

Program szkolenia

Cyberbezpieczeństwo dla kadry menedżerskiej w świetle NIS2 i KSC

<https://bloomwise.pl/consulting/training/cyberbezpieczenstwo-dla-kadry-menedzerskiej-w-swietle-nis2-i-ksc>

Poniższy zakres stanowi bazę, którą możemy dopasować do specyfiki Twojej marki, zespołu i modelu pracy z klientem.

Moduł 1. NIS2 i KSC jako obowiązek zarządczy, a nie wyłącznie techniczny

- 1.1 NIS2, KSC i zakres odpowiedzialności Spółki — różnica między dyrektywą UE, ustawą krajową, wymogami sektorowymi, normami technicznymi i wewnętrznymi politykami bezpieczeństwa.
- 1.2 Podmioty kluczowe i podmioty ważne — znaczenie kwalifikacji prawnej Spółki, wpisu do wykazu KSC, danych kontaktowych, domen, adresów IP i odpowiedzialności za aktualność informacji.
- 1.3 Rola najwyższego kierownictwa — cyberbezpieczeństwo jako element ładu organizacyjnego, nadzoru nad ryzykiem, budżetowania, ciągłości działania i kontroli wewnętrznej. Nowelizacja KSC wprowadza odpowiedzialność kierownika podmiotu kluczowego i ważnego za realizację zadań z zakresu cyberbezpieczeństwa.
- 1.4 Ryzyko interpretacyjne i praktyczne — dlaczego zgodność formalna nie jest równoznaczna z realną odpornością organizacji; znaczenie dowodów zgodności, rejestrów, decyzji, raportów i przeglądów.
- 1.5 Ćwiczenie menadżerskie — szybka samoocena: „Czy Spółka potrafi wykazać, kto odpowiada za najważniejsze ryzyka cyberbezpieczeństwa i jak są one raportowane do zarządu?”.

Moduł 2. Cyberzagrożenia krytyczne w codziennej działalności Spółki

- 2.1 Phishing, BEC i przejęcie kont menadżerskich — zagrożenia dla poczty, autoryzacji płatności, obiegu dokumentów, kontaktów z kontrahentami i decyzji finansowych.
- 2.2 Ransomware i niedostępność systemów — wpływ na produkcję, logistykę, obsługę klienta, księgowość, HR, systemy ERP, pocztę, systemy chmurowe i komunikację wewnętrzną.
- 2.3 Ryzyko dostawców i usług zewnętrznych — outsourcing IT, usługi chmurowe, serwisanci, dostawcy oprogramowania, dostawcy usług zarządzanych i zależność od łańcucha dostaw.
- 2.4 Wyciek danych i utrata poufności — informacje handlowe, dane osobowe, tajemnica przedsiębiorstwa, dane finansowe, dokumentacja techniczna, informacje o klientach i kontrahentach.
- 2.5 Ćwiczenie decyzyjne — scenariusz: „Konto dyrektora finansowego zostało przejęte, a z niego wysłano polecenie płatności do księgowości” — decyzje w pierwszych 30 minutach.

Moduł 3. Środki ochrony wymagające nadzoru menedżerskiego

- 3.1 Zarządzanie ryzykiem cyberbezpieczeństwa — identyfikacja aktywów, właściciele ryzyk, poziom akceptowalnego ryzyka, plan postępowania z ryzykiem, cykliczne raportowanie i dowody wykonania działań.
- 3.2 Kontrola dostępu i tożsamości — MFA, zasada najmniejszych uprawnień, recertyfikacja dostępów, konta uprzywilejowane, dostęp dostawców, szybkie odbieranie uprawnień po zmianie stanowiska lub zakończeniu współpracy.
- 3.3 Bezpieczeństwo techniczne w języku zarządczym — segmentacja sieci, VPN, szyfrowanie, EDR, kopie zapasowe, testy odtworzeniowe, podatności, aktualizacje, logowanie i monitoring. W dokumentacji projektowej wskazano m.in. model strefowy sieci, separację VLAN, zasadę „deny all, allow by exception”, MFA dla VPN oraz monitoring SIEM jako przykładowe mechanizmy ograniczające ryzyko cyberzagrożeń.
- 3.4 Ciągłość działania i odporność operacyjna — RTO, RPO, procesy krytyczne, alternatywne kanały pracy, testy planów awaryjnych, decyzje o priorytetach odtworzenia usług.
- 3.5 Warsztat praktyczny — mapa krytycznych procesów Spółki: „które procesy muszą działać po 4, 24 i 72 godzinach od incydentu oraz kto podejmuje decyzję o ich priorytecie?”.

Moduł 4. Incydenty, raportowanie, komunikacja i utrzymanie zgodności

- 4.1 Rozpoznanie i kwalifikacja incydentu — incydent, incydent poważny, podatność, cyberzagrożenie, potencjalne zdarzenie dla cyberbezpieczeństwa; znaczenie szybkiego wykrycia i jednoznacznej ścieżki eskalacji.
- 4.2 Zgłaszanie i współpraca z CSIRT — obowiązki raportowe, wewnętrzna ścieżka powiadamiania, rola CISO/IT/compliance/prawników/komunikacji i zarządu; w świetle KSC CSIRT sektorowy może m.in. wspierać analizę ryzyka, analizę incydentów, koordynację obsługi incydentów i podnoszenie świadomości cyberzagrożeń.
- 4.3 Komunikacja kryzysowa — komunikacja do pracowników, klientów, dostawców, organów nadzorczych, ubezpieczyciela, mediów i właścicieli biznesowych; czego nie komunikować bez potwierdzonych faktów.
- 4.4 Dowody zgodności i audytowalność — rejestry incydentów, raporty z testów backupu, wyniki audytów, decyzje zarządcze, protokoły przeglądów, rejestr ryzyk, dokumentacja szkoleń i działania korygujące.
- 4.5 Podsumowanie zarządcze — lista 10 pytań kontrolnych dla menadżera: „co powinienem regularnie wiedzieć o cyberbezpieczeństwie swojego obszaru, aby realnie nadzorować ryzyko?”