być wymagane zmiany w procedurach lub politykach organizacyjnych.

1. Zintegrowanego systemu monitorowania

Zintegrowany system monitorowania umożliwi ciągłe monitorowanie systemów teleinformatycznych, sieci i zasobów informacyjnych. Te systemy mogą wykrywać anomalie, nieprawidłowości i potencjalne zagrożenia, co umożliwi szybką reakcję i minimalizację ryzyka.

2. Regularne przeprowadzanie proaktywnych testów penetracyjnych

Proaktywne test penetracyjne pomogą zidentyfikować słabe punkty i luki w zabezpieczeniach systemowych. Takie testy powinny być przeprowadzane przez specjalistów, którzy symulują ataki cyberprzestępców w celu oceny skuteczności obecnych środków ochronnych i identyfikacji obszarów wymagających poprawy.

3. Regularne aktualizacje oprogramowania i stosowanie poprawek bezpieczeństwa

Zdarza się, że w nieaktualnym oprogramowaniu występują luki w zabezpieczeniach, które mogą być wykorzystane przez cyberprzestępców. Należy upewnić się, że wszelkie używane systemy operacyjne, aplikacje i urządzenia są regularnie aktualizowane, aby minimalizować ryzyko.

4. Zadbanie o odpowiednie zabezpieczenia fizyczne

Zabezpieczenia fizyczne, takie jak kontrola dostępu do pomieszczeń, monitorowanie wideo, zabezpieczenie serwerowni i centrum danych, pozwalają na ochronę fizycznego dostępu do urządzeń i zasobów informacyjnych.

5. Opracowanie planu reagowania na incydenty

Plan reagowania na incydenty określa procedury, odpowiedzialności i kroki do podjęcia w przypadku naruszenia bezpieczeństwa informacji. Szybka i skuteczna reakcja na incydenty pomoże minimalizować skutki i ograniczyć ryzyko dla integralności, dostępności i poufności informacji.

Każda jednostka jest inna, powinna zatem dostosować swoje działania i mechanizmy doskonalące do własnego specyficznego środowiska i potrzeb. Ważne jest regularne monitorowanie i aktualizacja działań w celu zapewnienia optymalnego poziomu cyberbezpieczeństwa.

05

Role, udział i odpowiedzialność za elementy bezpieczeństwa informacji

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §20 UST. 2 PKT 4**

TREŚĆ PODSTAWY

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji.

Opis wymagania

Spełnienie wymagania można osiągnąć w kilku etapach:

1. **Dokładne określenie uprawnień i odpowiedzialności** każdej osoby zaangażowanej w proces przetwarzania informacji. To oznacza, że należy jasno zdefiniować, jakie zadania i obowiązki są związane z przetwarzaniem informacji, jakie są wymagania w zakresie bezpieczeństwa oraz do jakich danych wskazana osoba ma mieć dostęp. Na podstawie tych informacji można określić, jakie uprawnienia i kwalifikacje są niezbędne dla poszczególnych osób.

2. Zapewnienie, aby osoby zaangażowane w proces przetwarzania informacji otrzymały **odpowiednie szkolenia i miały niezbędne kwalifikacje**. Szkolenia powinny obejmować zarówno ogólne zasady bezpieczeństwa informacji, jak i specyficzne procedury i praktyki związane z przetwarzaniem danych w danej jednostce. W zależności od rodzaju informacji i ryzyka może być konieczne uzyskanie certyfikacji lub specjalistycznych umiejętności.

3. Stworzenie i wdrożenie **procesu weryfikacji i nadzoru**, który zapewni, że osoby zaangażowane w proces przetwarzania informacji będą do tego uprawnione oraz że będą się angażować w sposób odpowiedni do swoich zadań. Proces ten może obejmować regularne oceny kwalifikacji, weryfikację poziomu dostępu do systemów i danych, a także **monitorowanie działań i audyty**, aby upewnić się, że osoby przestrzegają określonych procedur i zasad bezpieczeństwa.

4. W miarę jak zmieniają się zadania, obowiązki i wymagania w zakresie bezpieczeństwa informacji, należy **regularnie aktualizować uprawnienia i kwalifikacje osób** zaangażowanych w proces przetwarzania danych. Proces zarządzania zmianą jest ważny, aby upewnić się, że każda osoba posiada aktualne i adekwatne umiejętności i wiedzę, aby wykonywać swoje zadania w sposób bezpieczny i skuteczny. Może to wymagać dodatkowych szkoleń, przeprowadzenia przeglądu i dostosowania uprawnień lub wprowadzenia nowych procedur.

5. Istotne jest, aby **promować i rozwijać kulturę bezpieczeństwa informacji** w jednostce. To oznacza, że każda osoba powinna być świadoma znaczenia bezpieczeństwa informacji i odpowiedzialności związanych z przetwarzaniem danych. Jednostka powinna promować świadomość i edukację w zakresie bezpieczeństwa, a także zachęcać do zgłaszania incydentów i udziału w programach szkoleniowych i inicjatywach związanych z bezpieczeństwem informacji.

Rekomendowane działania – przykłady

1. Wdrożenie polityki uprawnień i dostępu

Polityka uprawnień i dostępu pozwoli na kontrolę dostępu do danych i systemów. Zapewnia, że tylko uprawnione osoby mają dostęp do odpowiednich zasobów. Polityka powinna określać jasno, jakie uprawnienia są wymagane dla poszczególnych ról i stanowisk, a także jakie są zasady nadawania, zarządzania i odbierania uprawnień. Regularne przeglądy i audyty uprawnień powinny być przeprowadzane w celu zapewnienia, że osoby posiadające dostęp są nadal uprawnione i działają w sposób zgodny z obowiązującymi zasadami bezpieczeństwa.

2. Wykorzystywanie skutecznych procesów rekrutacyjnych

Skuteczne procesy rekrutacyjne obejmują weryfikację kwalifikacji i sprawdzanie referencji potencjalnych pracowników. Zapewnienie, że nowo zatrudnione osoby otrzymują odpowiednie szkolenia z zakresu bezpieczeństwa informacji, które dostosowane są do ich roli i odpowiedzialności. Szkolenia powinny obejmować zasady bezpieczeństwa, procedury, polityki i świadomość zagrożeń cybernetycznych. Regularne szkolenia powinny być również dostępne dla wszystkich pracowników w celu utrzymania i aktualizacji ich wiedzy.

3. Wdrożenie polityki zarządzania uprawnieniami

Zapewnienie, że osoby zaangażowane w proces przetwarzania informacji posiadają odpowiednie uprawnienia, wymaga systematycznego zarządzania zmianą w jednostce. W przypadku zmiany ról, zadań lub obowiązków istotne jest, żeby przeprowadzać odpowiednie przeglądy i aktualizacje uprawnień.

4. Wykorzystanie zaawansowanych systemów identyfikacji i uwierzytelniania

Zastosowanie uwierzytelniania wieloskładnikowego (MFA) może znacznie zwiększyć bezpieczeństwo informacji. Wdrożenie MFA wymaga od pracowników posiadania dodatkowego czynnika uwierzytelniającego, np. kodu jednorazowego generowanego na urządzeniu mobilnym, tokenu lub certyfikatu – oprócz tradycyjnego hasła. Tego rodzaju dodatkowe zabezpieczenie utrudnia nieuprawnionym osobom dostęp do danych, nawet jeśli uzyskają dostęp do hasła.

5. Monitorowanie zmian w jednostce

Dział IT lub zespół ds. bezpieczeństwa informacji powinien monitorować zmiany w jednostce, weryfikować potrzeby dotyczące uprawnień i dostępu oraz wprowadzać odpowiednie modyfikacje w systemie zarządzania uprawnieniami.

6. Przeglądy i audyty systemów

Regularne przeglądy i audyty systemów oraz działań związanych z przetwarzaniem informacji są niezbędne do zapewnienia zgodności z zasadami bezpieczeństwa. Należy przeprowadzać regularne przeglądy uprawnień i dostępu, weryfikować, czy osoby posiadające dostęp mają odpowiednie uprawnienia, oraz monitorować ich działania w systemie.

06

Nadawanie, zarządzanie, przegląd i weryfikacja oraz odbieranie uprawnień użytkowników

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §20 UST. 2 PKT 5**

TREŚĆ PODSTAWY

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.

Opis wymagania

Spełnienie wymagania można zapewnić, podejmując następujące kroki:

1. **Regularne monitorowanie zmian w organizacji**, szczególnie dotyczących zadań, obowiązków i odpowiedzialności osób zaangażowanych w proces przetwarzania informacji, a także zmian personalnych, takich jak awanse, przeniesienia czy zwolnienia.

2. **Utrzymywanie komunikacji** pomiędzy wszystkimi działami i działem zarządzania zasobami ludzkimi oraz z przełożonymi osób zaangażowanych w przetwarzanie informacji. Informowanie ich wszystkich o potrzebie zmiany uprawnień w przypadku zmiany zadań. Dzielenie się istotnymi informacjami dotyczącymi bezpieczeństwa informacji i związanych z tym wymogów.

3. Zapewnienie, że organizacja **posiada odpowiednie procesy wewnętrzne** dotyczące zmian uprawnień. Ustalenie szybkich i efektywnych mechanizmów, które umożliwią dostosowanie uprawnień osób zaangażowanych w przetwarzanie informacji do ich aktualnych zadań i obowiązków. Wdrożenie takiego procesu pomoże zapewnić, że uprawnienia będą aktualizowane bezzwłocznie w przypadku zmian zadań osób.

4. Przeprowadzanie **regularnych przeglądów uprawnień** w celu potwierdzenia, czy osoby posiadające dostęp do danych mają odpowiednie uprawnienia i są one nadal zgodne z realizowanymi zadaniami. Dokonywanie weryfikacji i dostosowywania uprawnień zgodnie z nowymi wymaganiami – jeśli dochodzi do zmian w zadaniach określonych osób.

5. Rozważenie **wdrożenia automatyzacji** procesu zmiany uprawnień. Można skorzystać z systemów zarządzania uprawnieniami, które umożliwiają elastyczne zarządzanie i łatwą zmianę dostępów w zależności od aktualnych zadań i obowiązków pracowników.

Rekomendowane działania – przykłady

1. Wdrożenie narzędzi monitorujących aktywność użytkowników w systemach i aplikacjach

Pozwala to na monitorowanie, jakie czynności podejmują osoby zaangażowane w proces przetwarzania informacji i czy ich działania są zgodne z przyznanymi uprawnieniami. W przypadku zmiany zadań monitorowanie aktywności pomoże w wykryciu potencjalnych nieprawidłowości i wykaże konieczność zmiany uprawnień.

2. Zapewnienie regularnych szkoleń z zakresu bezpieczeństwa informacji

Szkolenia powinny obejmować również procedury dotyczące zmiany uprawnień, a także podkreślać znaczenie szybkiej i skutecznej zmiany uprawnień w przypadku zmiany zadań. Ważna jest również edukacja pracowników na temat potencjalnych zagrożeń i ryzyka związanego z niewłaściwymi uprawnieniami.

3. Opracowanie i wdrożenie procedur wewnętrznych

Procedury powinny jasno określać kroki do podjęcia w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji oraz zawierać wytyczne dotyczące identyfikacji zmian, komunikacji, weryfikacji uprawnień i wprowadzania zmian w systemach. Procesy te powinny być zrozumiałe, łatwo dostępne i stosowane w praktyce.

4. Regularne przeprowadzanie przeglądów i audytów

W celu zweryfikowania, czy uprawnienia są nadawane i zmieniane zgodnie z wymaganiami, niezbędne jest regularne przeprowadzanie przeglądów i audytów – sprawdzanie, czy procesy zmiany uprawnień są skuteczne i czy są przestrzegane. Przeglądy i audyty mogą pomóc w identyfikacji ewentualnych słabości i wprowadzeniu odpowiednich ulepszeń.

5. Wykorzystanie systemu zarządzania uprawnieniami

Wykorzystanie rozwiązań (systemu) umożliwia elastyczne zarządzanie uprawnieniami i szybką zmianę dostępu w przypadku zmiany zadań. Taki system powinien umożliwiać łatwą identyfikację i modyfikację uprawnień, a także automatyczne powiadamianie o potrzebie zmiany uprawnień.

07

Podnoszenie świadomości, kształcenie i szkolenia z zakresu bezpieczeństwa informacji

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §20 UST. 2 PKT 6**

TREŚĆ PODSTAWY

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: zagrożenia bezpieczeństwa informacji; skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna; stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

Opis wymagania

Spełnienie wymaganie można osiągnąć w następujący sposób:

1. **Opracowanie programu szkoleniowego**, który będzie obejmował wszystkie istotne zagadnienia związane z bezpieczeństwem informacji. W ramach programu szkoleniowego należy uwzględnić zagrożenia związane z cyberbezpieczeństwem, takie jak hacking, phishing, malware itp. Wyjaśnienie potencjalnych skutków naruszenia zasad bezpieczeństwa informacji, zarówno dla organizacji, jak i dla jednostek odpowiedzialnych za przetwarzanie danych. Poruszenie kwestii prawnych, takich jak: ochrona danych osobowych, przepisy dotyczące poufności informacji oraz odpowiedzialność prawna za naruszenie zasad bezpieczeństwa informacji.
2. **Przygotowanie materiałów szkoleniowych**, które będą łatwo dostępne dla pracowników. Mogą to być prezentacje, broszury, pliki PDF lub filmy instruktażowe. Materiały powinny być zrozumiałe dla odbiorców i zawierać praktyczne wskazówki dotyczące zapewnienia bezpieczeństwa informacji.
3. **Organizowanie szkoleń praktycznych**, które umożliwią osobom zaangażowanym w proces przetwarzania informacji zrozumienie i praktyczne zastosowanie środków zapewniających bezpieczeństwo informacji.
4. **Promowanie świadomości bezpieczeństwa informacji przez kampanie edukacyjne i testy wiedzy.** Przeprowadzanie regularnych testów sprawdzających poziom wiedzy pracowników na temat zasad bezpieczeństwa informacji. Umożliwienie pracownikom regularnego sprawdzania swojej wiedzy i umiejętności może pomóc w utrzymaniu wysokiego poziomu świadomości i zaangażowania w kwestiach bezpieczeństwa informacji.
5. **Monitorowanie efektywności szkoleń i ocena ich skuteczności.** Regularne zbieranie informacji zwrotnych od uczestników szkoleń pomoże dowiedzieć się, czy szkolenia są zrozumiałe, pomocne i adekwatne do potrzeb. Analizowanie wyników, dostosowywanie programu szkoleniowego i ulepszanie go w celu ciągłego doskonalenia wiedzy o bezpieczeństwie informacji.

Dążenie do ciągłego doskonalenia szkoleń i podnoszenia świadomości w zakresie bezpieczeństwa informacji pomoże osobom zaangażowanym w proces przetwarzania informacji lepiej zrozumieć zagrożenia i skutki naruszeń zasad bezpieczeństwa, jak również skutecznie stosować środki zapewniające bezpieczeństwo informacji w codziennej pracy.

Rekomendowane działania – przykłady

1. Organizowanie szkoleń z zakresu cyberbezpieczeństwa

Tematyka szkoleń powinna dotyczyć m.in. zagrożeń bezpieczeństwa informacji, takich jak hacking, phishing, malware, ataki ransomware itp. Szczególną uwagę należy zwrócić na zagadnienia związane z identyfikacją podejrzanych wiadomości e-mail, bezpiecznym korzystaniem z haseł, zabezpieczaniem urządzeń mobilnych i ochroną danych osobowych, a także aspektami prawnymi cyberbezpieczeństwa.

2. Przeprowadzanie regularnych testów

Testy sprawdzające wiedzę i umiejętności pracowników powinny dotyczyć zagrożeń i zasad bezpieczeństwa informacji. Mogą obejmować symulacje ataków, zagadki dotyczące zasad bezpieczeństwa lub krótkie quizy online. Analizowanie wyników testów, identyfikowanie obszarów wymagających poprawy, koncentrowanie się na tych obszarach podczas kolejnych szkoleń.

3. Dostępność procedur i polityk

Polityki i procedury dotyczące bezpieczeństwa informacji powinny być jasne, zrozumiałe i dostępne dla wszystkich pracowników oraz obejmować tematy takie jak: bezpieczne korzystanie z systemów, ochrona poufności informacji, zarządzanie hasłami, korzystanie z urządzeń firmowych i zabezpieczanie sieci. Wszyscy pracownicy jednostki oraz kontrahenci powinni być regularnie informowani o aktualizacjach w politykach i procedurach bezpieczeństwa oraz przechodzić odpowiednie szkolenia w tym zakresie.

08

Rejestrowanie i monitorowanie zdarzeń w dostępie do informacji

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §20 UST. 2 PKT 7A**

TREŚĆ PODSTAWY

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez: a) monitorowanie dostępu do informacji, b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji.

Opis wymagania

Spełnienie wymagania może oznaczać konieczność wykonania następujących kroków:

1. W pierwszej kolejności konieczne jest **ustalenie odpowiednich zabezpieczeń** dostępu do informacji, takich jak hasła, identyfikatory, autoryzacja dwuetapowa itp. oraz upewnienie się, że wyłącznie upoważnione osoby mają dostęp do informacji.

2. **Stosowanie zasady minimalnego uprzywilejowania** oznacza nadawanie pracownikom uprawnień tylko na minimalnym poziomie dostępu i tylko do informacji, które są im niezbędne do wykonywania ich zadań. Celem takich działań jest minimalizowanie ryzyka nadużycia uprawnień.

3. **Przeprowadzanie regularnych audytów dostępu** w celu monitorowania, kto ma dostęp do informacji i jakie czynności wykonuje. W przypadku wykrycia podejrzanych aktywności należy podejmować odpowiednie środki zaradcze.

4. **Wdrożenie systemu monitorowania zdarzeń**, który będzie analizował aktywność w systemach teleinformatycznych i sieciach. Monitorowanie logów zdarzeń w celu wykrywania nieprawidłowości, podejrzanych aktywności lub prób nieuprawnionego dostępu.

5. **Wprowadzenie systemów alarmowych**, które będą reagować na podejrzane działania lub próby nieuprawnionego dostępu. Systemy te mogą ostrzegać administratorów lub personel odpowiedzialny za bezpieczeństwo informacji w przypadku wykrycia niepożądanych zdarzeń lub zagrożeń.

Ochrona informacji jest procesem ciągłym, dlatego ważne jest regularne monitorowanie, aktualizacja i doskonalenie środków ochronnych dla zapewnienia skutecznej ochrony przed wszelkimi zagrożeniami.

Rekomendowane działania – przykłady

1. Wdrożenie systemu zarządzania tożsamościami IAM

System umożliwia scentralizowane zarządzanie uprawnieniami dostępu do informacji. Pozwoli to uzyskać pełną kontrolę nad tym, kto ma dostęp do jakich danych i jakie czynności może wykonywać.

2. Wdrożenie systemów alarmowych i powiadamiania

Systemy będą ostrzegać przed podejrzanymi lub nieautoryzowanymi próbami dostępu do informacji. Powiadomienia powinny być wysyłane do administratorów, zespołu odpowiedzialnego za bezpieczeństwo informacji lub odpowiednich osób, aby umożliwić szybką reakcję w przypadku wykrycia zagrożeń.

3. Szczegółowe logowanie działań użytkowników i monitorowanie dzienników zdarzeń systemowych

Regularne przeglądanie tych dzienników w celu wykrywania nieprawidłowości, podejrzanych aktywności lub prób nieuprawnionego dostępu. Automatyczne narzędzia analizy logów mogą pomóc w identyfikacji podejrzanych wzorców lub zachowań.

4. Wdrożenie systemu monitorowania zdarzeń SIEM

System pozwoli na automatyczne gromadzenie, analizę i monitorowanie zdarzeń związanych z dostępem do informacji. Dzięki niemu można wykrywać podejrzane aktywności, ataki lub nieprawidłowości w systemach teleinformatycznych.

5. Ustanowienie zasad zbierania informacji

Informacje o zdarzeniach, ich korelacjach, powiadomieniach i alarmach w systemie monitoringu zdarzeń powinny być zbierane zgodnie z najlepszymi praktykami i ustanowionymi zasadami. Można dowolnie konfigurować powiadomienia informujące o wykrytych podejrzanych aktywnościach lub próbach naruszenia bezpieczeństwa informacji.

6. Wykorzystanie narzędzi do monitorowania ruchu sieciowego

Narzędzia pozwolą identyfikować nietypowe wzorce ruchu lub podejrzane aktywności. Może to umożliwić wykrycie prób nieuprawnionego dostępu lub ataków na systemy informatyczne.

7. Wykorzystanie narzędzi do analizy zachowań użytkowników

Narzędzia, które monitorują aktywność użytkowników i identyfikują podejrzane lub nietypowe zachowania, mogą wykrywać np. nieprawidłowe użycie uprawnień czy próby kradzieży informacji.

Dla skutecznej ochrony informacji przed kradzieżą lub nieuprawnionym dostępem ważne jest połączenie odpowiednich narzędzi technologicznych, procedur operacyjnych i świadomości pracowników. Systematyczne doskonalenie i aktualizacja tych działań są kluczowe dla zapewnienia wysokiego poziomu cyberbezpieczeństwa.

09

Wykrywanie niepożądanych zdarzeń w infrastrukturze IT

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §20 UST. 2 PKT 7B**

TREŚĆ PODSTAWY

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez: a) monitorowanie dostępu do informacji, b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji.

Opis wymagania

Do spełnienia tego wymagania niezbędne są warunki bardzo podobne do tych opisanych w wymaganiu dotyczącym zapewnienia monitorowania, ponieważ wykrywać można tylko te zdarzenia, które podlegają monitorowaniu w jakiejkolwiek formie. Zatem wykrywanie niepożądanych zdarzeń wiąże się z następującymi działaniami:

1. **Monitorowanie logów systemowych**, które może spowodować wykrycie aktywności, takich jak nieautoryzowane próby logowania, zmiany uprawnień czy podejrzane działania użytkowników.

2. **Analiza ruchu sieciowego** może pomóc w wykryciu nieautoryzowanych połączeń, prób ataków lub podejrzanych aktywności sieciowych. Narzędzia do ochrony sieci, takie jak IDS (Intrusion Detection System) lub IPS (Intrusion Prevention System), mogą automatycznie wykrywać niebezpieczne zachowania w sieci i reagować na nie.

3. **Wykorzystanie systemów detekcji anomalii** do analizy zachowania systemów i użytkowników pozwala identyfikować nieprawidłowości i nietypowe wzorce w ich działaniach. Przykładowo – niespodziewane zmiany we wzorcach ruchu sieciowego, podejrzane transfery danych lub nietypowe działania użytkowników mogą być sygnałem niepożądanych zdarzeń.

4. **Wykorzystanie systemów monitoringu zdarzeń** (SIEM – Security Information and Event Management), które zbierają, gromadzą, korelują, analizują i zgłaszają zdarzenia związane z bezpieczeństwem informacji. Mogą one wykrywać nieprawidłowości, podejrzane aktywności lub ataki, wykorzystując zaawansowane algorytmy i reguły.

5. **Wykonywanie testów penetracyjnych** (pentestów) polegające na symulowaniu ataków na systemy i aplikacje w celu identyfikacji ich słabości. Dzięki takim testom są wykrywane potencjalne luki w zabezpieczeniach, które mogłyby być wykorzystane do niepożądanych aktywności. Testy i badania bezpieczeństwa podsumowuje raport końcowy zawierający rekomendacje.

Rekomendowane działania – przykłady

1. Analizowanie logów systemowych

Analizowanie logów systemowych (dzienników zdarzeń, dostępów, bezpieczeństwa, aplikacji itp.) w celu wykrycia podejrzanych aktywności lub nieprawidłowości. Mogą one wskazywać na próby nieautoryzowanych działań związanych z przetwarzaniem informacji.

2. Wykorzystacie narzędzi do monitorowania ruchu sieciowego

Narzędzia do monitorowania ruchu sieciowego analizują i rejestrują wszelką komunikację w sieci. Dzięki nim można wykryć podejrzane wzorce ruchu, ataki sieciowe, próby penetracji systemów lub nieuprawnione transmisje danych.

3. Wdrożenie systemów detekcji zagrożeń IDS i systemów zapobiegania włamaniom IPS

Powyższe systemy analizują sieć i aplikacje w celu wykrywania nieprawidłowych lub złośliwych aktywności. Mogą ostrzegać o próbach włamań, atakach lub nieprawidłowym wykorzystaniu uprawnień oraz im zapobiegać.

4. Analiza zachowań użytkowników, monitorowanie i analiza ich aktywności w systemach i sieciach przy pomocy odpowiednich narzędzi

Dzięki temu można nie tylko wykryć nieautoryzowane działania, nieprawidłowe użycie uprawnień, próby kradzieży danych lub inne podejrzane zachowania, ale także blokować próby tego typu działań.

5. Wykorzystanie systemów wykrywania złośliwego oprogramowania

Rozwiązania te analizują i skanują systemy w poszukiwaniu potencjalnych zagrożeń. Takie systemy mogą wykrywać i blokować aktywności wirusów, trojanów, ransomware i innego złośliwego oprogramowania.

10

Zapobieganie niechcianym zdarzeniom w infrastrukturze IT

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §20 UST. 2 PKT 7C)**

TREŚĆ PODSTAWY

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez: a) monitorowanie dostępu do informacji, b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji.

Opis wymagania

Spełnienie wymagania można osiągnąć na bardzo wiele sposobów i przy pomocy bardzo wielu mechanizmów:

1. Można osiągnąć to pośrednio – przez wykorzystanie odpowiednich rodzajów **prewencji** oraz wielu zabezpieczeń adekwatnych do indywidulanych potrzeb, oczekiwanych poziomów bezpieczeństwa oraz rodzajów zabezpieczanych zasobów i informacji.
2. Można stosować wiele **mechanizmów ochrony aktywnej**, która działa cały czas i filtruje, szyfruje lub blokuje określone rodzaje aktywności czy transmisje.
3. Można stosować bardziej bezpośrednie formy reagowania na konkretne typy zagrożeń materializujących się już w infrastrukturze IT w postaci wirusów, ataków różnych typów (phishing, malware, DDoS, ransomware) czy innych incydentów.

Wiele form reakcji na niepożądane zdarzenia czy ataki można automatyzować.

Istnieje wiele innych technik i narzędzi, które można wykorzystać w celu zapewnienia bezpieczeństwa na poziomie systemów operacyjnych, usług sieciowych i aplikacji. Ważne jest systematyczne i kompleksowe podejście do zabezpieczeń, uwzględniające zarówno techniczne, jak i organizacyjne aspekty ochrony informacji.

Rekomendowane działania – przykłady

1. **Wymaganie stosowania silnych haseł i implementacja autoryzacji dwuskładnikowej,** które pomagają w zabezpieczeniu dostępu do systemów i aplikacji przed nieautoryzowanym dostępem.

2. **Regularne aktualizowanie systemów operacyjnych, usług sieciowych i aplikacji**

Regularne aktualizacje dostarczają poprawek bezpieczeństwa, które zamykają znane luki i usuwają podatności. Regularne stosowanie aktualizacji minimalizuje ryzyko wykorzystania słabych punktów przez nieautoryzowany dostęp.

3. **Używanie zapór sieciowych**

Pozwala to na kontrolę ruchu sieciowego i blokowanie nieautoryzowanego dostępu do systemów i usług sieciowych. Firewall może blokować podejrzane lub niepożądane połączenia.

4. **Kontrola dostępu na poziomie użytkowników**

Implementacja odpowiednich mechanizmów kontroli dostępu, takich jak nadawanie uprawnień użytkownikom na zasadzie najmniejszych przywilejów, ogranicza możliwość nieautoryzowanego dostępu do poufnych danych czy krytycznych funkcji systemu.

5. **Wykorzystanie systemu klasy IDM do ujednoliconego zarządzania tożsamościami użytkowników w danej infrastrukturze**

6. **Wykorzystanie mechanizmów kontroli dostępu uprzywilejowanego (PAM) do baz danych, aplikacji czy innych zasobów**

7. **Wykorzystanie mechanizmów wykrywania incydentów i automatycznego reagowania na nie (XDR, EDR)**

8. **Wykorzystanie polityki braku zaufania (Zero Trust) i konieczność uwierzytelniania** wszelkich użytkowników i ich działań w dostępie do wszelkich zasobów.

9. **Szyfrowanie danych**

Zastosowanie mechanizmów szyfrowania danych na poziomie systemów operacyjnych, usług sieciowych i aplikacji zapewnia ochronę przed nieautoryzowanym odczytem lub modyfikacją danych. Szyfrowanie może być wykorzystywane na różnych warstwach, takich jak szyfrowanie dysków, protokołów sieciowych czy baz danych.

Istnieje bardzo wiele klas rozwiązań zabezpieczających do zastosowania w różnych organizacjach, w różnej skali i do bardzo różnych celów.

11

Zasady bezpiecznej pracy z urządzeniami mobilnymi

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §20 UST. 2 PKT 8**

TREŚĆ PODSTAWY

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.

Opis wymagania

Spełnienie wymagania oznacza, że organizacja stawia nacisk na zapewnienie odpowiednich środków ochrony danych i informacji, które są przetwarzane na urządzeniach mobilnych (takich jak smartfony, tablety) oraz podczas pracy wykonywanej z dowolnego miejsca poza tradycyjnym miejscem pracy (np. z domu).

Te zasady mają na celu minimalizowanie ryzyka naruszenia bezpieczeństwa informacji. Ponadto chronią pracowników oraz organizację przed różnymi zagrożeniami, takimi jak kradzież danych, nieautoryzowany dostęp, utrata poufności lub uszkodzenie informacji.

Zasadne jest stworzenie **osobnej polityki korzystania z urządzeń mobilnych** przez użytkowników w danej organizacji i opisanie w niej zarówno procedur wewnętrznych, jak i zastosowanych w organizacji mechanizmów zabezpieczających związanych z wykorzystywaniem urządzeń mobilnych. Osobna polityka może precyzować zasady pracy zdalnej.

Rekomendowane działania – przykłady

1. Korzystanie z **bezpiecznych połączeń internetowych** podczas pracy na odległość.

2. **Wykorzystywanie protokołów szyfrowania**, takich jak VPN do ochrony przesyłanych danych przed nieautoryzowanym dostępem.

3. Regularne **aktualizacje oprogramowania urządzenia mobilnego, systemu operacyjnego i aplikacji** do najnowszych wersji. Aktualizacje często zawierają poprawki bezpieczeństwa, które pomagają w zapobieganiu zagrożeniom.

4. **Używanie silnych, unikalnych haseł** do logowania się do urządzeń mobilnych i aplikacji. Unikanie używania tych samych haseł na różnych platformach, korzystanie z menedżera haseł, który pomoże w zarządzaniu bezpiecznymi hasłami i generowaniu ich.

5. Ochrona urządzenia przez **włączenie funkcji blokady ekranu**, takiej jak kod PIN, wzór twarzy lub odcisk palca. W przypadku kradzieży lub utraty urządzenia taka ochrona uniemożliwi dostęp do danych osobom nieuprawnionym.

6. **Unikanie korzystania z publicznych sieci Wi-Fi**, które mogą być podatne na ataki.

7. **Budowanie świadomości cyberbezpieczeństwa**

Systematyczne informowanie i przypominanie pracownikom podstawowych zasad bezpieczeństwa, takich jak nieklikanie w podejrzane odsyłacze, nieotwieranie załączników od nieznanych osób i nieudostępnianie poufnych informacji na niezaufanych stronach lub aplikacjach.

8. **Regularne szkolenia**

Przeprowadzanie regularnych szkoleń dotyczących bezpieczeństwa informacji, w tym pracy przy przetwarzaniu mobilnym i pracy na odległość. Informowanie pracowników o aktualnych zagrożeniach, zasadach bezpiecznego korzystania z urządzeń mobilnych i przypominanie o procedurach postępowania w przypadku wystąpienia incydentu bezpieczeństwa.

12

Zabezpieczenia uniemożliwiające ujawnienie, modyfikacje, usunięcie lub zniszczenie informacji

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §20 UST. 2 PKT 9**

TREŚĆ PODSTAWY

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie.

Opis wymagania

Spełnienie wymagania polega na podjęciu działań, mających na celu ochronę informacji przed niepowołanym dostępem lub osobami, które nie mają uprawnień do ich przetwarzania. Aby spełnić to wymaganie, organizacja powinna wprowadzić różne środki bezpieczeństwa, takie jak:

1. Zapewnienie, że **tylko osoby uprawnione będą miały dostęp do informacji.**

2. Zastosowanie **technik szyfrowania danych**, które przekształcają informacje w nieczytelny dla osób nieuprawnionych sposób. Szyfrowanie może być stosowane podczas przechowywania danych, ich przetwarzania oraz ich transmisji – aby zabezpieczyć je przed odczytem lub manipulacjami (integralność danych).

3. **Monitorowanie działań i zdarzeń** związanych z przetwarzaniem informacji w celu wykrycia nieautoryzowanych lub podejrzanych aktywności. Audyt pozwoli na śledzenie, kto, kiedy i w jaki sposób korzysta z informacji, oraz identyfikowanie potencjalnych zagrożeń.

4. **Ochrona fizyczna miejsc przechowywania informacji**, takich jak serwery, centra danych czy pomieszczenia biurowe. Może obejmować zastosowanie kart dostępu, monitorowania wideo, systemów antywłamaniowych i innych środków mających na celu zapobieganie nieautoryzowanemu dostępowi do nośników danych i miejsc ich przechowywania.

Te oraz inne środki i działania zapewniają, że informacje są chronione przed nieuprawnionym dostępem, zmianami, usunięciem lub zniszczeniem.

Rekomendowane działania – przykłady

1. Opracowanie i wdrożenie polityki bezpieczeństwa informacji (PBI)

PBI określa zasady, procedury i wytyczne dotyczące zabezpieczania informacji. Polityka powinna uwzględniać aspekty takie jak kontrola dostępu, poufność danych, procedury zarządzania hasłami i inne środki bezpieczeństwa.

2. Systematyczna ocena ryzyka

Ocena ryzyka pozwala na identyfikowanie potencjalnych zagrożeń i wprowadzanie odpowiednich środków zapobiegawczych w celu minimalizacji ryzyka utraty, modyfikacji lub ujawnienia informacji.

3. Wykorzystanie mechanizmów kontroli dostępu

Różne mechanizmy kontroli dostępu, takie jak hasła, karty dostępu, uwierzytelnianie wielo-składnikowe, wykorzystywane dla zapewnienia, że tylko osoby uprawnione mają dostęp do informacji. Regularna aktualizacja haseł oraz ograniczenie dostępu do kluczowych danych tylko do niezbędnych użytkowników są równie istotne.

4. Szyfrowanie danych

Szyfrowanie danych, zarówno podczas ich przechowywania, jak i transmisji, w celu zabezpie-czenia informacji przed nieuprawnionym dostępem sprawia, że dane są nieczytelne dla osób, które nie mają odpowiednich kluczy deszyfrujących.

5. Regularne monitorowanie i analiza logów systemowych, zdarzeń sieciowych oraz działań użytkowników

W celu wykrycia nieautoryzowanych aktywności należy regularne monitorować i analizować logi systemowe, zdarzenia sieciowe oraz działania użytkowników. Audyt pozwala na identyfikację potencjalnych zagrożeń, naruszeń bezpieczeństwa i nieprawidło-wości w systemach. Zastosowanie zabezpieczeń fizycznych, serwerów, centrum danych i innych miejsc przechowywania informacji poprzez kontrolę dostępu, monitorowanie wideo, alarmy antywłamaniowe i inne środki zapobiegające nieautoryzowanemu dostępowi.

13

Zapisy w polityce bezpieczeństwa informacji w relacjach z dostawcami

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §20 UST. 2 PKT 10**

TREŚĆ PODSTAWY

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

Opis wymagania

Aby spełnić wymaganie, należy wziąć pod uwagę kilka kluczowych czynników:

1. Określanie wymagań. W umowie serwisowej należy **jasno sprecyzować wymagania** dotyczące bezpieczeństwa informacji. Mogą one obejmować zabezpieczenia techniczne, procedury dostępu, polityki haseł, poufność danych itp.

2. Badanie dostawców. Przed podpisaniem umowy warto **dokładnie zbadać dostawców**, z którymi planowana jest współpraca. Sprawdzenie ich referencji, certyfikatów bezpieczeństwa, audytów zewnętrznych itp. pomoże ocenić ich zdolność do zapewnienia odpowiedniego poziomu bezpieczeństwa.

3. Klauzule o ochronie danych. Umowa serwisowa powinna **zawierać klauzule dotyczące ochrony danych** osobowych, w tym konieczność zawierania umów powierzenia danych osobowych, o ile są konieczne, i poufności informacji. Te klauzule precyzują obowiązki dostawcy w zakresie przetwarzania danych i zabezpieczania informacji przed nieuprawnionym dostępem.

4. Monitorowanie i audyty. Należy uwzględnić w umowie **możliwość monitorowania działań dostawcy oraz przeprowadzania audytów** w celu sprawdzenia zgodności z ustalonymi standardami bezpieczeństwa.

5. Szkolenia i świadomość. Warto **wymagać od dostawcy zapewnienia szkoleń dla personelu** dotyczących bezpieczeństwa informacji i zagrożeń cybernetycznych. Dzięki temu pracownicy będą świadomi ryzyka i dowiedzą się, jak postępować w przypadku potencjalnych incydentów.

6. Zarządzanie incydentami. Umowa powinna zawierać **procedury zarządzania incydentami**, które określają sposób reagowania na ewentualne naruszenia bezpieczeństwa informacji. Ważnym aspektem jest sprecyzowanie zasady informowania o wystąpieniu incydentu oraz zasad jego zgłaszania. Pozwoli to szybko i skutecznie podjąć działania w przypadku wystąpienia zagrożeń.

7. Klauzule dotyczące zmian. Umowa powinna uwzględniać **klauzule, które umożliwią wprowadzenie zmian w związku z ewolucją zagrożeń i technologii. Dzięki temu można dostosować zabezpieczenia do zmieniających się warunków.**

Wprowadzenie takich zapisów i mechanizmów w procesie zawierania umów serwisowych zwiększy poziom cyberbezpieczeństwa. Dzięki temu strony trzecie będą odpowiedzialne za odpowiedni poziom ochrony informacji i zabezpieczeń.

Rekomendowane działania – przykłady

1. **Przeprowadzanie audytów bezpieczeństwa** stron trzecich przed podpisaniem umowy. Audyt ma na celu ocenę poziomu bezpieczeństwa i zabezpieczeń stosowanych przez danego dostawcę.

2. **Staranne i rzetelne badanie dostawców** przed podpisaniem umowy, uwzględniające ich reputację, doświadczenie, certyfikacje bezpieczeństwa, audyty zewnętrzne itp.

3. **Włączanie do umowy jasno sprecyzowanych wymagań** dotyczących bezpieczeństwa, takich jak standardy bezpieczeństwa, zasady dostępu, polityki haseł, szyfrowanie danych itp.

4. **Ustanowienie systemu monitorowania działań** stron trzecich w celu wykrywania potencjalnych zagrożeń i nieprawidłowości w przetwarzaniu informacji.

5. **Zapewnienie odpowiednich szkoleń dla personelu** stron trzecich, aby był świadomy ryzyk i zasad bezpieczeństwa informacji.

6. **Określenie procedur zarządzania incydentami**, w tym raportowania, reagowania i powiadamiania o ewentualnych naruszeniach bezpieczeństwa informacji.

7. **Wprowadzenie klauzul o ochronie danych osobowych**, w tym umów powierzenia danych osobowych i poufności informacji w umowach, które określają obowiązki stron trzecich w zakresie przetwarzania danych.

8. **Regularne monitorowanie i sprawdzanie zgodności działań stron trzecich z umową** oraz przepisami dotyczącymi ochrony danych i cyberbezpieczeństwa.

9. **Wymaganie od dostawców posiadania odpowiednich certyfikatów bezpieczeństwa** (np. ISO 27001) oraz przeprowadzanie regularnych audytów zewnętrznych.

10. **Zawarcie w umowie prawa do przeprowadzania kontroli i audytów bezpieczeństwa** u dostawców w celu sprawdzenia zgodności z ustalonymi wymaganiami.

14

Zasady akceptowalnego użycia aktywów informacyjnych

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §20 UST. 2 PKT 11**

TREŚĆ PODSTAWY

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.

Opis wymagania

Aby spełnić wymaganie, należy podjąć działania w następujących obszarach:

1. **Ustanowienie polityki bezpieczeństwa**, która określa ogólne zasady i wytyczne dotyczące ochrony informacji. Polityka powinna obejmować zasady dotyczące zarządzania hasłami, dostępu do informacji, korzystania z urządzeń mobilnych i innych zasad istotnych dla bezpiecznego przetwarzania informacji.

2. **Przeprowadzenie szkoleń dla pracowników** na temat bezpiecznego postępowania z informacjami i środkami przetwarzania. Pracownicy powinni być świadomi zagrożeń związanych z kradzieżą informacji i znać procedury postępowania w przypadku incydentów bezpieczeństwa.

3. **Wprowadzenie środków kontroli dostępu**, takich jak hasła, uwierzytelnianie dwuskładnikowe, karty dostępu itp., które minimalizują ryzyko nieuprawnionego dostępu do informacji. W przypadku urządzeń mobilnych i laptopów należy również uwzględnić funkcje zabezpieczające, takie jak blokowanie ekranu, szyfrowanie danych itp.

4. **Regularne monitorowanie działań** związanych z przetwarzaniem informacji oraz przeprowadzanie audytów w celu wykrywania ewentualnych naruszeń i identyfikacji słabych punktów w systemach. Dzięki temu można wcześniej wykrywać nieprawidłowości i podejmować działania naprawcze.

5. **Ustanowienie zasad dotyczących korzystania z urządzeń mobilnych**, takich jak smartfony, tablety itp. Wskazane jest wskazanie, jakich aplikacji i usług można używać na urządzeniach służbowych, jak przechowywać i przesyłać dane oraz jak postępować w przypadku zgubienia lub kradzieży urządzenia.

6. **Wdrożenie odpowiednich zabezpieczeń technicznych**, takich jak firewalle, programy antywirusowe, aktualizacje systemów operacyjnych i aplikacji, szyfrowanie danych, systemy dostępu zdalnego do zasobów służbowych itp. Te środki techniczne pomagają minimalizować ryzyko kradzieży informacji przez utrudnienie nieuprawnionego dostępu do systemów.

7. **Ustanowienie polityki monitorowania działań i reagowania na incydenty bezpieczeństwa.** Polityka powinna określać, jakie działania należy podjąć w przypadku np. wykrycia próby kradzieży informacji lub naruszenia bezpieczeństwa, oraz wskazywać zasady zgłaszania incydentów, sposoby przeprowadzania analizy przyczyn i podjmowania działań naprawczych itp.

Przyjęcie tych działań i zasad pomoże minimalizować ryzyko np. kradzieży informacji i środków przetwarzania, a także zapewni odpowiedni poziom bezpieczeństwa danych. Ważne jest, aby te zasady były jasne, zrozumiałe dla pracowników i regularnie aktualizowane w związku z ewolucją zagrożeń. Każda organizacja powinna dostosować działania i mechanizmy do swoich indywidualnych potrzeb, specyfiki działalności i specyfiki środowiska.

Rekomendowane działania – przykłady

1. Opracowanie i wdrożenie polityki bezpieczeństwa informacji (PBI)

PBI określa m.in. zasady postępowania z danymi i urządzeniami mobilnymi. Polityka powinna uwzględniać wymogi dotyczące haseł, uwierzytelniania, korzystania z urządzeń mobilnych, zarządzania nośnikami wymiennymi, przechowywania danych, udostępniania informacji, wycofywania nośników, lokalizacji i ochrony sprzętu, zasad jego wynoszenia poza siedzibę organizacji, bezpieczeństwa sprzętu, bezpiecznego zbywania lub przekazywania do ponownego użycia, pozostawiania sprzętu bez opieki, polityki czystego biurka i czystego ekranu.

2. Regularne szkolenia pracowników

Przeprowadzanie regularnych szkoleń dotyczących bezpieczeństwa informacji i postępowania z urządzeniami mobilnymi. Szkolenia powinny obejmować zagrożenia związane z kradzieżą danych, phishingiem, szkodliwym oprogramowaniem, zasadami korzystania z urządzeń mobilnych i sieci bezprzewodowych.

3. Wprowadzenie zasad zarządzania dostępem do informacji i urządzeń mobilnych

Należy określić, kto ma dostęp do jakich danych i urządzeń, na jakiej zasadzie i w jakim zakresie. Wykorzystanie mechanizmów uwierzytelniania, takich jak hasła, kody dostępu czy identyfikatory, może ograniczyć ryzyko nieuprawnionego dostępu.

4. Szyfrowanie danych

Zastosowanie mechanizmów szyfrowania danych na urządzeniach mobilnych oraz w systemach przechowywania i przetwarzania informacji. Szyfrowanie danych utrudnia odczytanie ich przez osoby nieuprawnione, nawet w przypadku kradzieży urządzenia.

5. Regularne aktualizacje oprogramowania

Aktualizacje należy przeprowadzać zarówno na urządzeniach mobilnych, jak i w innych systemach, aby korzystać z najnowszych poprawek bezpieczeństwa. Aktualizacje eliminują znane luki i podatności.

6. Wdrożenie systemów monitorowania aktywności sieciowej, logów zdarzeń i alarmów bezpieczeństwa

Monitorowanie pozwala wykrywać podejrzane aktywności, próby nieautoryzowanego dostępu lub działania niezgodne z zasadami bezpieczeństwa. Wczesne wykrycie zagrożeń umożliwia szybką reakcję i ograniczenie szkód.

7. Regularna analiza ryzyka związana z przetwarzaniem informacji i korzystaniem z urządzeń mobilnych

Identyfikacja potencjalnych zagrożeń i podjęcie odpowiednich środków zapobiegawczych, takich jak wdrożenie zabezpieczeń technicznych, procedur awaryjnych i planów odzyskiwania danych.

8. Regularne przeprowadzanie audytów bezpieczeństwa

Audyty mogą obejmować testy penetracyjne, przeglądy systemów, ocenę zgodności z wymaganiami prawno-regulacyjnymi itp.

15 Aktualność oprogramowania

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §20 UST. 2 PKT 12A)**

TREŚĆ PODSTAWY

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na dbałości o aktualizację oprogramowania.

Opis wymagania

Dbałość o aktualizację oprogramowania oznacza, że organizacja musi regularnie aktualizować zainstalowane na swoich systemach i urządzeniach (komputery, laptopy, urządzenia mobilne, sprzęt sieciowy) oprogramowanie. Zapewnia to jego bezpieczeństwo i poprawne działanie.

Aktualizacje oprogramowania to specjalne modyfikacje, poprawki i uaktualnienia, które są udostępniane przez producentów oprogramowania. Mają one na celu naprawienie błędów, usunięcie luk w zabezpieczeniach oraz dodanie nowych funkcji lub ulepszeń. Dlatego ważne jest, aby systemy informatyczne oraz urządzenia były stale aktualizowane.

Dbałość o aktualizację oprogramowania polega na regularnym sprawdzaniu dostępnych aktualizacji i instalowaniu ich na wszystkich systemach. Organizacja powinna monitorować informacje o nowych wersjach oprogramowania udostępnianych przez producentów oraz otrzymywać powiadomienia o dostępnych aktualizacjach. Następnie należy przeprowadzić odpowiednie procedury aktualizacyjne, które mogą obejmować pobieranie i instalowanie aktualizacji, restartowanie systemów lub wykonywanie innych czynności zgodnie z instrukcjami producenta.

Dbałość o aktualizację oprogramowania ma kluczowe znaczenie dla zapewnienia bezpieczeństwa systemów teleinformatycznych. Aktualizacje często zawierają poprawki zabezpieczeń, które usuwają luki wykorzystywane przez cyberprzestępców. Nieaktualne oprogramowanie może być podatne na ataki i naruszenia bezpieczeństwa, co może prowadzić do kradzieży danych, utraty poufności informacji lub innych poważnych problemów.

Dlatego ważne jest, aby organizacja miała wdrożone odpowiednie procedury i mechanizmy techniczne, które umożliwią regularne sprawdzanie, testowanie i instalowanie aktualizacji oprogramowania. Może to obejmować automatyczne narzędzia do zarządzania aktualizacjami, harmonogramy aktualizacji czy dedykowane zespoły odpowiedzialne za monitorowanie, testowanie i realizację aktualizacji.

Dbałość o aktualizacje oprogramowania jest istotnym elementem zapewnienia cyberbezpieczeństwa, ponieważ pomaga organizacji chronić swoje systemy przed nowymi zagrożeniami i lukami w zabezpieczeniach.

Rekomendowane działania – przykłady

1. Wprowadzenie narzędzi automatyzujących proces aktualizacji oprogramowania

Automatyczne narzędzia mogą monitorować dostępność nowych aktualizacji, pobierać je i instalować na systemach, eliminując potrzebę manualnego sprawdzania i aktualizowania każdego systemu oddzielnie.

2. Opracowanie i wdrożenie polityki aktualizacji,

Polityka aktualizacji powinna określać częstotliwość i priorytet aktualizacji oprogramowania. Może pomóc w utrzymaniu systemów w aktualnym i bezpiecznym stanie. Polityka powinna obejmować zarówno systemy operacyjne, jak i inne oprogramowanie, takie jak przeglądarki internetowe, aplikacje biurowe czy narzędzia zabezpieczające.

3. Przeprowadzanie testów

Przed wprowadzeniem nowych aktualizacji do produkcji warto przeprowadzać testy, aby upewnić się, że nowe aktualizacje nie powodują niezamierzonych skutków ubocznych ani nie zakłócają działania systemów. Testowanie może obejmować uruchamianie aktualizacji na dedykowanych środowiskach testowych i weryfikację poprawności działania systemów po zainstalowaniu aktualizacji.

4. Monitorowanie dostępności aktualizacji oprogramowania

Ważne jest utrzymanie bieżącej wiedzy o dostępnych aktualizacjach oprogramowania. Można to osiągnąć przez monitorowanie komunikatów producentów oprogramowania, subskrypcję powiadomień o nowych wersjach lub korzystanie z usług śledzenia podatności, które dostarczają informacji na temat luk w zabezpieczeniach i udostępnionych poprawek.

5. Budowanie świadomości

Pracownicy powinni być świadomi znaczenia aktualizacji oprogramowania i odpowiedzialności za ich instalowanie. Dlatego istotne jest prowadzenie szkoleń i edukacji dotyczących znaczenia aktualizacji, korzyści płynących z ich regularnego stosowania oraz sposobów postępowania w przypadku otrzymania powiadomień o dostępnych aktualizacjach.

6. Prowadzenie rejestru zainstalowanego oprogramowania

Jednostka powinna utrzymywać dokładny rejestr zainstalowanego oprogramowania i jego wersji. Dzięki temu można skoncentrować się na aktualizacji tych wersji, które zawierają poprawki związane z bezpieczeństwem.

Wprowadzenie tych działań doskonalących może przyczynić się do podniesienia poziomu cyberbezpieczeństwa poprzez zapewnienie regularnej i skutecznej aktualizacji oprogramowania, co minimalizuje ryzyko wykorzystania luk w zabezpieczeniach przez potencjalnych atakujących.

16

Ograniczanie ryzyka utraty informacji

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §20 UST. 2 PKT 12B**

TREŚĆ PODSTAWY

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii.

Opis wymagania

Minimalizowanie ryzyka utraty informacji w wyniku awarii oznacza podejmowanie działań mających na celu zmniejszenie prawdopodobieństwa utraty danych w przypadku awarii systemu lub infrastruktury.

Aby spełnić to wymaganie, można zastosować różne działania doskonalące, takie jak:

1. **Regularne tworzenie kopii zapasowych danych** i przechowywanie ich na zewnętrznych nośnikach lub w chmurze może pomóc w odtworzeniu danych w przypadku awarii. Ważne jest również sprawdzanie regularności tworzenia kopii zapasowych oraz ich spójności i przywracanie ich w celu potwierdzenia, że są one funkcjonalne.

2. Stosowanie redundancji oznacza **posiadanie duplikatów danych, systemów lub infrastruktury** w celu zapewnienia dostępności w przypadku awarii. Przykładowo korzystanie z systemów RAID w celu replikacji danych na wiele dysków twardych lub wykorzystanie klastrów serwerowych, gdzie wiele serwerów pracuje jako jeden logiczny, może zapewnić ciągłość działania w przypadku awarii pojedynczych komponentów.

3. Wyposażenie systemów **w rozwiązania zasilania awaryjnego**, takie jak zasilacze UPS i generatory, może pomóc w utrzymaniu działania systemów w przypadku awarii zasilania. Zapewnia to dodatkowy czas na bezpieczne zakończenie działania i uniknięcie utraty danych.

4. **Wdrożenie systemów monitorujących i zarządzających awariami** pozwala na szybkie wykrycie i reakcję na problemy w infrastrukturze IT. Monitoring może obejmować zarówno sprzętowy status systemu, jak i wykrywanie nieprawidłowości w dostępie do danych. Ważne jest również dokumentowanie procedur reagowania na awarie oraz przeprowadzanie regularnych testów, aby upewnić się, że działania ratunkowe są skuteczne.

5. Pracownicy powinni znać **procedury postępowania w przypadku awarii**, powinni wiedzieć, jak zgłaszać incydenty, jak działać w przypadku utraty dostępu do danych i jak przywracać działanie systemów. Odpowiednie szkolenia powinny być prowadzone regularnie i uwzględniać aktualne procedury awaryjne.

Wdrożenie tych działań doskonalących pozwala na minimalizowanie ryzyka utraty informacji w przypadku awarii, co przyczynia się do utrzymania ciągłości działania i ochrony danych przed nieprzewidywalnymi sytuacjami.

Rekomendowane działania – przykłady

1. Redundancja – nadmiarowość systemów

W przypadku utraty jednego systemu dane są dostępne na innych, co minimalizuje ryzyko ich całkowitej utraty.. Tworzenie kopii zapasowych i replikacja danych na różnych systemach lub serwerach pozwala na szybkie przywrócenie działania w przypadku awarii.

2. Wykorzystanie rozwiązań wysokiej dostępności

Implementacja systemów wysokiej dostępności, takich jak klastry serwerowe, które automatycznie przejmują obciążenie w przypadku awarii jednego z węzłów, umożliwia nieprzerwaną pracę systemu.

3. Regularne przeglądy sprzętu, sieci i innych składników infrastruktury IT

Regularne przeglądy pozwalają wykryć ewentualne słabe punkty, które mogą prowadzić do awarii. Naprawa lub wymiana uszkodzonych lub przestarzałych komponentów minimalizuje ryzyko awarii i utraty danych.

4. Opracowanie planu awaryjnego

Opracowanie szczegółowego planu awaryjnego, obejmującego procedury działania w przypadku awarii, w tym procesu odzyskiwania danych i przywracania systemów, jest kluczowe. Regularne aktualizacje planu i przeprowadzanie symulacji awarii pozwala na sprawdzenie skuteczności procedur i ich dostosowanie do zmieniających się wymagań.

5. Stosowanie rozwiązań zasilania awaryjnego

Stosowanie zasilania awaryjnego, np. zasilaczy UPS (niezakłócone źródło zasilania) lub generatorów, minimalizuje ryzyko utraty danych w przypadku nagłej przerwy w dostawie energii elektrycznej.

6. Systematyczne monitorowanie infrastruktury

Systematyczne monitorowanie infrastruktury w tym sprzętu, sieci i usług, pozwala na wczesne wykrywanie awarii i szybką reakcję. Powiadomienia i alarmy umożliwiają podjęcie natychmiastowych działań naprawczych i minimalizują czas niedostępności systemu.

7. Szkolenie pracowników

Regularne szkolenie pracowników z zakresu procedur awaryjnych, obsługi kopii zapasowych, odzyskiwania danych i innych aspektów związanych z minimalizowaniem ryzyka utraty informacji pozwalają na skuteczne reagowanie w przypadku awarii i ogranicza potencjalne szkody.

Wdrożenie tych działań doskonalących pozwala na minimalizowanie ryzyka utraty informacji w przypadku awarii, zwiększa odporność systemu na zakłócenia i podnosi poziom cyberbezpieczeństwa. Do skutecznego wdrożenia działań i mechanizmów niezbędne jest poprawne przeprowadzenia analizy ryzyka.

17 Ochrona danych

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §20 UST. 2 PKT 12C**

TREŚĆ PODSTAWY

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na ochronie przed błędami, utratą, nieuprawnioną modyfikacją.

Opis wymagania

Ochrona informacji przed błędami, utratą i nieuprawnioną modyfikacją obejmuje działania mające na celu zabezpieczenie informacji przed różnymi zagrożeniami. Informacje powinny być bezpieczne i niezmienione, a jednocześnie dostępne dla uprawnionych użytkowników.

Aby spełnić to wymaganie, można podjąć następujące działania:

1. Tworzenie kopii zapasowych

Regularne tworzenie kopii zapasowych danych i przechowywanie ich w bezpiecznym miejscu zapewnia ochronę przed utratą informacji. W przypadku awarii lub uszkodzenia danych można przywrócić kopię zapasową i odzyskać utracone dane.

2. Zastosowanie mechanizmów uwierzytelniania i autoryzacji

Stosowanie silnych metod uwierzytelniania, takich jak hasła, certyfikaty cyfrowe lub biometryczne, pozwala kontrolować dostęp do informacji. Mechanizmy autoryzacji określają, kto ma uprawnienia do modyfikacji danych, co zapobiega nieuprawnionej modyfikacji.

3. Zabezpieczanie fizyczne i logiczne

Zapewnienie odpowiednich zabezpieczeń fizycznych, takich jak odpowiednie zamki, monitoring czy kontrola dostępu, chroni przed nieautoryzowanym dostępem do informacji. Również zabezpieczenia logiczne, takie jak firewall, antywirusy czy szyfrowanie danych, pomagają ochronić informacje przed nieuprawnioną modyfikacją.

4. Monitorowanie i wykrywanie zagrożeń

Wykorzystanie systemów monitorujących i wykrywających zagrożenia, takich jak systemy IPS (Intrusion Prevention System) czy SIEM (Security Information and Event Management), pozwala szybko reagować na potencjalne ataki lub nieprawidłowości w systemie i chroni przed nieuprawnionymi modyfikacjami.

5. Szkolenie pracowników

Edukowanie pracowników na temat zasad bezpieczeństwa informacji, unikania phishingu, stosowania silnych haseł czy rozpoznawania podejrzanych zachowań pomaga w ochronie informacji przed błędami i nieuprawnioną modyfikacją. Świadomość pracowników jest kluczowa dla skutecznej ochrony danych.

Poprzez wdrożenie tych działań doskonalących można zabezpieczyć informacje przed błędami, utratą i nieuprawnioną modyfikacją, co przyczyni się do podniesienia poziomu cyberbezpieczeństwa.

Rekomendowane działania – przykłady

1. **Regularne wykonywanie kopii zapasowych** danych i przechowywanie ich na osobnych nośnikach lub w chmurze umożliwia szybkie odtworzenie informacji w przypadku awarii, uszkodzenia lub utraty danych.

2. **Wymuszanie na użytkownikach korzystania z silnych haseł** oraz ich regularne zmiany mogą pomóc w ochronie informacji przed nieuprawnionym dostępem i nieautoryzowaną modyfikacją.

3. **Regularne aktualizacje oprogramowania**, w tym systemów operacyjnych, aplikacji i zabezpieczeń, umożliwiają łatanie luk w zabezpieczeniach i minimalizują ryzyko wykorzystania znanych podatności przez atakujących.

4. **Implementacja mechanizmów uwierzytelniania wielopoziomowego**, takich jak kody SMS, tokeny lub aplikacje uwierzytelniające, dodaje dodatkową warstwę ochrony przed nieuprawnionym dostępem.

5. **Szyfrowanie danych** na poziomie przechowywania i transmisji zapewnia ochronę przed nieautoryzowanym odczytem i modyfikacją danych w przypadku ich przechwycenia.

6. **Wdrożenie systemów monitorujących i wykrywających próby włamań (IDS/IPS)** pozwala na szybkie wykrywanie nieautoryzowanych prób dostępu lub modyfikacji informacji.

7. **Stosowanie odpowiednich polityk kontroli dostępu**, takich jak przydzielenie uprawnień na podstawie zasady najmniejszych przywilejów (ang. *principle of least privilege*) oraz monitorowanie aktywności użytkowników, pomaga w minimalizowaniu ryzyka nieuprawnionej modyfikacji informacji.

8. **Szkolenie pracowników w zakresie świadomości bezpieczeństwa informacji**, zasad higieny cybernetycznej, rozpoznawania zagrożeń i raportowania incydentów, może pomóc w minimalizowaniu ryzyka ludzkiego błędu i zwiększeniu poziomu ochrony informacji.

9. **Regularne przeprowadzanie testów penetracyjnych i audytów bezpieczeństwa**, zarówno wewnętrznych, jak i zewnętrznych, umożliwia identyfikację słabych punktów w systemach i infrastrukturze, które mogą być wykorzystane przez potencjalnych atakujących.

10. **Konfiguracja systemów monitorowania incydentów i reagowanie** na niepożądane zdarzenia pozwala na szybką odpowiedź w przypadku wykrycia nieautoryzowanych modyfikacji lub prób naruszenia bezpieczeństwa informacji.

Implementacja tych działań doskonalących przyczyni się do podniesienia poziomu cyberbezpieczeństwa i zminimalizuje ryzyko błędów, utraty danych oraz nieuprawnionej modyfikacji informacji.

18

Stosowanie mechanizmów kryptograficznych

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §20 UST. 2 PKT 12D**

TREŚĆ PODSTAWY

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa.

Opis wymagania

Stosowanie mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa polega na odpowiednim dostosowaniu wykorzystywanych technik kryptograficznych do istniejących zagrożeń oraz wymagań wynikających z przepisów prawnych.

W praktyce oznacza to, że organizacja powinna:

1. **Ocenić zagrożenia.** Zidentyfikować potencjalne zagrożenia dla swoich danych i systemów, takie jak nieuprawniony dostęp, przechwycenie danych czy ataki cyberprzestępców. Na podstawie tej oceny organizacja określa, jakie mechanizmy kryptograficzne są potrzebne do odpowiedniej ochrony.

2. **Wybrać odpowiednie mechanizmy i dobrze zrozumieć różne techniki kryptograficzne**, takie jak szyfrowanie symetryczne, asymetryczne czy funkcje skrótu. Następnie wybrać te, które są odpowiednie dla konkretnych potrzeb organizacji, uwzględniając zarówno poziom ochrony, jak i jej efektywność.

3. **Dostosować do wymogów prawa:** Przepisy prawne mogą określać specyficzne wymogi dotyczące stosowania kryptografii, takie jak długość kluczy, algorytmy kryptograficzne czy certyfikaty. Organizacja powinna być świadoma tych wymogów i dostosować swoje mechanizmy kryptograficzne, aby spełniały przepisy obowiązujące w danym obszarze.

4. **Regularnie aktualizować technologie kryptograficzne**, które są stale rozwijane. Jako że w zabezpieczeniach ciągle pojawiają się luki, ważne jest regularne aktualizowanie zastosowanych mechanizmów kryptograficznych, które pozwala zapewnić ochronę przed najnowszymi zagrożeniami.

5. **Regularnie testować i audytować systemy kryptograficzne**, co pomoże upewnić się, że mechanizmy są w pełni funkcjonalne i skuteczne. W razie potrzeby można wprowadzić poprawki lub ulepszenia, aby zapewnić odpowiedni poziom ochrony.

Stosowanie mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisów prawa zapewnia skuteczną ochronę informacji przez wykorzystanie odpowiednich technik kryptograficznych i dostosowanie ich do konkretnych potrzeb organizacji oraz wymogów.

Rekomendowane działania – przykłady

1. Przeprowadzanie kompleksowej oceny ryzyka

Ocenę ryzyka przeprowadza się w celu identyfikacji zagrożenia i wrażliwych obszarów, które wymagają zastosowania mechanizmów kryptograficznych. Zrozumienie specyficznych wymagań przepisów prawnych pomoże w określeniu odpowiednich rozwiązań.

2. Dobór algorytmów kryptograficznych

Istotny jest **właściwy** dobór algorytmów kryptograficznych, które są silne, sprawdzone i zgodne z wymaganiami prawnymi. Należy stosować aktualne standardy kryptograficzne i unikać przestarzałych lub podatnych na ataki algorytmów.

3. Zapewnienie bezpiecznego przechowywania, zarządzania i dystrybucji kluczy kryptograficznych

Wykorzystanie technik takich jak kryptografia klucza publicznego (asymetryczna) do bezpiecznego udostępniania kluczy i wymiany informacji.

4. Regularna aktualizacja i monitoring zastosowanych mechanizmów kryptograficznych w celu uwzględnienia najnowszych poprawek bezpieczeństwa

Monitorowanie ich wydajności i skuteczności dla zapewnienia ciągłej ochrony informacji.

5. Szkolenie pracowników

W celu zwiększania świadomości cyberbezpieczeństwa pracowników szkolenia powinny obejmować tematykę dotyczącą znaczenia i zasad stosowania mechanizmów kryptograficznych, a także procedur bezpiecznego przechowywania kluczy czy korzystania z kryptografii w komunikacji.

6. Przeprowadzanie regularnych audytów bezpieczeństwa, w tym audytów kryptografii

Przeprowadzanie regularnych audytów pozwala na zweryfikowanie zgodności z wymaganiami i wykrywanie potencjalnych luk lub słabych punktów. Natomiast wykonywanie testów penetracyjnych pozwala na sprawdzenie odporności systemów na ataki związane z kryptografią.

7. Utrzymywanie systemu monitoringu

System monitoringu pozwala wykryć ewentualne naruszenia bezpieczeństwa kryptograficznego. Konieczne jest bezzwłoczne reagowanie w razie wystąpienia incydentu, podejmowanie odpowiednich działań naprawczych i ewentualne przeprowadzanie śledztwa.

Przyjęcie tych działań, adekwatnie do zagrożeń lub wymogów przepisów prawnych, pomoże w zwiększeniu poziomu cyberbezpieczeństwa i ochronie informacji przed nieuprawnionym dostępem, modyfikacją czy utratą.

19

Zapewnienie bezpieczeństwa plików systemowych

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §20 UST. 2 PKT 12E**

TREŚĆ PODSTAWY

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na zapewnieniu bezpieczeństwa plików systemowych.

Opis wymagania

Zapewnienie bezpieczeństwa plików systemowych oznacza konieczność ich ochrony przed nieuprawnionym dostępem, modyfikacją lub usunięciem. Bezpieczeństwo plików systemowych jest istotne, ponieważ są one ważnymi elementami systemu operacyjnego lub innych programów, które wspierają działanie komputera.

Aby spełnić to wymaganie, można podjąć następujące działania doskonalące:

1. **Stosowanie odpowiednich mechanizmów kontroli dostępu**, takich jak uprawnienia użytkowników i grup, aby ograniczyć dostęp do plików systemowych tylko do osób, które mają do tego uprawnienia. Zapewnienie, że tylko niezbędne osoby będą miały możliwość odczytu, zapisu lub modyfikacji tych plików.

2. **Regularne sprawdzanie integralności plików systemowych** przez porównywanie ich sum kontrolnych (np. sumy MD5 lub SHA) z wcześniej zapisanymi wartościami. Jeśli zostaną wykryte jakiekolwiek zmiany w plikach, może to oznaczać możliwość naruszenia bezpieczeństwa i konieczność podjęcia odpowiednich działań naprawczych.

3. **Zabezpieczanie lokalizacji plików** – umieszczanie plików systemowych w chronionych lokalizacjach, do których mają dostęp tylko upoważnione osoby. Zapewnienie, że katalogi zawierające pliki systemowe są odpowiednio zabezpieczone przed nieautoryzowanym dostępem.

4. **Przeprowadzanie regularnych aktualizacji** systemu operacyjnego oraz innego oprogramowania, które korzysta z plików systemowych. Aktualizacje i łaty często zawierają poprawki bezpieczeństwa, które pomagają zapobiec znanej lub potencjalnej luce w zabezpieczeniach.

5. **Korzystanie z oprogramowania antywirusowego**, które może skanować pliki systemowe w poszukiwaniu wirusów, malware lub innych szkodliwych programów. Dzięki regularnym aktualizacjom baz danych antywirusowych, oprogramowanie rozpoznaje najnowsze sygnatury zagrożeń.

6. **Regularne wykonywanie kopii zapasowych plików systemowych**, aby w przypadku awarii lub uszkodzenia można było je przywrócić. Kopie zapasowe powinny być przechowywane w bezpiecznym miejscu, z dala od potencjalnych zagrożeń.

7. **Regularne przeprowadzanie audytów bezpieczeństwa**, które obejmują ocenę zabezpieczeń plików systemowych. Identyfikacja ewentualnych słabych punktów i podjęcie odpowiednich działań naprawczych.

Zapewnienie bezpieczeństwa plików systemowych wymaga systematyczności i stałej uwagi. Ważne jest, aby być świadomym zagrożeń i regularnie aktualizować i monitorować działanie systemów.

Rekomendowane działania – przykłady

1. Wdrażanie zasad minimalnego uprzywilejowania

Ograniczanie dostępu do plików systemowych tylko do użytkowników lub procesów, które wymagają tych uprawnień. Unikanie nadawania nadmiernych uprawnień administracyjnych.

2. Regularne skanowanie plików systemowych

Wykorzystanie antywirusów lub skanerów bezpieczeństwa do regularnego skanowania plików systemowych w celu wykrywania i usuwania potencjalnego złośliwego oprogramowania.

3. Regularne aktualizowanie systemu operacyjnego oraz oprogramowania

Aktualizacje umożliwiają dostęp do najnowszych poprawek bezpieczeństwa.

4. Wykorzystywanie narzędzi monitorujących

Narzędzia sprawdzają integralność plików systemowych przez porównywanie ich sum kontrolnych z wcześniej ustalonymi wartościami. W przypadku wykrycia nieprawidłowości należy podjąć odpowiednie kroki w celu identyfikacji i naprawy problemu.

5. Stosowanie mechanizmów kontroli dostępu

Mechanizmy kontroli dostępu, takie jak uprawnienia użytkowników, grupy użytkowników i zarządzanie uprawnieniami, kontrolują, kto ma dostęp do plików systemowych i jakie działania może na nich wykonywać.

6. Uruchomienie rejestracji zdarzeń, która umożliwi monitorowanie aktywności związanej z plikami systemowymi

Analiza logów w celu wykrywania nieprawidłowości, podejrzanych działań lub prób naruszenia bezpieczeństwa plików systemowych.

7. Zastosowanie mechanizmów szyfrowania

W przypadku plików systemowych zawierających wrażliwe informacje można rozważyć zastosowanie mechanizmów szyfrowania, które zabezpieczą te dane przed nieuprawnionym dostępem.

8. Regularne wykonywanie kopii zapasowych plików systemowych

Regularne wykonywanie kopii zapasowych plików systemowych umożliwia – w przypadku awarii, utraty danych lub ataku – przywrócenie plików do poprzedniego stanu.

9. Przeprowadzanie regularnych testów penetracyjnych

Testy mają na celu identyfikację luk w zabezpieczeniach plików systemowych oraz pomagają w identyfikacji potencjalnych słabości i podjęciu odpowiednich środków zaradczych.

10. Szkolenie pracowników

Zapewnienie pracownikom szkoleń dotyczących bezpieczeństwa plików systemowych, w tym zagrożeń, praktyk bezpieczeństwa i procedur postępowania w przypadku podejrzenia naruszenia bezpieczeństwa.

Wymagane działania doskonalące mogą się różnić w zależności od specyfiki systemu, branży i innych czynników. Ważne jest, aby opracować indywidualne podejście do zapewnienia bezpieczeństwa plików systemowych, uwzględniające konkretne potrzeby i zagrożenia związane z danym środowiskiem.

20

Zarządzanie podatnościami technicznymi

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §20 UST. 2 PKT 12F)**

TREŚĆ PODSTAWY

Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Opis wymagania

Wymaganie dotyczące redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych oznacza, że należy podjąć środki w celu zminimalizowania ryzyka wykorzystania znanych luk w zabezpieczeniach systemów komputerowych. Oto proste wyjaśnienie tego wymagania: kiedy dostawcy oprogramowania lub producenci odkrywają luki w zabezpieczeniach swoich systemów teleinformatycznych, publikują informacje na ten temat, aby użytkownicy mogli podjąć odpowiednie środki zapobiegawcze. Dla organizacji wymaganie polega na podjęciu działań, które zmniejszą ryzyko wykorzystania tych podatności.

Można to osiągnąć poprzez:

1. **Regularne aktualizacje systemów teleinformatycznych**, w tym oprogramowania i firmware, aby korzystać z najnowszych poprawek bezpieczeństwa udostępnianych przez dostawców.
2. **Śledzenie informacji o nowych podatnościach technicznych**, które są publikowane przez dostawców usług i organizacje odpowiedzialne za bezpieczeństwo IT.
3. **Regularne przeprowadzanie audytów bezpieczeństwa**, które pomogą zidentyfikować potencjalne luki w zabezpieczeniach i podatności w systemach teleinformatycznych. Audyty powinny być przeprowadzane przez profesjonalistów z zakresu bezpieczeństwa IT.
4. **Przeprowadzanie testów penetracyjnych**, które symulują ataki cyberprzestępców na systemy teleinformatyczne. Dzięki nim można zidentyfikować słabe punkty i podjąć działania naprawcze.
5. **Opracowanie i wdrożenie polityki aktualizacji**, która określa, jak często i w jaki sposób systemy teleinformatyczne powinny być aktualizowane w celu minimalizacji ryzyka wykorzystania podatności technicznych.
6. **Wdrożenie narzędzia do zarządzania podatnościami**, które pomoże w identyfikacji, śledzeniu i zarządzaniu znalezionymi podatnościami w systemach teleinformatycznych.

W ten sposób można uzyskać pełny obraz podatności i działań podejmowanych w celu ich naprawy.

Ważne jest, aby podjąć działania doskonalące odpowiednie dla danej organizacji i jej systemów teleinformatycznych przy konieczności dostosowania tych działań do specyfiki branży, rodzaju systemów i zagrożeń, z którymi się styka.

Rekomendowane działania – przykłady

1. Regularne aktualizowanie oprogramowania

Regularne aktualizowanie oprogramowania w systemach teleinformatycznych, w tym systemów operacyjnych, aplikacji i innych składników, pozwala korzystać z najnowszych poprawek bezpieczeństwa udostępnianych przez dostawców. Aktualizacje zawierają poprawki dla znanych podatności.

2. Monitorowanie i śledzenie informacji o podatnościach

Należy śledzić publikacje dostawców i organizacji odpowiedzialnych za bezpieczeństwo IT, takich jak National Vulnerability Database (Narodowa Baza Podatności), aby być na bieżąco z informacjami o nowo odkrytych podatnościach. To pozwoli podjąć szybkie działania naprawcze.

3. Wdrażanie systemów automatycznego skanowania podatności

Warto wykorzystać narzędzia do skanowania podatności, które automatycznie przeszukują systemy teleinformatyczne w poszukiwaniu znanych podatności. Umożliwia to identyfikację potencjalnych luk w zabezpieczeniach i podjęcie odpowiednich działań naprawczych.

4. Penetracyjne testy bezpieczeństwa

Regularnie przeprowadzanie testów penetracyjnych, które symulują ataki cyberprzestępców na systemy teleinformatyczne, pozwala odkryć słabe punkty i podatności w infrastrukturze IT oraz podjąć działania naprawcze przed wykorzystaniem ich przez niepożądane osoby.

5. Polityka zarządzania podatnościami

Należy opracować i wdrożyć politykę zarządzania podatnościami, która określi procedury reagowania na odkryte podatności. Polityka powinna określać, kto jest odpowiedzialny za zarządzanie podatnościami, jakie są kroki naprawcze i jakie są terminy realizacji działań.

6. Szkolenie pracowników

Należy zadbać o odpowiednie szkolenie pracowników w zakresie bezpieczeństwa IT, w tym świadomość zagrożeń wynikających z podatności systemó teleinformatycznych. Pracownicy powinni być świadomi znaczenia aktualizacji, zgłaszania podatności i przestrzegania procedur bezpieczeństwa.

7. Monitoring i reagowanie na incydenty

System monitorowania i reagowania na incydenty bezpieczeństwa pozwala wykrywać ataki i podatności w systemach teleinformatycznych oraz reagować na nie. Wczesne wykrycie i szybka reakcja mogą ograniczyć skutki naruszeń.

8. Ocena ryzyka

Należy przeprowadzać regularne oceny ryzyka w celu identyfikacji i priorytetyzacji podatności systemów teleinformatycznych. Na podstawie wyników oceny można opracować plan działań naprawczych i inwestycji w zabezpieczenia.

Każda organizacja ma swoje unikalne potrzeby i specyfikę, dlatego ważne jest dostosowanie działań doskonalących do indywidualnych wymagań i środowiska.

21

Zarządzanie nieujawnionymi podatnościami i możliwościami naruszenia bezpieczeństwa

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §20 UST. 2 PKT 12G)**

TREŚĆ PODSTAWY

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa.

Opis wymagania

Gdy w systemach teleinformatycznych zostaną zauważone nieujawnione podatności, które mogą naruszać bezpieczeństwo, należy natychmiast podjąć działania **zabezpieczające lub usuwające te luki**.

W takich przypadkach należy **działać szybko** i podjąć wszelkie konieczne kroki naprawcze, aby **usunąć podatności lub ograniczyć ich wykorzystanie**.

To wymaganie ma zapewniać, że organizacja reaguje niezwłocznie na odkryte podatności i nie pozostawia ich bez odpowiedzi. Jest to istotne, ponieważ opóźnienie w podjęciu działań może prowadzić do wykorzystania podatności przez atakujących, co z kolei może prowadzić do utraty poufnych informacji lub zakłóceń w funkcjonowaniu systemu.

Ważne jest, aby organizacja miała wdrożone odpowiednie procedury i mechanizmy, umożliwiające szybką identyfikację, analizę i usunięcie podatności. Takie działania przyczyniają się do zwiększenia poziomu bezpieczeństwa systemów teleinformatycznych i minimalizowania ryzyka wykorzystania podatności przez niepożądane osoby.

Rekomendowane działania – przykłady

1. Przeprowadzanie regularnych skanów podatności

Przeprowadzanie regularnych skanów podatności w systemach teleinformatycznych pozwala na wczesne wykrywanie potencjalnych luk w zabezpieczeniach. Można wykorzystać narzędzia automatyczne lub usługi zewnętrzne do przeprowadzania skanów i identyfikowania nieujawnionych podatności.

2. Wykorzystanie mechanizmów reagowania na alerty bezpieczeństwa

Wykorzystanie mechanizmów reagowania na alerty bezpieczeństwa umożliwia szybkie identyfikowanie i analizowanie zgłoszeń dotyczących potencjalnych podatności. Zespół odpowiedzialny za bezpieczeństwo powinien być dobrze przygotowany do analizy i reagowania na takie zgłoszenia, aby niezwłocznie podejmować działania naprawcze.

3. Regularne aktualizacje oprogramowania

Aktualizacje oprogramowania, w tym systemów operacyjnych, aplikacji i innych komponentów, są niezwykle ważne w celu zapewnienia ochrony przed znanymi podatnościami. Wdrażanie poprawek i łat, które adresują znane podatności, minimalizuje ryzyko ich wykorzystania przez atakujących.

4. Opracowanie i wdrożenie procedur reagowania na incydenty

Powyższe działanie pozwala na szybką identyfikację, analizę i rozwiązanie nieujawnionych podatności. Określenie kroków, które należy podjąć w przypadku wykrycia podatności, umożliwia skuteczną reakcję i minimalizację ryzyka.

5. Monitorowanie i zbieranie logów z systemów

Skuteczne monitorowanie i zbieranie logów z systemów teleinformatycznych umożliwia wczesne wykrywanie nieprawidłowości i podejrzanych aktywności. Monitorowanie może obejmować analizę logów, wykrywanie anomalii w ruchu sieciowym oraz monitorowanie zachowań użytkowników. Wczesne wykrycie nieprawidłowości może wskazywać na potencjalne podatności, które można szybko naprawić lub usunąć.

6. Szkolenie pracowników

Edukacja pracowników w zakresie cyberbezpieczeństwa jest niezwykle istotna. Pracownicy powinni być świadomi znaczenia niezwłocznego zgłaszania potencjalnych podatności i niebezpiecznych sytuacji. Szkolenia powinny obejmować rozpoznawanie oznak podatności, procedury zgłaszania incydentów i właściwe postępowanie w przypadku wykrycia nieprawidłowości.

Te działania doskonalące przyczynią się do podniesienia poziomu cyberbezpieczeństwa przez szybką identyfikację i reagowanie na nieujawnione podatności w systemach teleinformatycznych. Pozwalają one minimalizować ryzyko naruszeń bezpieczeństwa i skutecznie chronić informacje przed atakami.

22

Kontrola zgodności systemów

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §20 UST. 2 PKT 12H)**

TREŚĆ PODSTAWY

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.

Opis wymagania

Kontrola zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa oznacza, że systemy te muszą spełniać określone standardy i zasady bezpieczeństwa. Kontrola zgodności polega na regularnym **sprawdzaniu, czy systemy są zgodne z ustalonymi normami i politykami**.

W praktyce oznacza to, że systemy teleinformatyczne są oceniane pod kątem zgodności z określonymi wymaganiami bezpieczeństwa. Mogą to być normy branżowe, regulacje prawne, polityki bezpieczeństwa organizacji lub inne wytyczne. Kontrola zgodności **może obejmować audyty, oceny bezpieczeństwa, przeglądy kodu, testy penetracyjne i inne metody oceny**.

Celem kontroli zgodności jest upewnienie się, że systemy teleinformatyczne są odpowiednio zabezpieczone i chronią informacje przed nieuprawnionym dostępem, utratą lub modyfikacją. Zapewnienie zgodności wiąże się z wdrażaniem odpowiednich środków ochrony, procedur i polityk bezpieczeństwa, a także regularnym monitorowaniem i aktualizacją systemów w celu dostosowania ich do zmieniających się zagrożeń.

Kontrola zgodności pomaga organizacjom utrzymać wysoki poziom bezpieczeństwa informacji i zapewniać zgodność ze standardami i wymogami, które są istotne dla danej branży lub organizacji.

Rekomendowane działania – przykłady

1. Określenie polityk bezpieczeństwa

Ustanowienie jasnych i spójnych polityk bezpieczeństwa, które precyzują wymagania i oczekiwania dotyczące bezpieczeństwa systemów teleinformatycznych.

2. Audyty bezpieczeństwa

Regularne przeprowadzanie audytów bezpieczeństwa w celu oceny zgodności systemów teleinformatycznych z normami i politykami bezpieczeństwa. Audyty mogą obejmować przeglądy konfiguracji, oceny ryzyka, testy bezpieczeństwa, analizę zdarzeń itp.

3. Monitorowanie zgodności

Wykorzystanie systemu monitorowania, dzięki któremu regularnie będzie sprawdzana zgodność systemów teleinformatycznych z normami i politykami bezpieczeństwa. Monitorowanie może obejmować logowanie zdarzeń, analizę logów, wykrywanie zagrożeń i anomalii oraz powiadamianie o nieprawidłowościach.

4. Aktualizacje i łaty bezpieczeństwa

Regularne aktualizacje oprogramowania i systemów operacyjnych w celu naprawienia znanych podatności i luk bezpieczeństwa. Zapewnienie, że systemy są zawsze aktualne i chronione przed znanymi zagrożeniami.

5. Szkolenie pracowników

Zapewnienie odpowiednich szkoleń pomoże podnieść świadomość pracowników w zakresie zasad bezpieczeństwa informacji. Zdobędą oni odpowiednią wiedzę i umiejętności, które pozwolą przestrzegać norm i polityk bezpieczeństwa.

6. Regularne przeglądy i oceny

Regularne przeglądy i oceny systemów teleinformatycznych w celu identyfikacji ewentualnych luk bezpieczeństwa, błędów konfiguracji lub innych problemów, które mogą naruszać zgodność z normami i politykami bezpieczeństwa.

7. System zarządzania bezpieczeństwem.

Wdrożenie systemu zarządzania bezpieczeństwem, który obejmuje procesy, procedury i narzędzia do skutecznego zarządzania zgodnością systemów teleinformatycznych z normami i politykami bezpieczeństwa.

23

Bezzwłoczne zgłaszanie incydentów bezpieczeństwa

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §20 UST. 2 PKT 13**

TREŚĆ PODSTAWY

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie bezzwłocznego zgłaszania incydentów bezpieczeństwa w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących (patrz → wymaganie W32).

Opis wymagania

Wymaganie mówi o konieczności natychmiastowego zgłaszania incydentów bezpieczeństwa w określony i wcześniej ustalony sposób. Zgłaszanie powinno odbywać się bez zwłoki, aby umożliwić szybkie podjęcie działań naprawczych. Pomoże to ograniczyć skutki incydentu i zapobiec potencjalnemu rozprzestrzenianiu się zagrożenia.

W praktyce oznacza to, że jeśli wystąpi incydent, taki jak atak cyberprzestępców, wyciek danych lub inne naruszenie bezpieczeństwa informacji, powinno się to bezzwłocznie zgłosić odpowiednim osobom lub działom w organizacji, zgodnie z ustalonymi wcześniej procedurami.

Sposób zgłaszania incydentów w organizacji powinien być z góry ustalony. Może to obejmować:

1. **Określenie odpowiednich punktów kontaktowych**. Organizacja powinna wyznaczyć osoby lub zespoły, które będą odpowiedzialne za otrzymywanie zgłoszeń dotyczących incydentów bezpieczeństwa informacji. Mogą to być np. dział IT, zespół ds. bezpieczeństwa informacji lub osoba odpowiedzialna za zarządzanie incydentami.

2. **Ustalenie jasnych, zrozumiałych procedur**, które określą, jakie informacje i w jaki sposób powinny być przekazywane w zgłoszeniach dotyczących incydentów. Mogą to być formularze zgłoszeniowe, wyznaczone kanały komunikacji, adresy e-mail lub numery telefoniczne do osób wskazanych do bezpośredniego kontaktu.

3. **Priorytety i hierarchię zgłoszeń** – w przypadku różnych rodzajów incydentów należy ustalić, że najpilniejsze incydenty będą rozpatrywane w pierwszej kolejności, a działania korygujące będą podejmowane jak najszybciej.

4. **Szybkie podejmowanie działań korygujących** po zgłoszeniu incydentu w celu ograniczenia szkód i przywrócenia normalnych warunków funkcjonowania systemu. Mogą to być działania takie jak: izolowanie zainfekowanych systemów, zmiana haseł dostępowych, usuwanie podatności itp.

Bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji oraz stosowanie ustalonych procedur pozwala organizacji szybko reagować na zagrożenia i podejmować niezbędne działania, aby zminimalizować szkody wynikające z naruszeń bezpieczeństwa. Stosowane procedury muszą spełniać wymagania regulacji, którym podlega organizacja. Szczegóły wymagań wobec zgłoszeń do CSIRT znajdują się w UoKSC.

Rekomendowane działania – przykłady

1. Opracowanie procedur zgłaszania incydentów

Organizacja powinna opracować jasne i zrozumiałe procedury zgłaszania incydentów, które określają, kto i w jaki sposób powinien zgłaszać naruszenia bezpieczeństwa. Procedury te powinny być dostępne dla wszystkich pracowników.

2. Szkolenie pracowników

Pracownicy powinni być regularnie szkoleni w zakresie cyberbezpieczeństwa, aby potrafili rozpoznawać potencjalne zagrożenia i byli świadomi konsekwencji naruszenia bezpieczeństwa informacji. Szkolenia powinny obejmować m.in. identyfikację incydentów, procedury zgłaszania oraz podstawowe zasady bezpiecznego korzystania z systemów teleinformatycznych.

3. Wdrożenie narzędzi i systemów monitorujących oraz wykrywających incydenty

Jest to kluczowe dla szybkiego reagowania na nietypowe zdarzenia. **Automatyczne systemy monitorujące** mogą wykrywać nieprawidłowości, nieautoryzowane próby dostępu czy podejrzane aktywności, umożliwiając wczesne wykrycie incydentów i natychmiastowe ich zgłoszenie.

4. Wyznaczenie osób/zespołu odpowiedzialnego za reagowanie na incydenty

W organizacji powinien być wyznaczony zespół lub grupa osób odpowiedzialnych za reagowanie na incydenty. Osoby w tych grupach powinny mieć odpowiednie pełnomocnictwa i umiejętności, aby szybko podejmować działania korygujące w przypadku zidentyfikowania faktycznego naruszenia bezpieczeństwa informacji. Powinny być również odpowiednio szkolone i świadome procedur zgłaszania incydentów.

5. Przeprowadzanie regularnego przeglądu procedur zgłaszania incydentów

Organizacja powinna regularnie przeglądać i oceniać swoje procedury zgłaszania incydentów, aby upewnić się, że są one skuteczne i dostosowane do zmieniających się zagrożeń cyberbezpieczeństwa. Przeglądy te mogą uwzględniać identyfikację obszarów do poprawy, udoskonalenia i wprowadzać ulepszenia w celu zwiększenia efektywności i skuteczności procedur zgłaszania incydentów.

6. Przeprowadzenie analizy po zgłoszeniu incydentu

Po każdym zgłoszeniu incydentu należy przeprowadzić analizę, aby zrozumieć, jakie czynniki przyczyniły się do naruszenia bezpieczeństwa i jak można zapobiec podobnym incydentom w przyszłości. Na podstawie wniosków z analizy można wprowadzić odpowiednie poprawki, takie jak aktualizacje procedur, wzmocnienie zabezpieczeń czy szkolenia dodatkowe.

Działania doskonalące w powyższych obszarach pomogą organizacji w szybkim i skutecznym reagowaniu na incydenty bezpieczeństwa informacji, umożliwiając wczesne wykrycie, zgłaszanie i podejmowanie działań korygujących, co przyczyni się do zwiększenia poziomu cyberbezpieczeństwa.

24

Regularne prowadzenie audytów SZBI

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §20 UST. 2 PKT 14**

TREŚĆ PODSTAWY

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Opis wymagania

Należy **regularnie przeprowadzać audyt wewnętrzny,** który dotyczy bezpieczeństwa informacji. Audyt wewnętrzny to proces sprawdzania i oceny systemów, procedur i działań organizacji w celu upewnienia się, że są zgodne z określonymi standardami bezpieczeństwa. Audyt wewnętrzny powinien być przeprowadzany co najmniej raz w roku. Oznacza to, że specjaliści ds. bezpieczeństwa informacji w organizacji powinni regularnie przeglądać systemy, procedury i działania, aby sprawdzić, czy są one zgodne z przyjętymi standardami bezpieczeństwa.

Podczas audytu wewnętrznego przeprowadza się różne działania, takie jak:

1. **Ocena zgodności** – sprawdzenie czy organizacja przestrzega przyjętych standardów bezpieczeństwa informacji i polityk wewnętrznych.
2. **Identyfikacja i ocena ryzyka** związanego z bezpieczeństwem informacji oraz analiza istniejących kontroli i zabezpieczeń w celu zminimalizowania tych ryzyk.
3. **Przeprowadzanie testów zabezpieczeń**, np. testów bezpieczeństwa, aby sprawdzić, czy istniejące zabezpieczenia są skuteczne w zapobieganiu atakom i naruszeniom bezpieczeństwa.
4. **Analiza incydentów** – przeglądanie wcześniejszych wystąpień incydentów związanych z bezpieczeństwem informacji i analiza przyczyn ich wystąpienia oraz podejmowanie działań naprawczych.
5. **Określenie rekomendacji i działań naprawczych** na podstawie wyników audytu. Rekomendacje dotyczą poprawek, ulepszeń i działań naprawczych, które pomogą podnieść poziom bezpieczeństwa informacji.

Przeprowadzanie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji jest istotne, ponieważ pozwala organizacji monitorować i poprawiać swoje praktyki oraz zapobiegać potencjalnym zagrożeniom i incydentom związanym z bezpieczeństwem.

Rekomendowane działania – przykłady

1. **Opracowanie polityki prowadzenia audytów wewnętrznych**
2. **Opracowanie metodyki prowadzenia audytów wewnętrznych**
3. **Opracowanie procedury prowadzenia audytów wewnętrznych**
4. **Wyszkolenie zespołu odpowiedzialnego za prowadzenia audytów wewnętrznych**
5. **Wskazanie i umocowanie w jednostce zespołu odpowiedzialnego za prowadzenia audytów wewnętrznych**
6. **Regularne przeglądy i zarzadzanie wnioskami z audytów wewnętrznych**
7. **Regularne przeglądy dokumentacji z zakresu prowadzenia audytów w celu podejmowania działań doskonalących**

W przypadku braku wymaganych kompetencji i doświadczenia jednostki audyt należy zlecić ekspertom zewnętrznym. Dobrą praktyką jest włączenie audytorów wewnętrznych w prace ekspertów zewnętrznych w celu budowy kompetencji wewnętrznych.

25

Obligatoryjne zapisy działań w systemach

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §21 UST. 2**

TREŚĆ PODSTAWY

W dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do:

- systemu z uprawnieniami administracyjnymi;
- konfiguracji systemu, w tym konfiguracji zabezpieczeń;
- przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.

Opis wymagania

Wymaganie dotyczące dzienników systemów mówi nam o obowiązku rejestrowania pewnych działań, które podejmują użytkownicy lub elementy systemowe w ramach dostępu do systemu. Są trzy konkretne rodzaje działań, które muszą być zapisane w dziennikach:

1. **Działania związane z dostępem do systemu z uprawnieniami administracyjnymi.** Oznacza to, że korzystanie z specjalnych uprawnień administratora, takich jak pełny dostęp do systemu, za każdym razem musi być rejestrowane. Przykładowo, jeśli administrator zmienia ustawienia systemu, instaluje nowe oprogramowanie lub wykonuje inne czynności związane z zarządzaniem systemem, te informacje muszą zostać zapisane w dzienniku.

2. **Działania dotyczące konfiguracji systemu**, w tym konfiguracji zabezpieczeń. To oznacza, że wszelkie zmiany dokonywane w ustawieniach systemu, zwłaszcza związanych z zabezpieczeniami, muszą być rejestrowane – np. jeśli ktoś zmienia ustawienia firewalla, wprowadza nowe reguły bezpieczeństwa lub dokonuje innych modyfikacji mających wpływ na zabezpieczenia systemu, te informacje muszą być zapisane w dzienniku.

3. **Działania dotyczące przetwarzania danych objętych ochroną prawną.** Oznacza to, że jeśli w systemie przetwarzane są dane, które podlegają ochronie prawnej, np. dane osobowe, informacje finansowe lub inne poufne informacje, to wszystkie czynności związane z tym przetwarzaniem muszą być rejestrowane. Może to obejmować dostęp do danych, ich modyfikację, usuwanie lub inne operacje na danych objętych ochroną prawną. Te działania również muszą być zapisane w dziennikach zdarzeń.

Wszystkie te informacje są gromadzone w logach, w celu monitorowania i kontroli działań podejmowanych w systemach. Pomaga to w identyfikacji nieprawidłowości, audytach bezpieczeństwa oraz śledzeniu działań użytkowników w celu ochrony danych i zapewnienia zgodności z przepisami prawa dotyczącymi ochrony danych.

Rekomendowane działania – przykłady

1. **Wdrożenie wielopoziomowego uwierzytelniania** dla kont administratorów, takiego jak dwuskładnikowe uwierzytelnianie, aby utrudnić nieautoryzowany dostęp.

2. **Ustalenie polityki ograniczania uprawnień administracyjnych** tylko do niezbędnych zadań.

3. **Monitorowanie i analiza logów** związanych z działaniami administratorów w celu wczesnego wykrywania nieprawidłowości lub podejrzanych aktywności.

4. **Regularne przeglądy i audyty działań administratorów** w celu identyfikacji nieprawidłowości oraz weryfikacji zgodności z politykami bezpieczeństwa.

5. **Utworzenie procedur zmiany konfiguracji**, które wymagają uwierzytelnienia i autoryzacji przed wprowadzeniem zmian.

6. **Wdrożenie systemu monitorowania zmian w konfiguracji**, który powiadamia o wszelkich nieautoryzowanych modyfikacjach.

7. **Regularne przeglądy i aktualizacje konfiguracji zabezpieczeń** w celu dostosowania ich do najnowszych zagrożeń i najlepszych praktyk. Wdrażanie narzędzi automatyzujących procesy konfiguracji i zabezpieczeń w celu uniknięcia błędów ludzkich i zapewnienia spójności.

8. **Stworzenie polityki zarządzania dostępem do danych objętych ochroną prawną**, w tym przypisywanie uprawnień tylko tym osobom, które ich potrzebują.

9. **Wdrożenie systemu monitorowania dostępu do danych** w celu wykrywania nieautoryzowanych prób dostępu.

10. **Zastosowanie szyfrowania danych w systemie**, szczególnie dla danych poufnych lub wrażliwych.

11. **Regularne szkolenie pracowników** dotyczące przetwarzania danych objętych ochroną prawną, w tym świadomości zagrożeń i postępowania w przypadku naruszeń.

Wszystkie te działania doskonalące mają na celu zwiększenie poziomu ochrony informacji i minimalizowanie ryzyka związanego z dostępem do systemu, konfiguracją oraz przetwarzaniem danych. Ważne jest, aby takie działania były systematyczne, regularnie monitorowane i dostosowywane do zmieniających się zagrożeń oraz przepisów prawnych.

26

Dodatkowe zapisy działań w systemach

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §21 UST. 3**

TREŚĆ PODSTAWY

Poza informacjami wymienionymi w ust. 2 mogą być odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci:

- działań użytkowników nieposiadających uprawnień administracyjnych,
- zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu,
- zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny – w zakresie wynikającym z analizy ryzyka.

Opis wymagania

Wymaganie mówi, że oprócz informacji określonych w ust. 2 należy rejestrować również inne działania użytkowników i obiektów systemowych oraz różne zdarzenia związane z eksploatacją systemu. Dotyczy to:

1. **Działań użytkowników nieposiadających uprawnień administracyjnych.** Są to aktywności wykonywane przez zwykłych użytkowników, które mogą mieć wpływ na bezpieczeństwo systemu.
2. **Zdarzeń systemowych, nieposiadających krytycznego znaczenia dla funkcjonowania systemu** – rejestrowanie różnych zdarzeń, które nie są kluczowe dla działania systemu, ale mogą dostarczyć ważnych informacji dotyczących bezpieczeństwa, np. błędy systemowe, komunikaty informacyjne, ostrzeżenia czy inne zdarzenia, które nie powodują awarii systemu, ale mogą wskazywać na potencjalne zagrożenia.
3. **Zdarzeń i parametrów środowiska**, w którym eksploatowany jest system teleinformatyczny – rejestrowanie różnych zdarzeń i parametrów związanych z otoczeniem, w którym działa system. Obejmuje to informacje o środowisku, w którym system jest eksploatowany, np. temperaturę, wilgotność, dostęp do sieci czy inne czynniki mające wpływ na bezpieczeństwo i wydajność systemu.

Wymagane informacje są określane w oparciu o analizę ryzyka, która identyfikuje kluczowe aspekty środowiskowe.

Ważne jest, aby odpowiednie mechanizmy rejestrowania zostały wdrożone. Wszystkie informacje powinny być przechowywane w odpowiednich dziennikach systemowych w celu monitorowania, analizy i reagowania na potencjalne zagrożenia cyberbezpieczeństwa.

Rekomendowane działania – przykłady

1. Działania użytkowników nieposiadających uprawnień administracyjnych:

- Wdrożenie systemu uwierzytelniania i autoryzacji, który zapewnia dostęp do systemu tylko uprawnionym użytkownikom.
- Ustalanie precyzyjnych zasad dostępu do różnych funkcji systemu, ograniczając dostęp tylko do niezbędnych zasobów.
- Monitorowanie i analiza logów dotyczących działań użytkowników nieposiadających uprawnień administracyjnych w celu wykrywania podejrzanych lub nieautoryzowanych aktywności.
- Edukacja użytkowników na temat świadomego i odpowiedzialnego korzystania z systemu oraz zasad bezpieczeństwa informatycznego.

2. Zdarzenia systemowe nieposiadające krytycznego znaczenia dla funkcjonowania systemu:

- Wdrożenie narzędzi do monitorowania i analizy zdarzeń systemowych, które pozwolą wykrywać potencjalne zagrożenia i reagować na nie.
- Definiowanie reguł i wytycznych, które określają, które zdarzenia systemowe powinny być odnotowywane, a które można pomijać.
- Regularne przeglądy logów systemowych w celu identyfikacji ewentualnych nieprawidłowości lub nieautoryzowanych aktywności.
- Ustalanie procedur reagowania na awarie systemowe i monitorowanie parametrów systemowych w celu wykrycia anomalii.

3. Zdarzenia i parametry środowiska, w którym eksploatowany jest system teleinformatyczny w zakresie wynikającym z analizy ryzyka:

- Przeprowadzenie szczegółowej analizy ryzyka identyfikującej kluczowe zdarzenia i parametry środowiskowe, które powinny być rejestrowane.
- Wdrożenie narzędzi monitorujących środowisko, które zbierają informacje o zdarzeniach i parametrach istotnych dla bezpieczeństwa systemu.
- Określenie proaktywnych procedur monitorowania i reagowania na zmiany w środowisku, które mogą mieć wpływ na bezpieczeństwo systemu.
- Utrzymywanie aktualnej wiedzy na temat zagrożeń zewnętrznych i zmieniających się warunków środowiskowych oraz dostosowywanie procedur zgodnie z tą wiedzą.

Ważne jest, aby te działania doskonalące były dostosowane do konkretnych potrzeb i kontekstu jednostki oraz systemu teleinformatycznego. Regularne przeglądy, testy penetracyjne i oceny ryzyka powinny być również uwzględnione w procesie doskonalenia i utrzymania bezpieczeństwa systemu.

27

Czas przechowywania zapisów w systemach

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §21 UST. 4**

TREŚĆ PODSTAWY

Informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.

Opis wymagania

Wszystkie informacje rejestrowane w dziennikach systemów, takie jak logi, zdarzenia czy aktywności, muszą być przechowywane przez pewien czas. Czas ten może być ustalony w przepisach prawnych lub wewnętrznych regulacjach jednostki.

Jeśli istnieją konkretne przepisy odrębne, to czas przechowywania musi być z nimi zgodny. Jeśli jednak nie ma takich przepisów, to informacje w dziennikach systemów powinny być przechowywane przez okres dwóch lat.

Przechowywanie tych informacji ma na celu zapewnienie możliwości audytu, analizy, monitorowania i śledzenia działań w systemach teleinformatycznych. Ważne jest, aby jednostki przestrzegały tych wymagań przechowywania i utrzymywały odpowiednie archiwum dzienników systemów przez określony czas.

Rekomendowane działania – przykłady

1. **Opracowanie i wdrożenie polityki przechowywania informacji w dziennikach zdarzeń**, która określa konkretny czas przechowywania zgodny z przepisami odrębnymi lub standardami branżowymi.

2. **Ustalanie klarownych zasad** dotyczących przechowywania, archiwizacji i usuwania informacji w celu zapewnienia zgodności z wymaganiami.

3. **Wykorzystanie zaawansowanych narzędzi do zarządzania dziennikami zdarzeń.** Narzędzia te umożliwiają skuteczną kontrolę przechowywania i analizy logów. Automatyzacja procesu przechowywania i archiwizacji logów w celu uniknięcia potencjalnych błędów.

4. **Regularne przeglądy i audyty dzienników zdarzeń** służą one zapewnieniu zgodności z wymaganiami przechowywania informacji. Monitorowanie i weryfikacja pokazują, czy przechowywane informacje są kompleksowe, dokładne i zawierają niezbędne dane.

5. **Zastosowanie odpowiednich mechanizmów zabezpieczeń technicznych**, takich jak szyfrowanie, uwierzytelnianie dwuskładnikowe czy kontrole dostępu, aby chronić informacje przechowywane w dziennikach zdarzeń przed nieautoryzowanym dostępem lub manipulacją.

6. **Szkolenie pracowników** powinno uwzględniać zagadnienia związane z wymogami dotyczącymi przechowywania informacji w dziennikach zdarzeń, w tym właściwe obsługiwanie i zarządzanie dziennikami zdarzeń oraz identyfikację nieprawidłowości czy podejrzanych aktywności.

Ważne jest, aby te działania doskonalące były dostosowane do specyficznych potrzeb i kontekstu jednostki. Regularne monitorowanie i ocena skuteczności tych działań są kluczowe dla zapewnienia bezpiecznego i zgodnego przechowywania informacji w dziennikach zdarzeń.

28

Sposób przechowywania zapisów dzienników systemowych

KIERUNEK ROZWOJU:

PODSTAWA: **KRI §21 UST. 5**

TREŚĆ PODSTAWY

Zapisy dzienników systemów mogą być składowane na zewnętrznych informatycznych nośnikach danych w warunkach zapewniających bezpieczeństwo informacji. W uzasadnionych przypadkach dzienniki systemów mogą być prowadzone na nośniku papierowym.

Opis wymagania

Zapisy dzienników zdarzeń mogą być przechowywane na zewnętrznych nośnikach danych, takich jak dyski twarde, pamięci, macierze, serwery lub inne urządzenia informatyczne. Ważne jest, aby te nośniki były bezpieczne i chronione przed nieautoryzowanym dostępem.

W niektórych uzasadnionych przypadkach informacje zapisane w dziennikach zdarzeń mogą być drukowane i przechowywane na papierze.

W celu zapewnienia bezpieczeństwa informacji, niezależnie od tego czy są przechowywane na nośnikach elektronicznych, czy papierowych, należy spełnić odpowiednie warunki. Obejmują one:

1. **Zastosowanie odpowiednich środków bezpieczeństwa**, takich jak hasła, szyfrowanie lub kontrole dostępu, aby chronić zapisy dzienników systemów przed nieupoważnionym dostępem, manipulacją lub kradzieżą. Regularne monitorowanie i zarządzanie fizycznym dostępem do nośników danych.
2. **Bezpieczne przechowywanie nośników danych w odpowiednich warunkach**, takich jak sejfy, pomieszczenia z kontrolą temperatury i wilgotności, aby zapewnić ochronę przed uszkodzeniem, zniszczeniem lub kradzieżą.
3. **Regularne wykonywanie kopii zapasowych zapisów w dzienników zdarzeń systemów** w celu zapewnienia możliwości ich odtworzenia w przypadku utraty danych lub awarii.
4. **Utrzymanie poufności informacji zawartych w zapisach dzienników zdarzeń** i zapewnienie, że tylko upoważnione osoby mają do nich dostęp.

Wszystkie te środki mają na celu zapewnienie bezpiecznego przechowywania informacji zapisanych w dziennikach zdarzeń, niezależnie od formy nośników. Jednostki powinny dostosować swoje procedury i praktyki do tych wymagań, aby zapewnić odpowiedni poziom bezpieczeństwa dla swoich danych.

Rekomendowane działania – przykłady

1. **Zastosowanie zaawansowanych środków zabezpieczeń,** takich jak hasła, szyfrowanie czy metody uwierzytelniania dwuskładnikowego, dla nośników elektronicznych w celu ochrony przed nieupoważnionym dostępem i manipulacją.

2. **Zabezpieczenie fizycznego dostępu do nośników danych** poprzez stosowanie sejfów, kontroli dostępu do pomieszczeń czy monitoringu.

3. **Systematyczne monitorowanie i logowanie dostępu do zapisów dzienników systemów** na nośnikach danych, w celu wykrywania potencjalnych incydentów lub nieprawidłowości.

4. **Ustanowienie kontroli dostępu**, które ograniczają uprawnienia użytkowników do odczytu, zapisu lub modyfikacji zapisów dzienników systemów.

5. **Regularne przeglądy i audyty** dotyczące zabezpieczeń nośników danych, pozwalające sprawdzić ich skuteczność i adekwatność do ryzyka. Ocena i analiza zapisów z monitoringu w celu wczesnego wykrywania i reagowania na ewentualne zagrożenia.

6. **Wykorzystanie systemów kopii zapasowych** lub replikacji danych na różnych nośnikach w celu zapewnienia ochrony przed utratą danych w przypadku awarii lub uszkodzenia jednego nośnika.

7. **Edukacja pracowników** na temat znaczenia bezpiecznego przechowywania zapisów dzienników zdarzeń i świadomości ryzyka związanego z utratą lub nieuprawnionym dostępem do danych.

8. **Regularne szkolenia dotyczące postępowania w przypadku incydentów** związanych z przechowywaniem zapisów dzienników zdarzeń.

Ważne jest, aby te działania doskonalące były dostosowane do specyficznych potrzeb i kontekstu jednostki oraz uwzględniały ocenę ryzyka. Ciągłe monitorowanie, ocena skuteczności i aktualizacja środków bezpieczeństwa są niezbędne do zapewnienia ochrony zapisów dzienników zdarzeń na zewnętrznych nośnikach danych lub nośnikach papierowych.

29

Wyznaczenie osoby do kontaktu

KIERUNEK ROZWOJU:

PODSTAWA: **UOKSC ART. 21**

TREŚĆ PODSTAWY

Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, realizujący zadanie publiczne zależne od systemu informacyjnego jest obowiązany do wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

Opis wymagania

Formalnie wskazanie przez najwyższe kierownictwo osoby do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa. Wskazówki dotyczące wyboru tej osoby, jej zadań, sposobów kontaktu i wiele innych informacji znaleźć można w rekomendacjach przygotowanych wspólnie przez zespoły CSIRT poziomu krajowego.

Rekomendowane działania – przykłady

Wskazanie osoby do kontaktu

Zgodnie z rekomendacjami opracowanymi wspólnie przez zespoły CSIRT poziomu krajowego zaleca się, aby była to osoba:

- DYSPOZYCYJNA – tak aby w przypadku incydentu lub zagrożenia można było z nią sprawnie i szybko nawiązać kontakt (zwłaszcza po godzinach pracy instytucji);
- DECYZYJNA – tak aby w razie potrzeby mogła podjąć decyzję o przekazaniu/udostępnieniu informacji niezbędnych do obsługi incydentu oraz podjąć działania rekomendowane przez CSIRT poziomu krajowego lub wydać konkretne polecenia w organizacji;
- Z TECHNICZNYM ZROZUMIENIEM TEMATU – tak aby mieć łatwość komunikacji z CSIRT poziomu krajowego. Nie oznacza to jednak, że musi być osobą techniczną;
- O SILNIE ROZWINIĘTEJ SIECI KONTAKTÓW wewnętrznych w organizacji.

Rola osoby do kontaktu może być pełniona równolegle z innymi, takimi jak np. pełnomocnik ds. bezpieczeństwa informacji czy Inspektor Ochrony Danych Osobowych.

30

Przekazanie danych osoby wyznaczonej do kontaktu

KIERUNEK ROZWOJU:

PODSTAWA: **UOKSC ART. 22 UST. 1 PKT 5**

TREŚĆ PODSTAWY

Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, realizujący zadanie publiczne zależne od systemu informacyjnego: 5) przekazuje do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV dane osoby, o której mowa w art. 21, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14. dni od jej wyznaczenia, a także informacje o zmianie tych danych w terminie 14. dni od ich zmiany.

Opis wymagania

Skuteczne przekazanie danych osoby wyznaczonej do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa tym podmiotom. Pomocne będą rekomendacje zawarte pod linkiem wskazanym w wymaganiu W29.

Rekomendowane działania – przykłady

Zgłoszenie osoby kontaktowej do odpowiedniego CSIRT (w przypadku JST najczęściej będzie to CSIRT NASK)

W celu zgłoszenia osoby kontaktowej do CSIRT NASK lub aktualizacji danych należy:

- wypełnić formularz na stornie incydent.cert.pl/osoba-kontaktowa;
- wygenerowane pismo opatrzyć podpisem – elektronicznym lub tradycyjnym – kierownika jednostki;
- przesłać pismo na skrzynkę ePUAP (Naukowa i Akademicka Sieć Komputerowa PIB; adres skrzynki: /NASK-Instytut/SkrytkaESP, w tytule wpisać „Zgłoszenie osoby kontaktowej do CSIRT NASK”) lub na adres NASK-PIB wskazany w dokumencie (w przypadku operatora usługi kluczowej należy załączyć skan decyzji administracyjnej uznającej podmiot za operatora usługi kluczowej).

31

Zapewnienie zarządzania incydentem

KIERUNEK ROZWOJU:

PODSTAWA: **UOKSC ART. 22 UST. 1 PKT 1**

TREŚĆ PODSTAWY

Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, realizujący zadanie publiczne zależne od systemu informacyjnego: 1) zapewnia zarządzanie incydentem w podmiocie publicznym.

Opis wymagania

Zapewnienie zarządzania incydentem odnosi się do procesu i praktyk mających na celu skuteczne reagowanie na incydenty w dziedzinie cyberbezpieczeństwa. Incydentem może być np. atak, wyciek danych, naruszenie bezpieczeństwa sieci czy uszkodzenie systemu informatycznego. Warto pamiętać, że według definicji UOKSC incydentem jest także zagrożenie, które się nie zmaterializowało, ale zostało np. zablokowane.

Zarządzanie incydentem ma na celu minimalizowanie szkód wynikających z incydentu oraz przywrócenie normalnego działania systemu i ochrony przed dalszymi zagrożeniami. Obsługa incydentu to czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu (art. 2 pkt 10 UOKSC).

Rekomendowane działania – przykłady

1. Wdrożenie procesu obejmującego wszystkie aspekty związane z zarządzaniem incydentami

Proces ten obejmuje różne etapy, które mogą się różnić w zależności od specyfiki jednostki. Można jednak wskazać kilka kluczowych kroków:

- **Wykrycie incydentu.** Pierwszym krokiem jest wykrycie i rozpoznanie incydentu. Może to obejmować analizę nieprawidłowości w systemie, alarmy zabezpieczeń, sygnały o nieautoryzowanym dostępie lub inne wskaźniki wskazujące na możliwość incydentu.

- **Ocena i klasyfikacja incydentu.** Po wykryciu incydentu należy przeprowadzić jego ocenę i klasyfikację. Chodzi tu o określenie rodzaju i skali incydentu oraz jego potencjalnego wpływu na jednostkę.

- **Reakcja i ograniczanie szkód.** Następnie podejmuje się działania mające na celu ograniczenie szkód wynikających z incydentu. Może to obejmować odizolowanie zagrożonych systemów, zablokowanie dostępu dla potencjalnych atakujących, przywracanie danych z kopii zapasowych czy rozpoczęcie procesu śledzenia incydentu.

- **Analiza i śledzenie.** Po zabezpieczeniu systemu i przywróceniu normalnego działania, przeprowadza się analizę incydentu w celu zrozumienia przyczyn i sposobu jego wystąpienia. Śledzenie incydentu może również pomóc w identyfikacji potencjalnych słabych punktów systemu i wzmocnieniu zabezpieczeń.

- **Zapobieganie przyszłym incydentom.** Na podstawie analizy incydentu podejmuje się działania w celu wzmocnienia bezpieczeństwa systemu i zapobiegania przyszłym incydentom. Może to obejmować aktualizacje oprogramowania, zmiany w politykach bezpieczeństwa, dodatkowe szkolenia personelu itp.

2. Wdrożenie procedur i szkoleń

Jednostka musi mieć odpowiednio opracowane procedury zarządzania incydentem i odpowiednio przeszkolony personel, który jest w stanie skutecznie reagować na incydenty oraz przywracać normalne funkcjonowanie systemu.

32 Zgłaszanie incydentu

KIERUNEK ROZWOJU:

PODSTAWA: **UoKSC ART. 22 UST. 1 PKT 2**

TREŚĆ PODSTAWY

Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, realizujący zadanie publiczne zależne od systemu informacyjnego: 2) zgłasza incydent w podmiocie publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV.

Opis wymagania

Osoba wyznaczona w podmiocie publicznym zgłasza incydent niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV.

Rekomendowane działania – przykłady

1. Zgłoszenie incydentu

Incydent należy zgłosić za pośrednictwem odpowiedniego formularza. W przypadku JST najczęściej będzie to CSIRT NASK.

- CSIRT NASK: incydent.cert.pl
- CSIRT GOV: csirt.gov.pl/cer/zgloszenie-incydentu/16,Zgloszenie-incydentu-do-CSIRT-GOV.html
- CSIRT MON: csirt-mon.wp.mil.pl/pl/pages/zgloszenie-incydentu/

2. Możliwość wykorzystania narzędzia S46 w procesie zgłaszania incydentów

33

Zapewnienie obsługi incydentu

KIERUNEK ROZWOJU:

PODSTAWA: **UOKSC ART. 22 UST. 1 PKT 3**

TREŚĆ PODSTAWY

Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, realizujący zadanie publiczne zależne od systemu informacyjnego: 3) zapewnia obsługę incydentu w podmiocie publicznym i incydentu krytycznego we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe.

Opis wymagania

Realizacja obsługi incydentu jest realizowana przez JST zgodnie z wdrożonymi procesami i z użyciem wdrożonych narzędzi w zakresie realizacji zarządzania incydentem. Obsługa incydentu (jak wskazano w wymaganiu W31) to czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu (art. 2 pkt 10 UOKSC).

JST jako podmiot publiczny może wnioskować do właściwego CSIRT o wsparcie w obsłudze incydentu (art. 26 ust. 2 UOKSC). Wsparcie takie może zostać udzielone w uzasadnionych przypadkach, o czym decyduje właściwy CSIRT.

Rekomendowane działania – przykłady

Wdrożenie procesu obejmującego wszystkie aspekty związane z zarządzaniem incydentami oraz dotyczące procedur i szkoleń (→ patrz: W31).

34

Zapewnienie dostępu do wiedzy

KIERUNEK ROZWOJU:

PODSTAWA: **UOKSC ART. 22 UST. 1 PKT 4**

TREŚĆ PODSTAWY

Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, realizujący zadanie publiczne zależne od systemu informacyjnego: 4) zapewnia osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej.

Opis wymagania	Rekomendowane działania – przykłady
Zapewnienie osobom, na rzecz których zadanie publiczne jest realizowane, dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowania skutecznych sposobów zabezpieczania się przed tymi zagrożeniami. Informacje mogą być dostępne w różny sposób – tradycyjny (plakaty, broszury) lub online.	**Publikacja i aktualizacji informacji dotyczących cyberbezpieczeństwa, w serwisach internetowych jednostek lub/i tablicach informacyjnych w JST.**

07

Katalog wybranych rozwiązań w obszarze cyberbezpieczeństwa

W poniższym rozdziale przedstawione zostały propozycje poszczególnych rozwiązań technicznych, organizacyjnych i związanych z podnoszeniem kompetencji pracowników, które JST powinny rozważyć podczas planowania swoich działań i zakupów.

WIELOETAPOWOŚĆ

Proces poprawiania odporności instytucji na zagrożenia cyberbezpieczeństwa w ramach projektu „Cyberbezpieczny Samorząd" jest przedsięwzięciem wieloetapowym. Powinien rozpocząć się od oceny aktualnego stanu cyberbezpieczeństwa jednostki, a następnie objąć realizację zaplanowanej ścieżki podnoszenia dojrzałości cyberbezpieczeństwa. Zatwierdzony plan należy realizować etapowo, w poszczególnych obszarach – w zależności od zidentyfikowanych potrzeb, a także dostępnych środków i możliwości. Na każdym z etapów niezbędna jest współpraca różnych osób. Oprócz specjalistów ds. IT i bezpieczeństwa, istotne jest zaangażowanie pracowników odpowiedzialnych za przygotowanie i prowadzenie procedur zakupowych dotyczących m. in. szacowania wartości zamówień oraz wyboru dostawców[2].

POSTĘPOWANIA ZAKUPOWE

Procedury odnoszące się do zakupów w zakresie cyberbezpieczeństwa, poza odpowiednim określeniem przedmiotu zakupu, powinny uwzględniać wymagania bezpieczeństwa. W szczególności w ramach prowadzonego postepowania zakupowego nie powinny być ujawniane publicznie informacje mogące ułatwić dostęp do systemu informatycznego niepowołanym osobom.

FUNDUSZE EUROPEJSKIE

W przypadku finansowania zakupów z funduszy europejskich należy pamiętać o zapewnieniu trwałości projektu na czas, który jest określony w regulaminie naboru. Oznacza to konieczność utrzymania zrealizowanych celów projektu, gdy finansowanie projektu będzie zakończone. Często zakupione w projekcie urządzenia czy oprogramowanie wymagają ponoszenia również kosztów w przyszłości. Koszty te związane są m.in. z utrzymaniem sprawnego działania kupowanych urządzeń i oprogramowania, a także kontynuacją finansowania subskrypcji usług po okresie trwania projektu. Koszty operacyjne powinny mieć zapewnione finansowanie. Dlatego przy planowaniu zakupów należy zadbać o ograniczenie przyszłych kosztów usług, minimalizując tym samym środki potrzebne do utrzymania projektu. Można również zapewnić dodatkowe gwarancje dla zakupionych urządzeń i oprogramowania, które przedłużą okres ich ochrony.

2 Rekomendacje Prezesa UZP dotyczące zamówień publicznych na systemy informatyczne (cyberbezpieczeństwa dotyczy bezpośrednio Rozdział 8, Tom II).

Wydatki w obszarze organizacyjnym

Środki można przeznaczyć na następujące działania (koszty osobowe lub usługi):

1. **Opracowanie, wdrożenie, przegląd, aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).**

2. **Audyt SZBI, audyt zgodności z wymaganiami KRI / uoKSC** przez wykwalifikowanych audytorów, (re)certyfikacja SZBI na zgodność z normami.

3. **Wprowadzenie lub aktualizacja Polityk Bezpieczeństwa Informacji (PBI)**, analiza ryzyka (w tym opracowanie i wdrożenie metodyk), opracowanie procedur: obsługi incydentów, ciągłości działania i zarządzania kryzysowego, stosowania kryptografii, kontroli dostępu, bezpieczeństwa pracy zdalnej, używania urządzeń mobilnych itp.

Wydatki w obszarze kompetencyjnym

Środki można przeznaczyć na następujące działania (koszty osobowe lub usługi):

1. **Podstawowe szkolenia** (lub dostęp do platform szkoleniowych) **budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników JST.**

2. **Szkolenia z zakresu cyberbezpieczeństwa dla wybranych przedstawicieli kadry JST,** istotnych z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji.

3. **Szkolenia specjalistyczne dla kadry zarządzającej i informatyków** w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa.

4. **Szkolenia powiązane z testami socjotechnicznymi,** które będą weryfikować świadomość zagrożeń i reakcje personelu, w szczególności sposób postępowania specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami.

Wydatki w obszarze technicznym

Środki można przeznaczyć na następujące działania (usługi lub dostawy):

1. **Zakup, wdrożenie i utrzymanie systemów teleinformatycznych,** w tym urządzeń, oprogramowania i usług zapewniających prewencję, detekcję i reakcję na zagrożenia cyberbezpieczeństwa, z niezbędnym wsparciem producenta.

2. **Zakup, wdrożenie i utrzymanie rozwiązań ciągłego monitorowania bezpieczeństwa** (skanery podatności, zarządzanie podatnościami, zarządzanie zasobami IT i aktywami podlegającymi ochronie) oraz innych narzędzi wymienionych poniżej w katalogu klas rozwiązań.

3. **Zakup, wdrożenie, konfiguracja oraz utrzymanie urządzeń i oprogramowania.**

4. **Zakup usług wsparcia** realizowanych przez zewnętrznych ekspertów z zakresu cyberbezpieczeństwa.

5. **Zakup, wdrożenie i utrzymanie systemów lub usług na potrzeby operacyjnych centrów cyberbezpieczeństwa** (SOC, ang. *Security Operations Centre*), także jako element Centrum Usług Wspólnych,

6. **Zakup testów i badań bezpieczeństwa, dostępu do usług rozpoznawania zagrożeń w cyberprzestrzeni – CTI** (ang. *Cyber Threat Intelligence*), dostępu do informacji bezpieczeństwa (np. ang. *feeds*) oraz innych usług integracyjnych dotyczących obszaru cyberbezpieczeństwa.

Katalog typów rozwiązań technicznych

Poniżej przedstawiony jest katalog typów rozwiązań technicznych (wraz z wyjaśnieniami), które warto rozważyć przy planowaniu wydatkowania środków przeznaczonych na cyberbezpieczeństwo). Należy pamiętać, że wybrane rozwiązania muszą spełniać warunki niezbędne do realizacji celów w ramach kosztów kwalifikowanych w projekcie.

Rozwiązania klasy Anty-DDoS
(ang. *Anti-Distributed Denial of Service*)

to środki, techniki i rozwiązania *(*sprzętowe, programowe lub usługi), realizujące ochronę przed atakami typu DDoS na systemy komputerowe lub usługi sieciowe. Zapobiegają przeciążeniu infrastruktury IT alokacją dużej ilości jej zasobów przez czynniki zewnętrzne, niezależne od organizacji, mające na celu zakłócenie dostępności docelowego systemu, sieci lub usługi poprzez przytłoczenie ich zalewem złośliwego ruchu z wielu źródeł. Zwykle Anty-DDoS jest wykorzystywany do ochrony punktów styku sieci organizacji z sieciami publicznymi. Anty-DDoS może być usługą utrzymywaną wewnątrz organizacji lub przez zewnętrznego operatora – np. dostawcę dostępu do internetu.

Anty-DDoS, znany również jako Anti-DDoS, odnosi się do środków, technik i rozwiązań wykorzystywanych do obrony przed atakami typu Distributed Denial of Service (DDoS). Ataki DDoS mają na celu zakłócenie dostępności docelowego systemu, sieci lub usługi poprzez przytłoczenie ich zalewem złośliwego ruchu z wielu źródeł.

Rozwiązania klasy EDR
(ang. *Endpoint Detection and Response*)

to zintegrowane systemy bezpieczeństwa, których główne funkcje to: monitorowanie i gromadzenie danych o aktywnościach użytkowników i oprogramowania na urządzeniach końcowych oraz analiza tych danych w celu identyfikacji wzorców zagrożeń, automatyczne reagowanie na zidentyfikowane zagrożenia w celu ich usunięcia lub powstrzymania oraz powiadamianie personelu bezpieczeństwa o zidentyfikowanych anomaliach. Narzędzia EDR odpowiadają także za wykrywanie zagrożeń i reagowanie na nie na urządzeniach końcowych (komputery stanowiskowe, komputery i urządzenia przenośne, serwery). Rozwiązania EDR analizują, monitorują oraz zapisują informacje o działaniu systemów oraz procesów za pomocą zainstalowanych agentów. Dają dzięki temu dużą widoczność i wiedzę o lokalnych zdarzeniach na stacjach roboczych i serwerach. Technologia ta pozwala na wykrywanie zagrożeń także w pamięci operacyjnej komputerów.

Rozwiązania klasy XDR
(ang. *Extended Detectio and Response*)

służą gromadzeniu i automatycznemu korelowaniu informacji z wielu źródeł (systemów operacyjnych, dzienników zdarzeń, poczty elektronicznej, urządzeń końcowych, serwerów, sieci, aplikacji itp.). Automatyczna analiza takich zbiorów danych o zdarzeniach w infrastrukturze pozwala na szybsze wykrywanie zagrożeń, dokładniejsze badanie anomalii, identyfikację incydentów i szybsze reagowanie na nie.

Zapora sieciowa
(ang. *Firewall lub Next Generation Firewall*)

to rozwiązanie, którego celem jest analiza i filtracja pakietów protokołów sieciowych przesyłanych na styku dwóch odseparowanych sieci informatycznych. Zapory sieciowe nowej generacji (NGFW) mogą być oparte na oprogramowaniu lub sprzęcie. Mają funkcjonalność znacznie rozszerzoną poza ocenę i filtrację pakietów danych. Dokonują głębokiej inspekcji pakietów, nie ograniczając się tylko do sprawdzenia numerów portów i typów protokołów. Umożliwiają kontrolę ruchu na poziomie warstwy aplikacji, zapobiegają włamaniom i mogą korzystać z różnych mechanizmów wykraczających poza funkcjonalność klasycznej zapory sieciowej.

Rozwiązania MDM
(ang. *Mobile device management*)

to oprogramowanie, które umożliwia administratorom IT monitorowanie, zarządzanie i zabezpieczanie służbowych urządzeń mobilnych, takich jak smartfon czy tablet. MDM pozwala zespołom IT na zdalną aktualizację i zabezpieczanie urządzeń mobilnych za pośrednictwem centralnej konsoli zarządzania. W zakres tego zarządzania może wchodzić: zarządzanie aplikacjami, wymuszanie zmian haseł, wymuszanie aktualizacji urządzeń, definiowanie polityk ściśle określających zakres działań użytkowników na urządzeniach mobilnych w celu zapewnienia im systemowych mechanizmów bezpieczeństwa.

Oprogramowanie antywirusowe
(ang. *antivirus, AV*)

to rozwiązania od lat stosowane do zabezpieczania komputerów stacjonarnych i mobilnych. Ich działanie oparte jest na wykrywaniu znanych zagrożeń w oparciu o specjalnie przygotowane zestawy sygnatur przygotowanych przez producenta danego rozwiązania. Producenci systemów AV zaczęli wbudowywać w swoje rozwiązania funkcje wykrywania anomalii, szkodliwego oprogramowania – w oparciu o jego zachowania (tzw. analiza heurystyczna, behawioralna).

Rozwiązania antymalware

to narzędzia wykrywające zagrożenia na urządzeniach końcowych. Ich zadaniem jest: skanowanie plików, dogłębna analiza ich struktury, danych i logiki w poszukiwaniu nietypowych instrukcji i szkodliwych fragmentów kodu.

Rozwiązania UTM
(ang. *Unified Threat Management*)

urządzenia sieciowe, odpowiadające za kompleksową ochronę, nadzorowanie ruchu w sieci lokalnej oraz styk/dostęp do internetu. Zamiast wielu rozwiązań typu: zapory sieciowe, IPS, filtry antyspamowe, routery itp. – jedno rozwiązanie, łączące wszystkie te funkcje. Zalecane jest zapoznanie się z zagadnieniami wydajności konkretnych urządzeń, ich możliwościami analizy pakietów oraz dodatkową funkcjonalnością.

Rozwiązania klasy IDS
(ang. *Intrusion Detection System*)

to systemy służące do wykrywania niepożądanych aktywności w infrastrukturze IT oraz informowania o ich wystąpieniu odpowiednich funkcji lub osób w organizacji. Bardziej zaawansowaną formą IDS są rozwiązania IPS.

Rozwiązania klasy IPS
(ang. *Intrusion Prevention System*)

to systemy służące do zapobiegania niepożądanym aktywnościom w infrastrukturze organizacji i ich skutkom, tj. próbom włamań czy przełamania zabezpieczeń. Zadaniem IPS jest także wykrywanie takich działań w sieci organizacji, podejmowanie prób zapobiegania ich skutkom oraz informowanie o ich wystąpieniu odpowiednich funkcji lub osób. IPS posiadają także funkcje analizy anomalii, pozwalające na wykrywanie nieobserwowanych wcześniej zagrożeń.

Rozwiązania klasy SIEM
(ang. *Security Information and Event Management*)

ułatwiają wykrywanie i analizowanie zagrożeń dla bezpieczeństwa oraz reagowanie na nie, zanim zaszkodzą one operacjom biznesowym. Rozwiązania te mogą być zasilane informacjami z różnych źródeł, takich jak zapory sieciowe, serwery usług, routerów, dzienników zdarzeń (ang. *logs*). Zbierane zdarzenia są analizowane i korelowane, co pozwala przewidywać potencjalne ataki. Dzięki przygotowanym specjalnym interfejsom do prezentacji sytuacji stanowią jedno z podstawowych narzędzi pracy operatorów/analityków w operacyjnych centrach bezpieczeństwa (ang. *Security Operations Center*, SOC).

Systemy klasy SOAR
(ang. *Security Orchestration Automation and Response*)

to uniwersalne platformy, które zapewniają jeden punkt wspólny pracy dla zespołów cyberbezpieczeństwa przy obsłudze incydentów bezpieczeństwa. Najważniejszą zaletą tego typu systemów jest możliwość automatyzacji częściowej lub całościowej procesu obsługi incydentu bezpieczeństwa w ramach tzw. playbooka, czyli możliwość szybkiej odpowiedź na incydenty poprzez generowanie alertów, tworzenie zautomatyzowanych reguł reakcji itp.

Rozwiązania klasy NAC
(ang. *Network Access Control*)

służą do kontroli dostępu do sieci korporacyjnej. Zapewniają pełny wgląd we wszystkie działania urządzeń i użytkowników korzystających z zasobów sieciowych instytucji – zarówno fizycznych, jak i wirtualnych. Systemy NAC egzekwują stosowanie polityki bezpieczeństwa informacji przez urządzenia próbujące otrzymać dostęp do sieci bezprzewodowych, przewodowych i VPN, blokując je w razie jakichkolwiek nieprawidłowości.

Rozwiązania IAM/IDM
(ang. *Identity Access Manager/ Identity Manager*)

umożliwiają zarządzanie tożsamościami cyfrowymi użytkowników oraz ich dostępami w obrębie infrastruktury IT organizacji. Dzięki wdrożeniu IAM/IDM można centralizować kontrolę dostępu użytkowników do określonych informacji w organizacji,

IAM/IDM umożliwia administratorom śledzenie działań użytkowników (rozliczalność), tworzenie raportów na temat ich działań oraz egzekwowanie zasad bezpieczeństwa. IAM/IDM pozwala zarządzać dostępami przez przypisywanie użytkowników do grup oraz nadawanie im ról, wyznaczanie zakresu dostępu do danych, administrację uprawnień oraz ich aktualizację, weryfikację i zarządzanie hasłami. Przy aktualnych wymogach prawnych są to rozwiązania niezbędne do odpowiedniego zarządzania dostępem do usług i danych w skali całej organizacji.

Rozwiązania BDR
(ang. *Backup and Disaster Recovery*)

to kompleksowe, scentralizowane narzędzia do tworzenia kopii zapasowych i odzyskiwania danych i całych systemów po awarii. Są niezbędne do utrzymaniu ciągłości działania instytucji – ograniczają ryzyko utraty danych.

Narzędzia oceny ryzyka
(ang. *Risk Assesment Tools*)

to narzędzia, które mogą pomóc usprawnić proces oceny ryzyka związanego z cyberbezpieczeństwem i poprawić dokładność wyników. Oceny ryzyka przygotowane przy wsparciu takich narzędzi mogą być przydatne do raportowania bezpieczeństwa do kierownictwa jednostki. Korzystanie z wyników oceny pozwala zweryfikować i uzasadnić plany inwestycyjne i zapewnić podjęcie kluczowych decyzji związanych z bezpieczeństwem. Pomogą również uzyskać zgodę zarządu JST na przyjęcie odpowiednich polityk i zasad w odniesieniu do różnych funkcji związanych z cyberbezpieczeństwem.

Systemy klasy GRC
(ang. *Goverment, Risk Management and Compliance*)

umożliwiają zarządzanie ryzykiem braku zgodności z obowiązującymi przepisami i wewnętrznymi procedurami, zapewniając stałe monitorowanie wymagań regulacyjnych i prawnych. Pomagają zorganizować i uporządkować współpracę i wspólne działania trzech grup procesów: zarządczych, zarządzania ryzykiem w skali organizacji oraz zarządzania zgodnością z wewnętrznymi i zewnętrznymi normami, regulacjami branżowymi i prawnymi. GRC pomaga instytucjom w identyfikacji, zarządzaniu i kontrolowaniu różnych rodzajów ryzyk związanych z działalnością oraz zapewnia, że organizacja działa zgodnie z wymaganiami i regulacjami otoczenia.

Oprogramowanie SAM
(ang. *Software Asset Management*)

to rozwiązanie pozwalające efektywnie zarządzać oprogramowaniem wykorzystywanym w instytucji. Skupia się przede wszystkim na aspekcie licencyjnym, natomiast umożliwia również kompleksowy wgląd w infrastrukturę IT, oprogramowanie w niej wykorzystywane oraz zagrożenia związane z jego użytkowaniem. Docelowo SAM pozwala instytucji na monitorowanie zgodności licencyjnej, optymalizowanie kosztów związanych z oprogramowaniem, eliminowanie niewspieranego oprogramowania oraz dostosowywanie inwestycji IT do potrzeb działalności.

Rozwiązania klasy DAM
(ang. *Database Access Management*)

pozwalają na zarządzanie dostępami do baz danych. Mogą określać: jakie konta mogą mieć dostęp do których baz i ich obszarów lub elementów oraz z jakie prawa do przetwarzania ich zawartości posiadają. DAM zapewnia nie tylko bezpieczeństwo danych przechowywanych w bazach, ale także monitorowanie i rozliczalność aktywności użytkowników baz danych.

Narzędzia CMDB
(ang. *Configuration Management DataBase*)

bazują na utrzymywaniu bazy danych, zawierającej dwa typy aktualizowanych na bieżąco informacji: szczegóły każdego komponentu infrastruktury IT (jego konfiguracji (ang. *Configuration Item, CI*) oraz bazę relacji między elementami CI. Baza CI mówi o sprzęcie i komponentach oprogramowania wykorzystywanych w usługach IT, którymi można zarządzać a także o samych usługach. CMDB pozwala na wykrywanie i odnotowywanie zmian inwentaryzacyjnych, a dzięki bazie relacji można oszacować wpływ tych zmian na wszystkie procesy, usługi i infrastrukturę. CMDB może także wspomagać automatyczną inwentaryzację zasobów IT organizacji oraz wspierać zarządzanie procesem zmian. CMDB pozwala dodatkowo na zbieranie, przechowywanie w uporządkowany sposób i zarządzanie konfiguracją usług, systemów i urządzeń. Ciągłe monitorowanie aktywnych konfiguracji pozwala wykryć nieautoryzowane lub nieudane zmiany konfiguracji, co ma istotny wpływ na cyberbezpieczeństwo.

Urządzenia HSM
(ang. *Hardware Security Module*)

to rozwiązania sprzętowe, dedykowane do bezpiecznego przechowywania, zarządzania i ochrony kluczy kryptograficznych, używane przede wszystkim jako procesory kryptograficzne do efektywnego i szybkiego szyfrowania i deszyfrowania informacji z użyciem kluczy.

08

Dobre praktyki

Celem niniejszego rozdziału jest prezentacja przykładów rozwiązań dostępnych w obszarze cyberbezpieczeństwa. Mogą one stanowić inspirację dla JST – obejmują zarówno technologiczne środki bezpieczeństwa, jak i procedury zarządzania ryzykiem, audyty bezpieczeństwa, szkolenia personelu oraz współpracę z innymi podmiotami w zakresie wymiany informacji i wspólnych działań w celu zapewnienia cyberbezpieczeństwa.

8.1 —— Organizacja Centrum Usług Wspólnych

Liczba przepisów nakładających na JST obowiązki w zakresie zapewnienia bezpieczeństwa infrastruktury i danych jest duża. Ograniczając się tylko do KRI, uoKSC i RODO, zakres wymagań nadal pozostaje bardzo szeroki, co pokazują wcześniejsze rozdziały. Jednocześnie wnioski płynące z „Diagnozy Cyberbezpieczeństwa" pokazują, że większość jednostek samorządu terytorialnego nie jest w stanie sprostać tym wymaganiom.

Główne problemy wynikają z niewystarczających zasobów finansowych i kompetencji personelu. Z drugiej strony w sytuacji małych podmiotów, do 50 stanowisk, kompleksowe inwestycje – czy to w środki trwałe, czy wyszkolony personel – nie zawsze będą racjonalne. W takich sytuacjach warto rozważyć mechanizm dostępny dla JST od 2017 r. Przychodzą tu z pomocą przepisy ustaw samorządowych (o samorządzie gminnym, powiatowym i wojewódzkim).

Centrum Usług Wspólnych (CUW) to rozwiązanie pozwalające skupić w ramach jednej, wyspecjalizowanej, jednostki obsługę, która może być realizowana na rzecz większości ekosystemu samorządowego. CUW może być utworzone w ramach jednej z jednostek lub być wydzieloną jednostką organizacyjną. W przypadku już istniejących Centrów, które nie świadczą obsługi z obszaru administracji i zarządzania bezpieczeństwem teleinformatycznym, warto rozważyć rozszerzenie ich zadań i kompetencji o te aspekty.

Jak utworzyć CUW?

Do pełnego operacyjnego działania Centrum potrzebne będzie lokum spełniające odpowiednie wymogi bezpieczeństwa, wyposażenie, narzędzia i oczywiście personel. Może to jednak pozwolić na pokonanie organizacyjnej lub finansowej bariery odnośnie do profesjonalnych usług IT i bezpieczeństwa oraz umożliwić dostęp do specjalistów poszczególnym jednostkom, niedysponującym wystarczającymi środkami do korzystania z usług o odpowiedniej jakości lub w wymiarze czasowym/ilościowym optymalnym dla ich potrzeb.

3 Przykłady dobrych praktyk można znaleźć na stronach internetowych wybranych CUW – (usługi sieciowe, obsługa teleinformatyczna) czy Centrum Cyberbezpieczeństwa i Ochrony Danych.

Jaki zakres obsługi mógłby realizować CUW w obszarze IT i bezpieczeństwa?

Katalog wewnętrznych usług, które zadaniem ekspertów[3] warto przenieść do Centrum Usług Wspólnych, jest szeroki. Można podzielić je w następujący sposób:

Usługi teleinformatyczne:

- obsługa dostępu do usług oraz infrastruktury teleinformatycznej na rzecz jednostek obsługiwanych, w tym dostępu do Internetu oraz telefonii stacjonarnej;
- zapewnienie prawidłowego działania systemów i infrastruktury teleinformatycznej;
- administrowanie systemami i infrastrukturą teleinformatyczną;
- zapewnienie zgodnego z warunkami umów, licencji, gwarancji nadzoru nad eksploatacją systemów i infrastruktury teleinformatycznej;

- zapewnienie wsparcia technicznego dla końcowych użytkowników;
- prowadzenie nadzoru nad zachowaniem spójności i interoperacyjności systemów teleinformatycznych i infrastruktury teleinformatycznej wdrażanej i eksploatowanej przez jednostki obsługiwane;
- współpraca z jednostkami obsługiwanymi przy wdrażaniu i aktualizowaniu procedur bezpieczeństwa systemów teleinformatycznych i infrastruktury teleinformatycznej;
- projektowanie i rozbudowa usług teleinformatycznych;
- współpraca z jednostkami obsługiwanymi przy:
  - zamawianiu dostaw i usług,
  - wdrażaniu nowych systemów teleinformatycznych,
  - uruchamianiu usług teleinformatycznych.

Usługi zapewnienia bezpieczeństwa informacji:

- włączenie obsługiwane podmioty we wspólny System Zarządzania Bezpieczeństwem Informacji;
- wsparcie w zakresie oceny ryzyka;
- wsparcie w procesie zarządzania incydentem i zgłoszeniu incydentu cyberbezpieczeństwa;
- włączenie obsługiwane podmioty do systemu agregacji i analizy zdarzeń w systemach teleinformatycznych;
- stanowienie osoby do kontaktu zgodnie z art. 21 ust 1–3 UOKSC;
- wsparcie w procesie ustawicznego podnoszenia odporności systemów poprzez rozwój techniczny i organizacyjny, a także podnoszenie świadomości pracowników obsługiwanych podmiotów.

Można rozważyć obsługę realizacji wybranych obowiązków administratora danych, wynikających z RODO, zwłaszcza dotyczących bezpieczeństwa przetwarzania danych, a także zatrudnienie w CUW wspólnego inspektora ochrony danych osobowych.

Powyższe listy warto przeanalizować zwłaszcza w kontekście wyboru spośród wskazanych zagadnień, w celu wpisania do uchwały rady gminy szczegółowych obowiązków CUW, o których mowa w art. 10b ust. 2 pkt 3. ustawy o samorządzie gminnym.

W przypadku gdy JST deleguje usługi na zewnątrz, konieczne będzie przeprowadzanie regularnych weryfikacji w celu upewnienia się, czy usługa jest zgodna z wymaganiami dotyczącymi Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz parametrami niezbędnymi do skutecznego świadczenia danej usługi.

8.2 Rozwiązania chmurowe w administracji państwowej

W celu spełnienia obowiązujących wymogów prawnych nałożonych na JST można rozważyć wdrożenie określonych rozwiązań techniczno-organizacyjnych, w tym rozwiązań chmurowych. Będą one korzystne także z perspektywy ekonomicznej.

W tym zakresie istotne są następujące regulacje:

- Narodowe Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO) wraz z pięcioma załącznikami, z których dwa ostatnie są osobnymi dokumentami (wszystkie dostępne na: chmura.gov.pl/informacje/scco);
- Uchwała nr 97 Rady Ministrów z 11. września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa”l (najnowsza wersja z 2021: isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WMP20210001006).

W cytowanej Uchwale znajduje się tabela z 15 kategoriami systemów, które można przenosić do trzech rodzajów chmur obliczeniowych:

1. Rządowa Chmura Obliczeniowa,
2. Publiczna Chmura Obliczeniowa w jurysdykcji krajowej,
3. Publiczna Chmura Obliczeniowa w jurysdykcji państwa UE.

Czym jest chmura obliczeniowa?

Według Narodowego Instytutu Norm i Technologii (*National Institute of Standards and Technology,* NIST – amerykańska agencja federalna) chmura obliczeniowa jest modelem umożliwiającym powszechny, wygodny dostęp do wspólnej puli konfigurowalnych zasobów obliczeniowych (np. sieci, serwerów, pamięci masowych, aplikacji i usług), które mogą być szybko dostarczone i uruchomione przy minimalnym wysiłku zarządczym lub interakcji z dostawcą usług.

Chmura obliczeniowa to metoda przechowywania, pobierania i przetwarzania danych oraz uzyskiwania dostępu do oprogramowania przez internet (lub inne sieci). Zamiast kupować, posiadać i utrzymywać określone aktywa fizyczne lokalnie (ang. *on-premise*), można uzyskiwać dostęp do usług chmurowych, takich jak moc obliczeniowa, przechowywanie i aplikacje, w zależności od aktualnych potrzeb. Może to pozwolić na szybsze wprowadzanie innowacji, elastyczne zmiany ilości zasobów i istotne korzyści skali.

Istnieją trzy główne modele świadczenia usług chmurowych:

1. **OPROGRAMOWANIE JAKO USŁUGA**

   (ang. *Software as a Service* – SaaS) umożliwia korzystanie z aplikacji za pomocą internetu;

2. **PLATFORMA JAKO USŁUGA**

   (ang. *Platform as a Service* – PaaS) dostarcza internetową platformę obliczeniową, na której można rozwijać, testować i wdrażać aplikacje;

3. **INFRASTRUKTURA JAKO USŁUGA**

   (ang. *Infrastructure as a Service* – IaaS) zapewnia dostęp za pomocą internetu do zwirtualizowanych zasobów fizycznych, co pozwala rozwijać oprogramowanie bez konieczności zakupu lub konserwacji własnego sprzętu.

Dlaczego warto używać technologii chmurowych?

Chmura obliczeniowa stanowi inny sposób wdrażania zasobów informatycznych, który oferuje istotne korzyści. Niektóre z nich zostały wymienione poniżej.

NAJLEPSZE W SWOJEJ KLASIE FUNKCJONALNOŚCI

Rozwiązaniom informatycznym typu *on-premise* trudno jest osiągnąć poziom dorównujący temu oferowanemu przez podstawowe produkty chmurowe. Przykładowo przy użyciu rozwiązania *on-premise* nie jest możliwe (a przynajmniej nie jest efektywne kosztowo) zapewnienie nieograniczonej pojemności danych dla pracowników ani umożliwienie dzielenia się dokumentami i zdalnej pracy nad nimi.

WSPARCIE I UTRZYMANIE

Rozwiązania IT typu *on-premise* (zarówno zewnętrzne, jak i wewnętrzne) wymagają odpowiedniego budżetu, wysiłku i planowania w celu zapewnienia wsparcia, utrzymania i aktualizacji. Wyzwaniem jest nadążanie za ciągłym zapotrzebowaniem na aktualizacje i poprawki bezpieczeństwa. W przypadku administracji publicznej, która podlega znacznemu nadzorowi budżetowemu, powstaje ryzyko, że technologia typu *on-premise* stanie się nieaktualna ze względu na koszty i trudności związane z jej wsparciem. Usługi chmurowe świadczone są zazwyczaj w ramach regularnego programu aktualizacji, poprawek i ulepszeń, przeważnie wliczanych w koszty. Oznacza to, że możliwe jest uniknięcie aktualizacji systemów operacyjnych serwerów, zakupu nowego sprzętu oraz zatrudniania konsultantów w celu utrzymania korzyści związanych z posiadaniem aktualnych technologii.

Rozwiązania nieoparte na chmurze często oznaczają oprogramowanie „klienckie", zainstalowane na urządzeniu użytkownika. Oprogramowanie to musi być zarządzane wraz z pozostałymi aplikacjami lokalnymi. W przeciwieństwie do rozwiązań nieopartych na chmurze usługi chmurowe zaprojektowane są w taki sposób, aby umożliwić dostęp do tych usług przez internet, za pomocą przeglądarki internetowej. W ten sposób liczba aplikacji lokalnych na urządzeniach użytkownika może zostać zminimalizowana. Dla JST, wykorzystujących setki lub nawet tysiące urządzeń takich jak komputery stacjonarne, laptopy i tablety, zmniejszenie ilości oprogramowania zainstalowanego na tych urządzeniach może być bardzo korzystne zarówno finansowo, jak i pod względem nakładów na ich utrzymanie i zarządzanie nimi.

ZAPEWNIENIE ELASTYCZNOŚCI DLA PRZYSZŁYCH ZASTOSOWAŃ

Rozwijanie rozwiązań *on-premise* prowadzi do powstania wysoce zindywidualizowanych, złożonych systemów, które trzeba utrzymywać lokalnie. To z kolei może utrudnić wspieranie takich rozwiązań, a z czasem doprowadzić do radykalnego zwiększenia kosztów, czasu i ryzyka związanego z realizacją programów rozwoju i zmian w zakresie IT. Rozwiązania chmurowe są z natury rzeczy ograniczone pod względem liczby dostępnych możliwości indywidualnego dostosowania, ale jednocześnie zapewniają możliwość wyboru konfiguracji. Pozwala to w pewnym stopniu dostosować te rozwiązania do potrzeb klientów, jednakże z pominięciem złożoności infrastruktury. Przykładowo dane z rozwiązań chmurowych są zazwyczaj pobierane za pomocą interfejsów API – co oznacza, że mogą być przenoszone w standardowym, rozpoznawanym formacie w celu łatwiejszej archiwizacji lub migracji do alternatywnych rozwiązań.

ELASTYCZNOŚĆ

Nawet najbardziej wydajne rozwiązania typu *on-premise* mają ograniczenia w zakresie pojemności zasobów dostępnych dla użytkowników. W miarę wzrostu zapotrzebowania na usługi (np. na skutek zmian w prawie mogą być wymagane dodatkowe zasoby) potrzebne będą regularne inwestycje i nakłady w zakresie zarządzania projektami, aby zapewnić utrzymanie wystarczającej pojemności zasobów. Zarządzanie wysoce zmiennym lub sezonowym zapotrzebowaniem na usługi wymaga zazwyczaj zakupu nadwyżki przepustowości, która poza okresami szczytowymi pozostaje niewykorzystana. Usługi chmurowe mogą pozwolić na uniknięcie tych wyzwań. Określone zasoby mogą być dostarczane w razie potrzeby i zwalniane wówczas, gdy nie są już potrzebne. To z kolei oznacza, że możliwe jest zapewnienie elastycznej skalowalności w celu zaspokojenia zapotrzebowania na wydajność nawet największych organów administracji publicznej – bez ponoszenia kosztów utrzymania nadmiarowych zasobów. Zwiększanie skali zazwyczaj nie wiąże się również z żadnymi (lub też wiąże się z marginalnymi) opóźnieniami, nie pociąga za sobą kosztów inwestycji kapitałowych w nowy sprzęt ani też skomplikowanego planowania zasobów lub zarządzania projektami i zmianami.

Czym jest system ZUCH i do czego jest wykorzystywany?

System ZUCH stanowi kluczowy element WIIP (Wspólnej Architektury Informacyjnej Państwa). Jest to platforma informatyczna, za pośrednictwem której organy administracji publicznej mogą wyszukiwać i pozyskiwać zweryfikowane pod względem bezpieczeństwa usługi chmurowe, zawarte w katalogu Rządowej Chmury Obliczeniowej (dalej: **RCHO**) lub katalogu Publicznej Chmury Obliczeniowej (dalej: **PCHO**). System ZUCH zapewnia również organom administracji publicznej dostęp do informacji oraz wsparcie przy zamawianiu usług chmurowych.

ZUCH to system Zapewniania Usług Chmurowych umożliwiający Kupującym zapoznanie się z szeroką gamą usług świadczonych w chmurze obliczeniowej i usług wsparcia związanych z chmurą obliczeniową oferowanych przez zweryfikowanych Sprzedających oraz zakup usług świadczonych w chmurze obliczeniowej, o zakresie i parametrach zdefiniowanych w Katalogu usług PCHO przez Operatora ZUCH, w postępowaniach zakupowych o wartości poniżej 130 000 PLN netto.

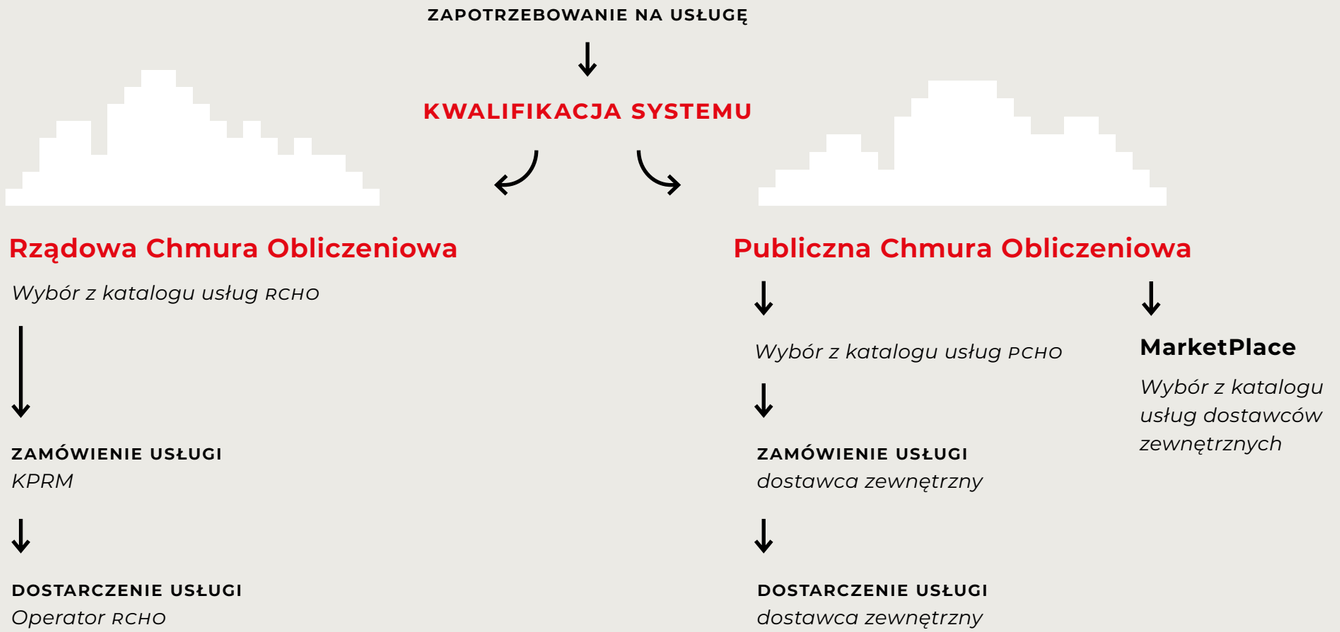
System ZUCH oferuje:

- wsparcie w zakresie kwalifikacji systemu informatycznego, umożliwiające określenie, czy dany system lub jego część może zostać umieszczona w PCHO lub RCHO, czy też należy go umieścić poza środowiskiem chmurowym;
- optymalizację procesu zamawiania usług przez podpisanie *ex ante* umów ramowych z wybranymi dostawcami (odbiorcy usług przystępują do postępowania na etapie realizacji umów wykonawczych);
- wsparcie procesu konfiguracji wstępnej i planowania usługi migracji, planowanych do kupienia przez odbiorców usług.

Korzyści Systemu ZUCH:

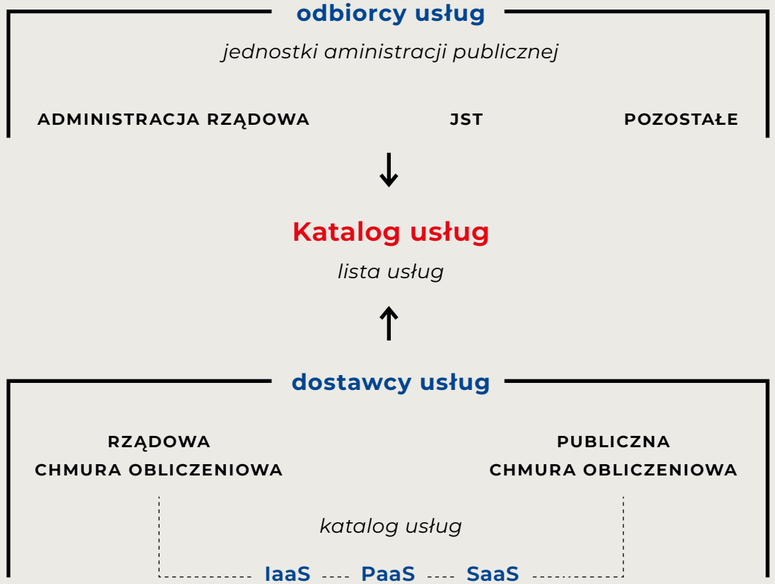
- ciągłe doskonalenie i rozwój katalogu usług RCHO lub PCHO;
- skrócenie czasu potrzebnego na wybór dostawcy usług i zawarcie umowy;
- ograniczenie kosztów oraz ryzyka związanego z procesem zakupu usług IT;
- zwiększenie transparentności procesów zakupowych i ograniczenie ryzyka nadużyć;
- ujednolicenie metod wykorzystania usług chmurowych;
- ujednolicenie standardów bezpieczeństwa dla dostaw usług chmury publicznej;
- stworzenie spójnej bazy danych w obszarze zamówień usług chmurowych dla administracji publicznej.

Katalog usług – proces



Rysunek 2. Proces pozyskiwania Usług Chmurowych w Systemie ZUCH.

System ZUCH



Rysunek 3. Katalogi usług w systemie ZUCH.

W ZUCH Katalogi Usług są dostępne w ramach kolejnych Wydań PCHO. W ramach Wydania 1 Kupujący uzyskują dostęp do otwartego Katalogu Usług, w ramach którego Sprzedający publikują Usługi na podstawie zdefiniowanego zakresu wymagań (szablonu), określonego przez Operatora ZUCH. **Więcej informacji można znaleźć w** Instrukcji dla Kupujących do Wydania 1.

W ramach Wydania 2 Kupujący uzyskują dostęp do zdefiniowanych przez Operatora ZUCH Katalogów Usług (Katalog PCHO RP, Katalog PCHO UE). **Szczegółowe informacje zawiera** Instrukcja dla Kupujących do Wydania 2.

Usługi chmurowe wymienione w katalogach PCHO są oferowane przez komercyjnych dostawców usług chmurowych, którzy zostali uprzednio zweryfikowani pod względem bezpieczeństwa. Rysunek 4 przedstawia zestawienie usług dostępnych w ramach katalogu PCHO.

- **Maszyna wirtualna**
- **Przestrzeń dyskowa**
- **Brama Sieciowa VPN**
- **Sieć prywatna**
- **Dodatkowe IP**
- **Równoważnik obciążeń** (ang. *Load Balancer*)
- **Środowisko kontenerowe** (ang. *Container enviroment*)
- **System Nazw Domen** (ang. *Domain Name System, DNS*)
- **Firewall Aplikacji Sieciowej** (ang. *WEB Application Firewall, WAF*)
- **Firewall**
- **Sieć Dostarczania Treści** (ang. *Content Delivery Network, CRN*)
- **System Zarządzania Kluczami** (ang. *Key Management System, KMS*)
- **System operacyjny**
- **Baza danych**

Rysunek 4. Usługi chmurowe w katalogu PCHO.

Szczegółowy opis usług jest opublikowany w Katalogu Usług do umowy ramowej.

Treść podpisanej umowy ramowej wraz z cennikiem producenta na czerwiec znajduje się w załącznikach do postępowania w zakładce „Centralne i wspólne" pod numerem postępowania 2023/08 na platformie zakupowej eB2B – Witamy na platformie zakupowej eB2B.

Rządowa Chmura Obliczeniowa (RCHO) to chmura wspólnotowa administracji publicznej. Infrastruktura jest przeznaczona do wyłącznego użytku przez określoną grupę organizacji mających wspólne założenia (m.in. misję, wymagania bezpieczeństwa, politykę, zgodność z regulacjami), może być własnością jednej lub więcej organizacji wchodzącej w skład grupy, strony trzeciej lub ich kombinacji bądź może być przez nie zarządzana oraz obsługiwana i jest zainstalowana w siedzibie organizacji lub poza nią.

Katalog RCHO jest wykorzystywany przede wszystkim do świadczenia usług IaaS, PaaS, DRaaS i SaaS, ale w przyszłości zostanie także rozszerzony o inne usługi chmurowe (takie jak XaaS). Wyznaczonym dostawcą usług chmurowych wymienionych w katalogu RCHO jest Minister Cyfryzacji.

Każda z usług wymienionych w katalogu RCHO jest indywidualnie oceniana pod kątem zgodności architektonicznej, integralności danych oraz bezpieczeństwa.

System ZUCH, łącznie z usługami wymienionymi w katalogach RCHO i PCHO, jest dostępny dla wymienionych poniżej kategorii podmiotów:

- podmioty sektora finansów publicznych, o których mowa w art. 9 ust. 1–13 ustawy z 27 sierpnia 2009 r. o finansach publicznych (Dz.U. z 2019 r. poz. 869);
- inne państwowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, banków i spółek prawa handlowego;
- nieposiadające osobowości prawnej państwowe jednostki organizacyjne inne niż określone w ustawie z 27 sierpnia 2009 o finansach publicznych, np. Państwowe Gospodarstwo Leśne „Lasy Państwowe".

Więcej informacji na temat systemu ZUCH znajduje się na stronie: chmura.gov.pl.

Cyberbezpieczeństwo w rozwiązaniach chmurowych – podzielona odpowiedzialność

Istotnym zagadnieniem w zakresie rozwiązań chmurowych jest zwrócenie uwagi na „podzieloną odpowiedzialność" – istotny element budowania bezpieczeństwa.

Podzielona odpowiedzialność (ang. *Shared Responsibility Model*) to model bezpieczeństwa funkcjonowania chmury obliczeniowej, opisujący ustalenia dotyczące odpowiedzialności **Dostawcy** i **Odbiorcy Usług** „Bezpieczeństwo chmury" w zakresie infrastruktury teleinformatycznej, przetwarzania danych oraz usług chmurowych.

Standard NIST[4] określa podział odpowiedzialności ze względu na model dostarczania usługi mianem stosu SPI (Software, Platform, Infrastructure as a service). Model ten w uproszczony sposób pozwala zilustrować, jakie elementy usługi chmurowej są dostarczane przez Dostawcę Usług, a jakie są instalowane przez Odbiorcę Usług. Ma to istotne znaczenie w zrozumieniu, jakie ryzyka są związane z poszczególnymi modelami dostarczania usług, oraz pomaga określić, kto jest odpowiedzialny za minimalizację tych ryzyk i zastosowanie odpowiednich zabezpieczeń.

Odbiorca Usług musi zdawać sobie sprawę z faktu, że migracja do chmury czy też zakup usług chmurowych nie zwalnia go z obowiązku zapewnienia bezpieczeństwa przetwarzanych danych czy uruchamianych w chmurze systemów. Korzystając z usług chmurowych, Odbiorca Usług powinien zapoznać się ze środkami bezpieczeństwa oferowanymi przez Dostawcę w ramach oferowanej usługi. Tutaj należy rozpatrzeć dwa zasadnicze zagadnienia:

- dana usługa posiada odpowiednie podstawowe środki bezpieczeństwa, ale Odbiorca Usług musi je włączyć i skonfigurować;
- środki bezpieczeństwa oferowane przez daną usługę w ocenie Odbiorcy są niewystarczające do zapewnienia bezpieczeństwa przetwarzania i przechowywania danych. W takim przypadku konieczne będzie zaimplementowanie dodatkowych usług bezpieczeństwa oferowanych przez Dostawcę Usług.

4 Narodowe Standardy Cyberbezpieczeństwa w serwisie gov.pl.

8.3 Wykorzystanie platformy samorząd.gov.pl

Projekt „Serwis samorzad.gov.pl" został stworzony w ramach projektu „Portal RP", którego organizatorem i realizatorem jest Ministerstwo Cyfryzacji. Głównym celem projektu jest przeniesienie kolejnych serwisów internetowych i stron Biuletynu Informacji Publicznej (BIP) jednostek sektora finansów publicznych na Portal RP.

Beneficjentami i odbiorcami projektu są wszystkie JST oraz jednostki podległe.

Główne założenia projektu to spójny rozwój i poprawa użyteczności serwisów publicznych w Polsce.

Migracja JST na serwis samorzad.gov.pl już trwa i przebiega zgodnie z harmonogramem.

Przystąpienie do samorzad.gov.pl może przynieść wiele korzyści dla JST. Dzięki uczestnictwu w projekcie „Cyberbezpieczny Samorząd” JST:

- będą mogły sprawnie i wygodnie zarządzać treścią witryn;
- zapłacą mniej za obsługę strony internetowej i BIP (będą korzystać z zasobów Ministerstwa Cyfryzacji);
- zwiększą bezpieczeństwo, funkcjonalność, wydajność i zapewnią zgodność z nowym prawem dotyczącym prowadzenia witryn informacyjnych;
- będą współtworzyć spójny, jednolity, przyjazny i intuicyjny portal, zaprojektowany zgodnie z potrzebami i oczekiwaniami użytkowników (m.in. z zasadą *mobile first*);
- skorzystają z gotowych rozwiązań – zgodnych z zasadami dostępności cyfrowej i dostosowywanych do potrzeb i wytycznych;
- będą korzystać z elastycznego i rozbudowanego panelu dla redaktorów;
- otrzymają wsparcie techniczne i redakcyjne, w tym dostęp do szkoleń z obsługi panelu redakcyjnego GovPress (redakcja.samorzad.gov.pl), dostępności cyfrowej i prostego języka.

Obecnie na samorzad.gov.pl znajduje się już ponad 200 JST i jednostek podległych, a kolejnych 90 wyraziło zainteresowanie migracją.

W celu zgłoszenia do projektu należy wypełnić formularz zgłoszeniowy do samorzad.gov.pl.

8.4 —— Szkolenia z zakresu cyberbezpieczeństwa

Kompetencje z zakresu cyberbezpieczeństwa mają kluczowe znaczenie dla sprawnego funkcjonowania nowoczesnego państwa. Systematyczne podnoszenie kwalifikacji kadr podmiotów krajowego systemu cyberbezpieczeństwa, w tym także jednostek samorządu terytorialnego i jednostek im podległych, to konieczność i jeden z priorytetów w dążeniu do bezpieczeństwa cyfrowego.

8.4.1. Szkolenia indywidualne dla przedstawicieli jednostek samorządu terytorialnego

Wychodząc naprzeciw potrzebom podnoszenia kompetencji z obszaru cyberbezpieczeństwa wśród kadr administracji publicznej, od 2021 r. prowadzone są szkolenia adresowane do najważniejszych osób w państwie (parlamentarzyści, kadra kierownicza administracji centralnej i samorządowej). Szkolenia te są realizowane w trybie indywidualnym, a ich terminy i zakres merytoryczny dostosowywane są do konkretnych potrzeb osoby szkolonej.

Bezpłatne, indywidualne szkolenia z zakresu cyberbezpieczeństwa dla przedstawicieli jednostek samorządu terytorialnego wszystkich szczebli są prowadzone przez **Państwowy Instytut Badawczy NASK** w ramach zadania zleconego przez Ministra Cyfryzacji pn. „Działania prewencyjno-edukacyjne z zakresu cyberbezpieczeństwa w 2023 roku – podnoszenie odporności Rzeczypospolitej Polskiej na zagrożenia w przestrzeni cyfrowej".

Szkolenia kierowane są w szczególności do: marszałków i wicemarszałków oraz członków zarządu województw, starostów, wicestarostów, wójtów, burmistrzów oraz prezydentów miast, ich zastępców, sekretarzy, jak również głównych księgowych, skarbników i kierowników urzędów stanu cywilnego. Istnieje możliwość zgłoszenia również dodatkowych osób, które mają dostęp do wrażliwych informacji oraz pełnią znaczące role z punktu widzenia cyberbezpieczeństwa danej jednostki.

Szkolenia prowadzone są **stacjonarnie w siedzibie zgłaszanej jednostki samorządu terytorialnego.**

Uczestnicy **szkolenia otrzymują narzędzia do uwierzytelniania dwuskładnikowego na czas pełnienia funkcji lub zajmowania stanowiska w jednostce samorządu terytorialnego.**

Zgłoszenia można przesyłać na adres mailowy: cyberszkolenia@nask.pl. Terminy szkoleń zostaną ustalone indywidualnie ze zgłoszonymi uczestnikami.

8.4.2. Szkolenia online dla podmiotów krajowego systemu cyberbezpieczeństwa

Od 2020 r. prowadzone są szkolenia online dla podmiotów krajowego systemu cyberbezpieczeństwa. Prowadzą je eksperci oraz praktycy, którzy na co dzień zajmują się kwestiami cyberbezpieczeństwa, związani z partnerami technologicznymi Programu Współpracy w Cyberbezpieczeństwie (PWCyber) oraz NASK-PIB.

Szkolenia kierowane są do każdej grupy użytkowników systemów teleinformacyjnych o różnym poziomie zaawansowania.

Zostały podzielone na trzy kategorie:

SZKOLENIA 100 — **cyberhigiena dla każdego**

podstawowe porady i najlepsze praktyki z zakresu cyberbezpieczeństwa dla wszystkich pracowników;

SZKOLENIA 200 — **dla kadry zarządzającej, pracowników działów IT**

podstawy prawne krajowego systemu cyberbezpieczeństwa, obowiązki podmiotów wynikające z ustawy, procedury zgłaszania incydentów, najczęstsze cyberzagrożenia i sposoby ochrony;

SZKOLENIA 300 — **warsztaty dla specjalistów IT, programistów, osób zarządzających cyberbezpieczeństwem w podmiotach krajowego systemu cyberbezpieczeństwa**

prezentacje projektów wspierających cyberbezpieczeństwo w organizacji, analizy rodzajów cyberataków, reagowanie na incydenty, zgłaszanie incydentów, profilaktyka cyberbezpieczeństwa w organizacji, szkolenia specjalistyczne dotyczące zastosowania konkretnych rozwiązań prowadzone przez partnerów technologicznych.

Celem szkoleń jest podniesienie świadomości kadr jednostek krajowego systemu cyberbezpieczeństwa o cyberbezpieczeństwie, obowiązkach wynikających z Ustawy o krajowym systemie cyberbezpieczeństwa oraz stosowanych standardach i dobrych praktykach w organizacjach w celu zapewniania cyberbezpieczeństwa w organizacji. Szkolenia pozwalają również na podniesienie umiejętności praktycznych związanych z wykorzystywaniem narzędzi informatycznych oraz radzeniem sobie w sytuacjach kryzysowych.

Szczegółowe informacje o bieżącej ofercie szkoleniowej dostępne są w bazie wiedzy o cyberbezpieczeństwie na portalu gov.pl.

8.5 Elektroniczne zarządzanie dokumentacją w administracji publicznej

Czym jest EZD?

Wdrożenie systemu klasy EZD (elektroniczne zarządzanie dokumentacją) umożliwia kompleksowe dokumentowanie przebiegu załatwiania spraw w postaci elektronicznej oraz kompletowanie i archiwizację akt, zgodnie z obowiązującymi przepisami prawa, zwłaszcza w zakresie norm kancelaryjnych i archiwalnych. Dodatkowo znacząco usprawnia i przyspiesza wymianę korespondencji między podmiotami publicznymi oraz komunikację z obywatelami.

Dzięki swojej charakterystyce system klasy EZD przyczynia się do podniesienia poziomu cyberbezpieczeństwa w instytucjach publicznych. Wykorzystanie nowoczesnego systemu teleinformatycznego do zarządzania dokumentacją i informacją gwarantuje poufność, integralność, dostępność i autentyczność przechowywanych oraz przetwarzanych danych. Wrażliwe informacje są odpowiednio chronione, a ryzyko wystąpienia zagrożeń i naruszeń bezpieczeństwa zostaje znacząco zredukowane.

Bezpłatne systemy EZD dla administracji publicznej

Podmioty publiczne mają możliwość skorzystania z dwóch bezpłatnych systemów do elektronicznego zarządzania dokumentacją: EZD RP i EZD PUW. Pierwszy z nich to stworzony w NASK-PIB, w partnerstwie z Wojewodą Podlaskim i pod nadzorem Ministerstwa Cyfryzacji, jednolity system do elektronicznego zarządzania dokumentacją przeznaczony dla polskiej administracji. Co ważne, EZD RP udostępnia dokumentację z wykorzystaniem przeglądarki WWW przy zachowaniu rygorów wynikających z rozporządzenia ogólnego o ochronie danych osobowych i wewnętrznych polityk bezpieczeństwa informacji. EZD RP ma rozbudowany system uprawnień, który zapewnia, że pracownik otrzymuje wgląd wyłącznie do dokumentacji wynikającej ze specyfiki stanowiska pracy oraz swojego zakresu obowiązków.

Z kolei EZD PUW to rozwijany od 2011 r. system do elektronicznego zarządzania dokumentacją autorstwa Podlaskiego Urzędu Wojewódzkiego w Białymstoku. Od wielu lat sprawdza się jako podstawowe narzędzie pracy w centralnych i wojewódzkich jednostkach administracji rządowej, samorządach oraz innych podmiotach realizujących zadania publiczne, takich jak sądy, szkolnictwo wyższe, instytuty i archiwa.

Oba systemy umożliwiają integrację z innymi aplikacjami dzięki wbudowanym metodom API.

Wdrożenie w modelu *on-premise*

Przed podjęciem decyzji dotyczącej wdrożenia systemu klasy EZD każda jednostka powinna dokładnie ocenić swoje umiejętności, zasoby i wymagania dotyczące cyberbezpieczeństwa. Po przeprowadzeniu takiej analizy możliwe jest wskazanie optymalnego modelu wdrożeniowego: *on-premise* lub *Software as a Service (SaaS)*.

Wdrożenie w środowisku chmurowym

W modelu SaaS podmiot korzysta z infrastruktury dostarczonej przez zewnętrznego dostawcę. W tym przypadku odpowiedzialność za bezpieczeństwo jest współdzielona. Co najważniejsze, dostawca odpowiada za implementację i utrzymanie całego stosu technologicznego (w tym za backup), natomiast rola podmiotu sprowadza się do odpowiedniego przygotowania procedur organizacyjnych, zarządzania dostępem do systemu, monitorowania działań użytkowników i stosowania dobrych praktyk związanych z bezpieczeństwem.

Przykładem kompleksowo przygotowanego systemu klasy EZD, który został dostosowany do wdrażania w środowisku chmurowym, jest EZD RP. Usługę nazwaną SaaS EZD RP samorządom dostarczają zewnętrzni dostawcy. Może być ona świadczona zarówno przez organizację, która jest jednocześnie dostawcą aplikacji i infrastruktury chmurowej, jak i przez dostawcę aplikacji, który infrastrukturę chmurową wynajmuje od innych podmiotów.

Wskazane jest, aby każdy dostawca wykazał, że spełnia minimalne wymagania określone normami ISO i posiada odpowiednie certyfikaty w zakresie:

- zarządzania bezpieczeństwem informacji;
- zarządzania ciągłością działania lub posiadania systemu do zapewnienia wysokiej dostępności usługi;
- zagadnień związanych z tematyką centrów przetwarzania danych pod kątem infrastruktury i wyposażenia centrów przetwarzania w zakresie systemów zapewniających odpowiednie warunki otoczenia.

Na wysoki poziom bezpieczeństwa usługi SaaS EZD RP wpływa również to, że dostęp do niej wymaga zestawienia bezpiecznego połączenia z wykorzystaniem wirtualnych sieci prywatnych VPN (Virtual Private Network) i zbioru protokołów IPSec (Internet Protocol Security) – służących do implementacji bezpiecznych połączeń i wymiany kluczy szyfrowania pomiędzy komputerami.

NASK-PIB jako dostawca usługi SaaS EZD RP dla podmiotów administracji rządowej przygotował szczegółowe rekomendacje w zakresie bezpieczeństwa. Mogą być one z powodzeniem stosowane przez samorządy.

Dobre praktyki oraz funkcje Zapewniające bezpieczeństwo

Podczas wdrażania systemu EZD w jednostce istotne jest powołanie zespołu wdrożeniowego, w którego skład powinni wchodzić pracownicy merytoryczni jednostki, odpowiedzialni za wprowadzenie nowego sposobu dokumentowania przebiegu załatwiania praw przy użyciu systemu teleinformatycznego.

Do dobrych praktyk należy dokonanie przeglądu i określenie oczekiwań wobec własnych zabezpieczeń w czterech obszarach:

- **zabezpieczenia organizacyjne**
- **zabezpieczenia związane z pracownikiem**
- **zabezpieczenia fizyczne**
- **zabezpieczenia technologiczne**

Warto zaznaczyć, że w systemach, dla których wsparcie wdrożeniowe świadczy NASK-PIB, zaimplementowano wiele funkcji, które mają na celu zwiększenie poziomu bezpieczeństwa. Przykładowo administrator ma możliwość przypisywania użytkownikom konkretnych ról i uprawnień, co pozwala nie tylko skonfigurować aplikację w sposób odpowiadający strukturze organizacyjnej jednostki, ale też udzielić użytkownikowi dostępu tylko do tych funkcji, dokumentów i danych, które są mu niezbędne do wykonywania swoich zadań. To ogranicza ryzyko nieautoryzowanego dostępu do danych oraz nieuprawnionych czynności.

Szczegółowe informacje dotyczące zasad wdrażania EZD RP można znaleźć na Portalu EZD RP w zakładce dotyczącej wdrożeń. Natomiast procedury wdrażania EZD PUW zostały opisane na stronie: ezd.gov.pl/www/ezd/wspolpraca.

8.6 Podłączenie do systemu S46

1 stycznia 2021 r. Minister Cyfryzacji uruchomił system, o którym mowa w art. 46 ust. 1 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, wspierający:

- współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa,
- generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa,
- zgłaszanie i obsługę incydentów,
- szacowanie ryzyka na poziomie krajowym,
- ostrzeganie o zagrożeniach cyberbezpieczeństwa.

System przeznaczony jest dla podmiotów objętych Ustawą o krajowym systemie cyberbezpieczeństwa, które podpiszą porozumienie z Ministerstwem Cyfryzacji. Minister Cyfryzacji upoważnił NASK-PIB do zawierania w jego imieniu porozumień w sprawie podłączenia do Systemu S46.

System S46 zapewnia podłączonym podmiotom dostęp do:

- aktualnej informacji o ryzyku dla świadczonych przez dany podmiot usług;
- informacji o podatnościach dla danego sektora;
- rekomendacji, których wdrożenie zwiększa bezpieczeństwo świadczenia usług;
- sugerowanych rozwiązań w postaci analiz technicznych;
- ostrzeżeń wydawanych przez CSIRT poziomu krajowego, a także możliwość:
  - historycznej analizy stanu cyberbezpieczeństwa świadczonych usług (raporty);
  - zgłaszania incydentów do CSIRT poziomu krajowego i uzyskania wsparcia w ich obsłudze;
  - zgłaszania podatności i ryzyka.

S46 jest systemem dwukierunkowej bezpiecznej wymiany informacji, którego wyłącznym właścicielem jest Minister Cyfryzacji. System Brzegowy Uczestnika (SBU) nie zbiera automatycznie żadnych danych samodzielnie i nie przeprowadza żadnych analiz czy badań.

Wprowadzanie danych i dostęp do Systemu S46 są realizowane przez portal użytkownika z dedykowanej stacji roboczej uprawnionej do dostępu do S46, poprzez podłączenie jej do SBU. Stacja robocza Operatora Uczestnika może być podłączona do SBU albo bezpośrednio, albo przez sieć podmiotu podłączanego do S46 (Uczestnika).

System Brzegowy Uczestnika to urządzenie montowane w szafie serwerowej Uczestnika, zajmujące wysokość 1U. SBU nie potrzebuje przydzielania mu żadnych uprawnień w infrastrukturze Podmiotu (Uczestnika Systemu S46), który podpisał porozumienie z Ministerstwem Cyfryzacji. SBU jest końcówką Systemu S46, którą zarządza NASK-PIB.

Wszelkie informacje wprowadza do S46, poprzez SBU, osoba upoważniona po stronie Uczestnika (Operator Uczestnika).

Rysunek 5. Schemat podłączenia do systemu S46.

Operatorami sieci S46 (sieć MPLS L3VPN_A i B) są NASK SA i Exatel. Łącza dostępowe pomiędzy lokalizacją SBU a węzłami tych sieci, które zamawia i które opłaca Uczestnik, mogą pochodzić od dowolnego operatora.

Po stronie Uczestnika występują koszty zestawienia dwóch połączeń dostępowych pomiędzy serwerownią z zainstalowanym SBU a najbliższym/najdogodniejszym węzłem sieci S46 (L3VPN_A i B) oraz koszty ich utrzymania.

Ponadto po stronie Uczestnika są koszty związane z utrzymaniem SBU w serwerowni (energia, klimatyzacja, miejsce, ochrona fizyczna) oraz koszty osobowe związane z użytkowaniem S46.

NASK-PIB jest koordynatorem i realizatorem działań w procesie podłączenia zainteresowanego Podmiotu i obsługi Podmiotu podłączonego.

8.7 Fundusz Wsparcia Jednostek Samorządu Terytorialnego NASK

Odpowiadając na bieżące wyzwania w zakresie poszukiwania środków na zwiększenie poziomu cyberbezpieczeństwa, ustawodawca przewidział – w Ustawie z dnia 1 grudnia 2022 r. o szczególnych rozwiązaniach służących realizacji ustawy budżetowej na rok 2023 r. – możliwość utworzenia przez instytut badawczy nadzorowany przez ministra właściwego do spraw informatyzacji Funduszu wsparcia jednostek samorządu terytorialnego. Taki Fundusz został utworzony przez NASK-PIB.

Fundusz ma charakter incydentalny – jako powołany na podstawie ustawy okołobudżetowej. Wsparcie z Funduszu może być udzielane i musi być wykorzystane nie później niż do dnia 31 grudnia 2023 r. Środki Funduszu przeznacza się, na podstawie umowy zawartej z NASK-PIB, na udzielanie wsparcia jednostkom samorządu terytorialnego – na realizację zadań z zakresu cyberbezpieczeństwa.

Fundusz nie jest typowym funduszem grantowym, a formą interwencyjnej pomocy jednostce samorządu terytorialnego dotkniętej incydentem szczególnie złożonym lub brzemiennym w skutki dla obywateli. Podstawowym warunkiem uzyskania wsparcia z Funduszu jest wystąpienie w danej JST lub jej jednostce organizacyjnej tego rodzaju incydentu w rozumieniu uoKSC i zgłoszenie go do właściwego CSIRT. Jeśli po przeprowadzonej analizie eksperci CSIRT NASK wydadzą stosowne rekomendacje, zgłaszającej jednostce samorządu terytorialnego może zostać udzielone wsparcie z przeznaczeniem wyłącznie na mitygację skutków zaistniałego incydentu i wzmocnienie odporności oraz zdolności do skutecznego zapobiegania i reagowania na kolejne incydenty. Decyzja w sprawie udzielenia bądź nieudzielenia wsparcia, jego formy lub kwoty nie podlega zaskarżeniu.

Wsparcie przyznawane jest w ramach wolnych środków Funduszu, w kolejności otrzymanych wniosków – w formie dotacji lub nieodpłatnego użyczenia urządzeń czy oprogramowania. Wsparcie może być wykorzystane wyłącznie na realizację zadań z zakresu cyberbezpieczeństwa, a jego wykorzystanie podlega kontroli NASK-PIB.

NASK