Opis szkolenia

Dane o szkoleniu

Kod szkolenia: 5024226

Temat: Obowiązki Kierownika podmiotu kluczowego i podmiotu ważnego w aspekcie nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (UKSC 2.0 / NIS2)

27 Marzec Transmisja ONLINE, Internet ,

Kod szkolenia: 5024226

Koszt szkolenia: 650.00 + 23% VAT

Program

Czas trwania: 1 dzień (9:00–16:00) **O szkoleniu W dniu 19 lutego 2026 r. Prezydent RP podpisał ustawę o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw. Nowelizacja nakłada na podmioty kluczowe lub podmioty ważne liczne obowiązki, w tym m.in. obowiązek wdrożenia w Jednostce systemu zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot. Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (UKSC 2.0), wdrażająca dyrektywę NIS2 do krajowego porządku prawnego wprowadza fundamentalną zmianę w zakresie odpowiedzialności kadry kierowniczej. Cyberbezpieczeństwo przestaje być wyłącznie obszarem IT – staje się obowiązkiem ustawowym zarządu i kierownictwa jednostki. Szkolenie kompleksowo przygotowuje osoby zarządzające do realizacji nowych obowiązków, minimalizując ryzyko odpowiedzialności administracyjnej i finansowej. Dla kogo jest to szkolenie?**

Szkolenie dedykowane jest w szczególności:

1)

Prezesom Zarządów i Członkom Zarządów

2)

Dyrektorom i Kierownikom jednostek organizacyjnych

3)

Kierownikom podmiotów kluczowych i podmiotów ważnych

4)

Kierownikom ds. cyberbezpieczeństwa

5)

Pełnomocnikom ds. SZBI i SZCD

6)

Osobom odpowiedzialnym za bezpieczeństwo informacji

Celem szkolenia jest przygotowanie kadry kierowniczej do:

1)

prawidłowej identyfikacji statusu podmiotu (kluczowy/ważny),

2)

wdrożenia i nadzoru nad systemem zarządzania bezpieczeństwem informacji (SZBI) oraz nad systemem zarządzania ciągłością działania (SZCD),

3)

prawidłowego zarządzania incydentami i obowiązkami raportowymi z wykorzystaniem S46,

4)

przygotowania organizacji do kontroli i nadzoru ze strony organów ds. cyberbezpieczeństwa,

5)

ograniczenia ryzyka kar pieniężnych oraz odpowiedzialności osobistej kierownika podmiotu.

Korzyści dla uczestników Po zakończeniu szkolenia uczestnicy: 1) rozumieją zakres swoich obowiązków ustawowych,

2)

potrafią określić status swojej jednostki,
3)
znają zasady wdrożenia i nadzoru nad SZBI i SZCD,
4)
wiedzą jak prawidłowo zgłaszać incydenty,
5)
potrafią przygotować organizację do kontroli ze strony organów ds. cyberbezpieczeństwa,
6)
znają konsekwencje finansowe i administracyjne niewykonania obowiązków wynikających z UKSC 2.0.

1. Nowelizacja UKSC 2.0 – nowe realia odpowiedzialności kierownictwa (implementacja dyrektywy NIS2; zakres zmian w ustawie o KSC; podmioty kluczowe i podmioty ważne – nowe definicje; rozszerzenie katalogu sektorów; osobista odpowiedzialność Kierownika jednostki; sankcje i kary pieniężne). 2. Kryteria klasyfikacji i samoidentyfikacja podmiotów (sektory kluczowe i sektory ważne; kategorie funkcji krytycznych; kryteria wielkościowe i jakościowe; obowiązek samoidentyfikacji i samorejestracji; najczęstsze błędy klasyfikacyjne).
3.
Obowiązki kierownika podmiotu kluczowego/ważnego (wyznaczenie osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami KSC; zapewnienie zasobów finansowych i organizacyjnych; obowiązek corocznych szkoleń kierownictwa; odpowiedzialność za dokumentowanie realizacji obowiązków wynikających z UKSC 2.0; delegowanie zadań a odpowiedzialność osobista).
4.
System zarządzania bezpieczeństwem informacji (SZBI) jako obowiązek ustawowy (zarządzanie ryzykiem jako obowiązek prawny; minimalne środki techniczne i organizacyjne; dokumentacja SZBI wymagana ustawą; rola kierownictwa w nadzorze nad SZBI; powiązania z ISO 27001, ISO 27005, KRI i RODO).
5.
System zarządzania ciągłością działania (SZCD) (zapewnienie odporności operacyjnej; analiza wpływu na działalność (BIA), plany ciągłości działania, testowanie i aktualizacja planów, odpowiedzialność Kierownika za zapewnienie ciągłości świadczonych usług).
6.
Zarządzanie incydentami i obowiązki raportowe (definicja incydentu, incydentu poważnego, cyberzagrożenia, potencjalnego zdarzenie dla cyberbezpieczeństwa; wewnętrzne procedury zgłaszania incydentów i zdarzeń; terminy raportowania do CSIRT; obsługa incydentów w systemie S46; powiązanie z obowiązkami wynikającymi z RODO w zakresie zgłaszania naruszeń ochrony danych osobowych poprzez S46).
7.
Nadzór, kontrola i odpowiedzialność administracyjna (organy właściwe ds. cyberbezpieczeństwa i ich kompetencje; postępowania kontrolne; dokumentowanie realizacji obowiązków z UKSC 2.0; kary pieniężne; odpowiedzialność osobista kierownika podmiotu).
8.
Plan działań wdrożeniowych dla kierownika podmiotu – praktyczna mapa drogowa (checklista obowiązków kierownictwa; plan działań na 30/60/90 dni; najczęstsze ryzyka i błędy organizacyjne).