Wdrażanie wymagań NIS2/ UoKSC w oparciu o wytyczne regulacji europejskich

Wykładowca: Artur Cieślik
MBA, IRCA lead auditor ISO/IEC 27001
IRCA lead auditor ISO/IEC 22301
ISACA Certified Information Systems Auditor (CISA)
redaktor naczelny „IT Professional”
artur.cieslik@politykabezpieczenstwa.com.pl

Artur Cieślik
politykabezpieczenstwa.com.pl

- **Założyciel i główny ekspert ACSEC Sp. z o.o.:**
- Audytor wiodący normy ISO/IEC 27001 IRCA Certified Lead Auditor (nr w rejestrze: 6035034).
- Audytor wiodący normy ISO/IEC 22301 uzyskany zgodnie z IRCA.
- Certified Information Systems Auditor (CISA)
- Członek SABI – Stowarzyszenia Inspektorów Ochrony Danych.
- Członek IIA – Instytutu Audytorów Wewnętrznych IIA Polska
- Redaktor naczelny miesięcznika „IT Professional”.
- Członek rady programowej „ABI Expert”.
- Szkolenia i wykłady: Akademia Leona Koźmińskiego, Politechnika Wrocławska, Uniwersytet Ekonomiczny we Wrocławiu, Uniwersytet im. Kardynała Wyszyńskiego „IT Professional Academy” „Informacja Publiczna”, „Forbes Academy”, „IT w Administracji”.

Podstawy prawne wymagań

Dyrektywa na rzecz wysokiego poziomu cyberbezpieczeństwa (NIS2)

Cel:

Zwiększenie ogólnego poziomu cyberbezpieczeństwa w Unii Europejskiej.

Obowiązki:

Nakłada obowiązki na państwa członkowskie i tym samym podmioty działające w sektorach krytycznych.

Wymagania:

Państwa członkowskie muszą zapewnić, że podmioty kluczowe wdrażają odpowiednie środki techniczne, operacyjne i organizacyjne w celu zarządzania ryzykiem cyberbezpieczeństwa.

Ustawa o Krajowym Systemie Cyberbezpieczeństwa (UoKSC)

Cel:

Implementacja dyrektywy NIS2 w Polsce i zapewnienie wysokiego poziomu bezpieczeństwa cyberprzestrzeni RP.

Obowiązki:

Podmioty kluczowe i ważne muszą wdrażać zabezpieczenia, szacować ryzyko oraz zgłaszać poważne incydenty do odpowiednich zespołów CSIRT.

Wymagania:

Podmioty muszą wyznaczyć osoby odpowiedzialne za cyberbezpieczeństwo, obsługę incydentów oraz udostępnianie wiedzy na temat cyberbezpieczeństwa.

Należy też wdrożyć szereg rozwiązań organizacyjnych i technicznych.

Obowiązki wynikające z NIS2

Dyrektywa **NIS2** stawia szereg szczegółowych wymogów, które z założenia mają zbudować zunifikowany system cyberbezpieczeństwa, zapewniający właściwy poziom zabezpieczenia podmiotów, jak również wymiany informacji.

1

Zarządzanie ryzykiem w cyberbezpieczeństwie

- Wdrożenie odpowiednich środków technicznych i organizacyjnych.
- Przeprowadzanie regularnych ocen ryzyka i audytów bezpieczeństwa.
- Prowadzenie regularnych szkolenia dla pracowników w zakresie cyberbezpieczeństwa.

2

Raportowanie incydentów

- Zgłaszanie poważnych incydentów cybernetycznych do odpowiednich organów: do **24 godzin**.
- Dostarczanie szczegółowych informacji na temat incydentu: do **72 godzin**.
- Przedstawienie finalnego raportu z incydentu: do miesiąca.

3

Współpraca z organami nadzoru

- Udzielanie wsparcia i informacji na żądanie organów nadzorczych, w tym sektorowych CSIRT.
- Przestrzeganie zaleceń i nakazów wydanych przez organy nadzorcze, zwłaszcza w zakresie listy HRV (High Risk Vendors), wskazujących zakazanych dostawców technologii.

Normy ISO dotyczące zarządzania ryzykiem cyberbezpieczeństwa

Norma	Cel
ISO/IEC 27001:2022	Podstawa wdrażania Systemu Zarządzania Bezpieczeństwem Informacji (ISMS)
ISO/IEC 27002:2022	Cele, wytyczne i praktyki kontroli bezpieczeństwa zgodne z normą 27001
ISO/IEC 27005:2022	Strukturalne podejście do oceny ryzyka i jego postępowania
ISO/IEC 27004:2016	Metryki i monitorowanie skuteczności ISMS

Obsługa podatności i incydentów

Norma	Cel
ISO/IEC 29147:2018	Ramy odpowiedzialnego ujawniania podatności
ISO/IEC 30111:2020	Proces analizy, triage'u i łagodzenia podatności
ISO/IEC 27035-1:2023	Zarządzanie cyklem życia incydentów bezpieczeństwa

Łańcuch dostaw i usługi IT

Norma	Cel
ISO/IEC 27036-1:2021	Zasady zabezpieczania interakcji z dostawcami i stronami trzecimi
ISO/IEC 27036-2:2022	Wymagania dotyczące zarządzania ryzykiem cybernetycznym w relacjach z dostawcami
ISO/IEC 20000-1:2018	Najlepsze praktyki zarządzania bezpiecznymi usługami IT zgodnie z normami IS

Ciągłość działania

Norma	Cel
ISO 22301:2019	Wymagania dotyczące wdrażania Systemu Zarządzania Ciągłością Działania (BCMS)
ISO 22313:2020	Wytyczne do stosowania kontroli ISO 22301
ISO/TS 22317:2021	Metodyka przeprowadzania Analizy Wpływu na Działalność (BIA)

Obowiązki podmiotu KSC

Zgłoszenie do wykazu

Podmiot musi dokonać wpisu do rejestru **podmiotów kluczowych**.

Termin: 3 miesiące
(od wejścia ustawy)

Podłączenie do systemu S46-react

Podmiot musi spełnić techniczne wymagania podłączenia do S46, służącego do wymiany informacji.

Termin: 6 miesięcy
(od wejścia ustawy)

Wdrożenie zasad bezpieczeństwa

Podmiot musi wdrożyć wszystkie wymagania, w tym powołać punkt kontaktowy.

Termin: 6 miesięcy
(od wejścia ustawy)

Szkolenie pracowników

Podmiot musi przeszkolić wszystkich pracowników, w tym kierownictwo, celem podniesienia poziomu cyberhigieny.

Termin: 6 miesięcy
(od wejścia ustawy)

Przeprowadzenie audytu

Podmiot musi przeprowadzić niezależny audyt spełnienia wszystkich wymogów NIS2/ UoKSC.

Termin: do 24 miesięcy
(od wejścia ustawy)

Niedopełnienie obowiązków

Dla podmiotów kluczowych kary pieniężne wynoszą:

od **20 000 PLN** do **10 000 000 EUR** lub **2%** rocznego, światowego obrotu

Podobnie restrykcyjne wymogi i kary wynikające z DORA (dyrektywa o odporności cyfrowej dla sektora bankowego), jak również zaostrzenie kar wynikających z łamania RODO, wskazują na wyraźny trend stawiania organizacjom coraz większych wymagań. Spodziewać się można twardego egzekwowania wymagań nakładanych przez NIS2.

Pozostałe sankcje

Zawieszenie, ograniczenie lub cofnięcie koncesji

Obowiązujące do czasu podjęcia działań niezbędnych do uchylenia naruszeń lub do czasu osiągnięcia zgodności.

Wykreślenie podmiotu

Z katalogu działalności regulowanej.

Cofnięcie zezwoleń

Obowiązujące do czasu podjęcia działań niezbędnych do uchylenia naruszeń lub do czasu osiągnięcia zgodności.

Nałożenie kary okresowej

Celem przymuszenia do wykonania obowiązków, nałożona może zostać kara w wysokości od **500 zł** do **100 000 zł** za każdy dzień opóźnienia.

Jeżeli PODMIOT naruszy UoKSC, powodując:

1. Bezpośrednie i poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi

2. Zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług

to organ właściwy do spraw cyberbezpieczeństwa może nałożyć karę

Czym jest norma ISO/IEC 27001?

NORMA ISO/IEC 27001:2022

Definicja:

Międzynarodowa norma standaryzująca systemy zarządzania bezpieczeństwem informacji (SZBI), część większego zespołu wzajemnie kompatybilnych norm.

Cel:

Zapewnienie ochrony informacji poprzez wdrożenie odpowiednich środków technicznych, organizacyjnych i proceduralnych.

Wymagania:

Norma określa wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia SZBI, w tym zarządzania ryzykiem związanym z bezpieczeństwem informacji.

System Zarządzania Bezpieczeństwem Informacji (SZBI)

Definicja:

SZBI to zbiór polityk, procedur, wytycznych oraz zasobów zarządzanych wspólnie przez organizację w celu ochrony jej zasobów informacyjnych.

Cel:

Zapewnienie poufności, integralności i dostępności informacji, minimalizowanie ryzyka utraty danych oraz zapewnienie ciągłości działania organizacji.

Wymagania:

SZBI obejmuje zarządzanie ryzykiem, kontrolę dostępu, zarządzanie incydentami, audyty wewnętrzne oraz ciągłe doskonalenie procesów bezpieczeństwa.

ISO/IEC 27001 — najważniejsze obowiązki

1

Polityka bezpieczeństwa informacji

Opracowanie i wdrożenie polityki bezpieczeństwa, która określa cele oraz zasady ochrony informacji.

2

Zarządzanie ryzykiem

Identyfikacja, analiza i ocena ryzyk związanych z bezpieczeństwem informacji oraz wdrożenie odpowiednich środków zaradczych.

3

Kontrola dostępu

Ustanowienie procedur i mechanizmów kontroli dostępu do informacji, aby zapewnić, że tylko uprawnione osoby mają dostęp do danych.

4

Zarządzanie incydentami

Opracowanie procedur identyfikacji, zgłaszania i reagowania na incydenty związane z bezpieczeństwem informacji.

5

Audyty wewnętrzne

Regularne przeprowadzanie audytów wewnętrznych w celu oceny zgodności z normą ISO 27001 i identyfikacji obszarów do poprawy.

6

Ciągłe doskonalenie

Monitorowanie, przegląd i doskonalenie procesów bezpieczeństwa informacji, aby zapewnić ich skuteczność i adekwatność w zmieniających się warunkach.

7

Szkolenia i podnoszenie świadomości

Regularne szkolenia pracowników oraz podnoszenie ich świadomości na temat zagrożeń i procedur związanych z bezpieczeństwem informacji.

8

Zarządzanie zasobami

Zapewnienie odpowiednich zasobów (ludzkich, technicznych, finansowych) do wdrożenia i utrzymania SZBI.

Czym jest norma ISO/IEC 22301?

NORMA
ISO 22301:2019

Definicja:

Międzynarodowa norma ustanawiająca System Zarządzania Ciągłością Działania (SZCD), która uzupełnia normę ISO27001 w przedmiotowym obszarze.

Cel:

Zapewnienie ciągłości działania organizacji w sytuacjach kryzysowych i awaryjnych.

Wymagania:

Norma określa wymagania dotyczące identyfikacja kluczowych ryzyk, opracowania planów ciągłości działania wraz z ich regularnym testowaniem i aktualizacją. Określa także zaangażowanie najwyższego kierownictwa, co pomaga spełnić wymogi NIS2.

System Zarządzania Ciągłością Działania (SZCD)

Definicja:

Zbiór działań i procedur mających na celu zapewnienie, że organizacja może kontynuować swoje kluczowe funkcje w przypadku zakłóceń.

Cel:

Osiągnięcie gotowości na sytuacje kryzysowe, minimalizacja wpływu zakłóceń na działalność organizacji, szybkie przywrócenie normalnego funkcjonowania.

Wymagania:

SZCD obejmuje szczegóły zarządzania ryzykiem, planowanie ciągłości działania, regularne testowanie i ćwiczenia, przeprowadzanie audytów wewnętrznych, jak również ciągłe doskonalenie.

Korzyści z ISO w świetle NIS2/UoKSC

1

ISO27001 pozwala osiągnąć większość wymagań UoKSC

NIS2 w znaczącej części pokrywa się z wymaganiami normy ISO27001. Dlatego wdrożenie SZBI jest jednym z najlepszych sposobów na osiągnięcie zgodności z UoKSC. Takie podejście:

— opiera się na sprawdzonych metodach,
— tworzy dobrze ustrukturyzowany, skalowalny i łatwy w zarządzaniu system,
— przez wykorzystanie istniejących rozwiązań, jest korzystne ekonomicznie.

2

Normy ISO zapewniają elastyczność wobec przyszłych wymagań

Obserwując wysiłki legislacyjne UE w różnych sektorach działalności, należy spodziewać się dalszego zaostrzania wymogów dotyczących cyberbezpieczeństwa.

Tworzenie systemu zarządzania bezpieczeństwem w oparciu o normy ISO pozwali na szybkie dostosowanie się do przyszłych regulacji — przez wzajemną kompatybilność oraz normy wyspecjalizowane w węższym obszarze, jak np. ciągłość działania czy bezpieczeństwo usług chmurowych.

Sposób implementowania NIS2 — jeszcze przed nowelizacją UoKSC

W związku z trwającymi pracami nowelizacyjnymi nad UoKSC, jak również krótkim terminem na uzyskanie zgodności po wejściu w życie ustawy, w implementacji wymagań NIS2 warto kierować się projektem wytycznych ENISA — Europejskiej Agencji ds. Cyberbezpieczeństwa oraz kontynuować doskonalenie według normy ISO/IEC 27001:2022.

ENISA odwołuje się do szeroko stosowanych praktyk

Projekt wytycznych w dużej części pokrywał się z praktykami przyjętymi w międzynarodowych normach, takich jako ISO/IEC 27001:2022.

ENISA wskazywała m.in. na obowiązek określania strategii, ról i odpowiedzialności, przeprowadzania analizy ryzyka i identyfikacji zagrożeń, tworzenia planów zarządzania ryzykiem, czy procedur zarządzania incydentami.

Sposób implementowania NIS2

W związku z trwającymi pracami nowelizacyjnymi, w implementacji wymagań **NIS2** można uwzględniać **wytyczne ENISA** — Europejskiej Agencji ds. Cyberbezpieczeństwa.

Stosowanie przyjętych praktyk

Wytyczne w dużej części pokrywają się z praktykami przyjętymi w międzynarodowych normach. ENISA wskazuje m.in. na obowiązek określania strategii, ról i odpowiedzialności, przeprowadzania analizy ryzyka i identyfikacji zagrożeń, tworzenia planów zarządzania ryzykiem, czy procedur zarządzania incydentami.

Część z wytycznych wykracza poza zakres norm ISO

Wyróżnić tu należy, m.in.:

- **Bezpieczeństwo łańcucha dostaw** — zarządzanie ryzykiem związanym z dostawcami i partnerami.
- **Bezpieczeństwo w rozwoju i utrzymaniu systemów IT** — wymagania dotyczące bezpiecznego kodowania i testowania.
- **Szczegółowe wymogi testowania** — określające sposoby weryfikacji bezpieczeństwa systemów, przede wszystkim przez testy penetracyjne.
- **Włączanie kadry kierowniczej w procesy bezpieczeństwa** — zarówno w obszarze szkolenia, jak również bezpośredniego ponoszenia odpowiedzialności za spełnienie wymagań NIS2.

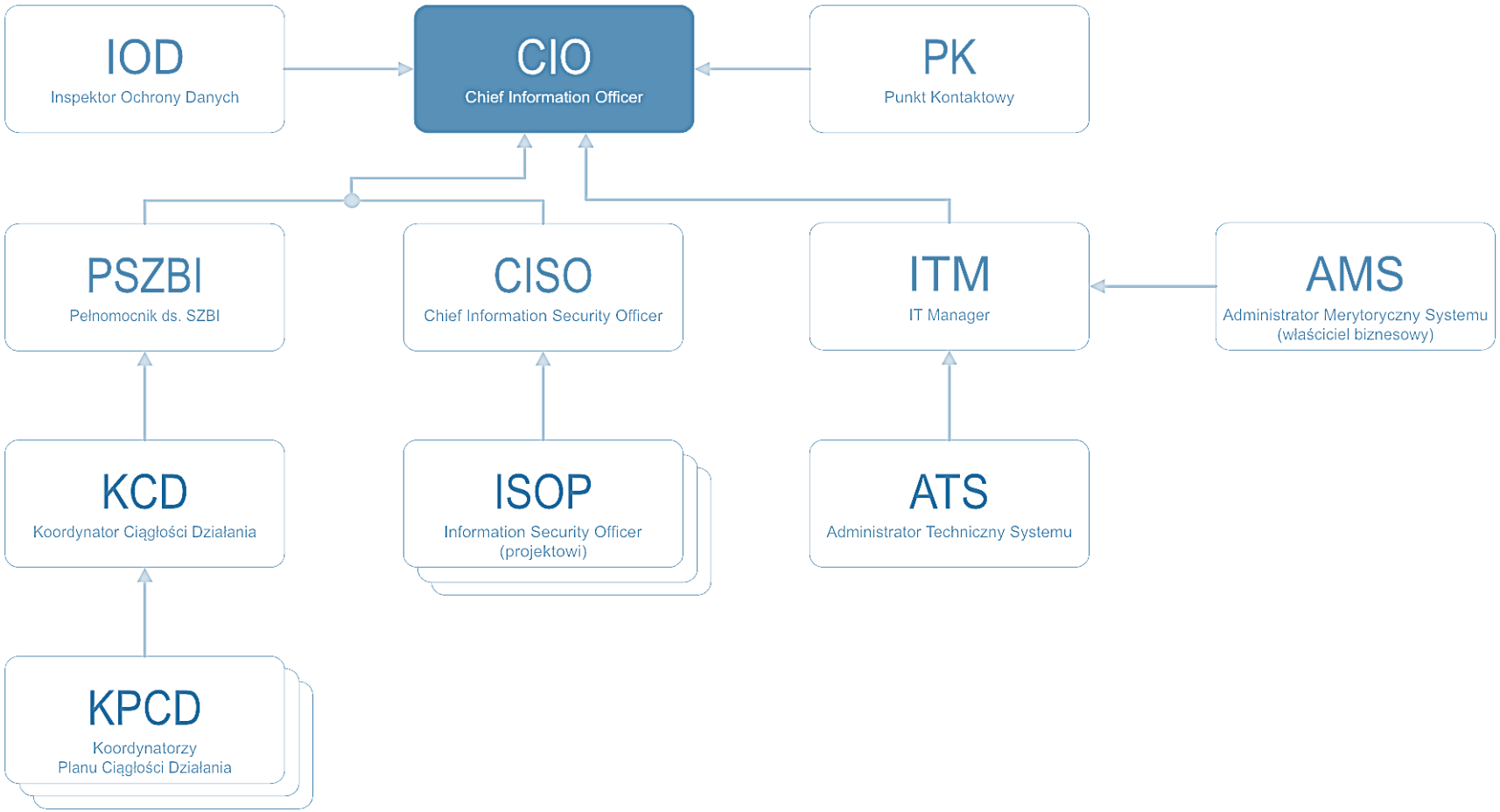
1. Polityka bezpieczeństwa systemów IT

- Definiuje podejście do zarządzania bezpieczeństwem
- Uwzględnia cele biznesowe i bezpieczeństwa
- Zawiera zobowiązanie do ciągłego doskonalenia
- Określa zasoby: kadrowe, techniczne, finansowe
- Wymaga zatwierdzenia przez kierownictwo
- Wskazuje wskaźniki i sposób przeglądu polityki

2. Role i odpowiedzialności w cyberbezpieczeństwie

- Jasno przypisane role i obowiązki
- CISO raportujący bezpośrednio do kierownictwa
- Rozdział konfliktowych obowiązków
- Zaangażowanie osób trzecich w przestrzeganie zasad
- Przegląd ról po incydentach i zmianach

Przykładowa struktura organizacyjna



3. Ramy zarządzania ryzykiem

- Identyfikacja zagrożeń i słabości
- Ocena ryzyk z uwzględnieniem ich wpływu i prawdopodobieństwa
- Plan postępowania z ryzykiem i przypisanie odpowiedzialnych
- Zatwierdzanie ryzyk resztkowych przez kierownictwo
- Włączenie ryzyk od stron trzecich
- Zgodność z przyjętym poziomem tolerancji ryzyka

4. Monitorowanie zgodności z politykami

- Regularne przeglądy zgodności z politykami i procedurami
- Tworzenie raportów dla kierownictwa
- Zbieranie informacji z różnych źródeł (audyt, monitoring)
- Uwzględnienie zmian w przepisach i środowisku
- Działania korygujące i raportowanie postępów
- Zgodność z ISO 27001 oraz NIST CSF

5. Niezależny przegląd bezpieczeństwa

- Wykonywany przez osoby bez konfliktu interesów
- Obejmuje ludzi, procesy i technologie
- Może być zlecany podmiotowi zewnętrznemu
- Powtarzany cyklicznie oraz po incydentach
- Dokumentowane wyniki i działania korygujące
- Wyniki raportowane do kierownictwa

6. Polityka obsługi incydentów

- Opisuje procedury reagowania na incydenty
- Zawiera system kategoryzacji zdarzeń
- Wskazuje role i odpowiedzialności
- Zawiera plany komunikacji i eskalacji
- Uwzględnia spójność z planem ciągłości działania
- Określa dokumenty i formularze do użycia

7. Monitorowanie i logowanie

- Monitorowanie aktywności systemów i sieci
- Logowanie zdarzeń bezpieczeństwa
- Analiza logów pod kątem anomalii
- Zabezpieczanie integralności logów
- Zgodność z przepisami dot. prywatności
- Przechowywanie logów przez określony czas

8. Zgłaszanie zdarzeń

- Ustanowienie procedury zgłaszania incydentów
- Kryteria oceny powagi zdarzenia
- Ścieżki eskalacji i powiadamiania
- Zgłoszenia do CSIRT
- Szablony raportów i zgłoszeń
- Zachowanie terminów zgłoszeniowych

9. Ocena i klasyfikacja incydentów

- Definicja kategorii incydentów
- Kryteria klasyfikacji: wpływ, zakres, czas trwania
- Identyfikacja incydentów istotnych
- Użycie jednolitego systemu klasyfikacji
- Spójność z analizą ryzyka
- Klasyfikacja wspomagana narzędziami IT

10. Reakcja na incydenty

- Aktywacja planów reagowania
- Podział ról w ramach zespołu reagowania
- Zasady izolacji i usuwania zagrożeń
- Współpraca z zespołami zewnętrznymi
- Zbieranie dowodów i dokumentacja
- Minimalizacja wpływu na usługi

11. Przegląd po incydencie

- Analiza przyczyn i przebiegu
- Identyfikacja luk w zabezpieczeniach
- Rekomendacje i działania naprawcze
- Aktualizacja procedur
- Udział zarządu w przeglądzie
- Raport końcowy i wnioski

12. Plan ciągłości działania (BCP)

- Identyfikacja procesów krytycznych
- Określenie RTO i RPO
- Scenariusze awaryjne i alternatywne sposoby przetwarzania
- Role i odpowiedzialności
- Testowanie i przeglądy planu
- Integracja z zarządzaniem ryzykiem

13. Zarządzanie kopiami zapasowymi

- Harmonogram wykonywania backupów
- Zasada 3-2-1 (trzy kopie, dwa nośniki, jedna poza siedzibą)
- Szyfrowanie danych zapasowych
- Testowanie przywracania kopii
- Izolacja backupów od systemów produkcyjnych
- Dokumentacja i monitorowanie procesu

14. Zarządzanie kryzysowe

- Zespół ds. zarządzania kryzysowego
- Definiowanie kryteriów sytuacji kryzysowej
- Scenariusze ćwiczeniowe i symulacje
- Komunikacja z interesariuszami i mediami
- Współpraca z władzami i służbami
- Ocena skuteczności po zakończeniu

15. Polityka bezpieczeństwa łańcucha dostaw

- Identyfikacja kluczowych dostawców
- Ocena ryzyka stron trzecich
- Wymagania bezpieczeństwa w umowach
- Monitoring zgodności dostawców
- Zarządzanie incydentami w łańcuchu
- Plan działania na wypadek przerwania dostaw

16. Ocena skuteczności środków bezpieczeństwa

- Określenie metryk skuteczności
- Regularne testy i przeglądy
- Korelacja z wynikami ryzyka
- Zgłaszanie wyników do zarządu
- Uwzględnienie działań korygujących
- Zgodność z wymaganiami NIS2

17. Cyberhigiena i świadomość użytkowników

- Podstawowe dobre praktyki (hasła, aktualizacje)
- Szkolenia okresowe i onboardingowe
- Kampanie uświadamiające
- Symulacje phishingu
- Materiały edukacyjne i testy wiedzy
- Weryfikacja skuteczności szkoleń

18. Szkolenia specjalistyczne

- Programy dla administratorów i developerów
- Certyfikacje branżowe (np. CISSP, CEH)
- Szkolenia dla zespołów SOC/CSIRT
- Ćwiczenia techniczne i red teaming
- Udział w konferencjach i społecznościach
- Ewaluacja kompetencji i luk

19. Kryptografia i zarządzanie kluczami

- Zasady stosowania algorytmów szyfrujących
- Bezpieczne przechowywanie kluczy
- Zarządzanie cyklem życia kluczy
- Stosowanie HSM i TPM
- Zgodność z rekomendacjami ENISA i ETSI
- Utrzymanie poufności i integralności danych

20. Kontrola dostępu i zarządzanie tożsamością

- Polityka nadawania i odbierania uprawnień
- Stosowanie zasady najmniejszych uprawnień
- MFA dla dostępu do zasobów krytycznych
- Zarządzanie kontami uprzywilejowanymi
- Regularne przeglądy dostępów
- Logowanie i monitorowanie prób dostępu

PYTANIA