Szkolenie: Compendium CE

# KSC/NIS2: Obowiązki i odpowiedzialność - szkolenie dla kadry zarządzającej

## Cel szkolenia:

Szkolenie przedstawia w praktyczny sposób obowiązki i odpowiedzialność kadry zarządzającej wynikające ze znowelizowanej ustawy o KSC oraz dyrektywy NIS2, ze szczególnym naciskiem na podejmowanie decyzji w modelu opartym o ryzyko. Uczestnicy poznają kluczowe wymagania organizacyjne i techniczne, zasady raportowania i obsługi incydentów oraz podejście do utrzymania gotowości audytowej. Program łączy ramy prawne z przykładami i scenariuszami, ułatwiając przełożenie wymagań na konkretne działania w organizacji.

Cele szkolenia:

- Zrozumienie odpowiedzialności (organizacyjnej i osobistej) wynikającej z KSC oraz roli kierownictwa w systemie SZBI.
- Znajomość wymogów operacyjnych, w tym niezbędnej dokumentacji, struktur oraz procesów raportowania incydentów.
- Zdolność do optymalnej alokacji budżetu i priorytetyzacji działań ochronnych na podstawie analizy ryzyka.
- Analiza wpływu cyberzagrożeń na biznes – identyfikacja skutków ataków typu phishing, BEC czy ransomware.
- Zapewnienie gotowości audytowej (audit-ready) poprzez systematyczne dokumentowanie realizacji obowiązków i szkoleń.

Grupa docelowa:

Kadra zarządzająca podmiotów kluczowych i ważnych (w tym członkowie organów wieloosobowych) oraz osoby pełniące funkcje kierownicze w obszarze cyberbezpieczeństwa.

## Plan szkolenia:

- Rola i odpowiedzialność kadry zarządzającej w świetle NIS2/KSC
  - Uzasadnienie objęcia organów decyzyjnych bezpośrednimi obowiązkami prawnymi.
- Obligatoryjne podnoszenie kompetencji
  - Wymóg cyklicznych szkoleń oraz obowiązek pełnego ewidencjonowania procesów



Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

edukacyjnych.

- Model CIANA+PS oraz jego wpływ na stabilność operacyjną
  - Analiza kluczowych atrybutów informacji w kontekście zachowania ciągłości procesów biznesowych.
- Klasyfikacja zdarzeń
  - Operacyjne i prawne rozróżnienie pomiędzy incydentem bezpieczeństwa, naruszeniem ochrony informacji a awarią techniczną.
- Kultura odpowiedzialności
  - Implementacja modelu „tone from the top" jako fundamentu skutecznego zarządzania ryzykiem w organizacji.
- Socjotechnika i kompromitacja tożsamości
  - Ataki typu Phishing, Business Email Compromise (BEC), Deepfake, oraz kradzież poświadczeń i danych uwierzytelniających.
- Ransomware i ataki wymuszeniowe
  - Oprogramowanie typu crypto-malware oraz wielopoziomowe kampanie wymuszeń okupu (Ransomware-as-a-Service).
- Naruszenia danych i błędy konfiguracyjne
  - Incydenty wycieku danych wynikające z błędów w konfiguracji środowisk chmurowych oraz niewłaściwego zarządzania uprawnieniami (IAM).
- Ryzyko łańcucha dostaw (Supply Chain)
  - Ataki ukierunkowane na zewnętrznych dostawców technologii oraz partnerów serwisowych ICT.
- Dostępność usług i ciągłość procesów
  - Ataki typu DDoS oraz inne zagrożenia wpływające na dostępność systemów i stabilność operacyjną.
- Kluczowe filary SZBI
  - Szacowanie ryzyka, dobór środków kontrolnych, zapewnienie ciągłości działania (BCP), budowanie świadomości pracowników oraz ciągłe monitorowanie procesów.
- Minimalny standard techniczno-organizacyjny
  - Wdrożenie uwierzytelniania wieloskładnikowego (MFA), mechanizmy kryptograficzne, zarządzanie tożsamością i uprawnieniami (IAM) oraz systematyczne zarządzanie podatnościami (patch management).
- Strategiczna alokacja zasobów
  - Priorytetyzacja działań oraz optymalizacja budżetu bezpieczeństwa w oparciu o podejście risk-based (koncentracja na obszarach o najwyższym poziomie ryzyka).
- Rejestracja w wykazie podmiotów kluczowych i ważnych
  - Procedury aktualizacji danych oraz harmonogram realizacji obowiązków ustawowych.
- Utrzymanie dostępności krytycznych zasobów informacyjnych



Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

    - Inwentaryzacja usług, struktura właścicielstwa biznesowego oraz matryca komunikacji kryzysowej.
- Zarządzanie incydentami
    - Priorytetyzacja, procedury zgłoszeniowe (24h/72h), struktura ról komunikacyjnych z CSIRT oraz mechanizmy decyzyjne i komunikacja kryzysowa kadry zarządzającej.
- Zarządzanie ładem dokumentacyjnym i operacyjnym oraz wdrożenie procedur retencji danych
- Weryfikacja wiarygodności personelu kluczowego (zespoły SZBI i IR) oraz mitygacje ryzyk personalnych
- Strategiczna optymalizacja modelu operacyjnego
    - Struktury wewnętrzne vs. outsourcing (MSSP) – kryteria kwalifikacji dostawców.
- Cykliczne audyty bezpieczeństwa oraz realizacja ustawowych obowiązków raportowych i sprawozdawczych.
- Strategiczna lista kontrolna dla kadry zarządzającej
    - Priorytetyzacja działań w modelu 30/60/90 dni.
- Formalizacja właścicielstwa procesowego oraz zatwierdzenie wiążącego harmonogramu realizacji.

## Wymagania:

Brak wymagań wstępnych w zakresie wiedzy technicznej. Zalecana jest ogólna znajomość funkcjonowania organizacji (procesy, struktura decyzyjna, podstawowe pojęcia ryzyka i zgodności), aby sprawniej odnieść omawiane obowiązki KSC/NIS2 do realiów własnego podmiotu.

## Poziom trudności



## Certyfikaty:

Uczestnicy szkolenia otrzymują certyfikat ukończenia szkolenia sygnowany przez Compendium CE (ukończenie szkolenia).

## Prowadzący:

Instruktor Compendium Centrum Edukacyjnego.

## Informacje dodatkowe:

Pokrycie ustawowego zakresu (art. 8e ust. 2 – Znowelizowana Ustawa o KSC) i elementy rozszerzające:



Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Art. 7b ust. 4, art. 7c, art. 7f ust. 3 (ewidencja / wykaz)
- Art. 8 (SZBI)
- Art. 8d (zadania i odpowiedzialność kierownika)
- Art. 8f ust. 1–2 (weryfikacja personelu)
- Art. 9–12b (współpraca, obsługa i raportowanie incydentów)
- Art. 14 (struktury wewnętrzne / usługi zewnętrzne)
- Art. 15 (audyt)
- Elementy rozszerzające ponad minimum ustawowe: (podstawy cyber i bezpieczeństwa informacji + przegląd zagrożeń).



Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001