PEŁNOMOCNIK DS. CYBERBEZPIECZEŃSTWA

NIS 2 I UKSC W PRAKTYCE

Szkolenie kompleksowo przygotowuje uczestników do praktycznego stosowania wymagań NIS 2 i ustawy o krajowym systemie cyberbezpieczeństwa – zarówno osoby odpowiedzialne za realizację tych obowiązków w organizacji, jak i osoby, które chcą zdobyć wiedzę pozwalającą wdrażać wymagania, doradzać lub szkolić innych w tym zakresie.

Podczas dwóch dni uczestnicy przechodzą przez cały proces: od ustalenia, czy i w jakim zakresie organizacja podlega UKSC, przez określenie ról i odpowiedzialności, zakres systemu zarządzania bezpieczeństwem informacji oraz wymaganą dokumentację, aż po obsługę incydentów, wymagania wobec dostawców, audyt, nadzór i odpowiedzialność kierownictwa.
Szkolenie nie ogranicza się do omówienia przepisów. Uczestnicy pracują na dokumentach, wzorach i rzeczywistym przypadku organizacji, dzięki czemu uczą się przekładać wymagania prawne na konkretne działania, procesy i dokumentację.

Zakres szkolenia obejmuje pełny zakres wskazany w art. 8e ust. 2 UKSC, czyli zakres corocznego szkolenia kierownika podmiotu oraz osoby, której powierzono obowiązki kierownika w zakresie cyberbezpieczeństwa.

PO SZKOLENIU UCZESTNIK BĘDZIE POTRAFIŁ:

- Zidentyfikować, czy i w jakiej kategorii organizacja podlega UKSC oraz sprawdzić kompletność wpisu w wykazie,
- Określić zakres systemu zarządzania bezpieczeństwem informacji dla świadczonej usługi,
- Wskazać role wymagane w organizacji, ich podstawy prawne oraz odpowiedzialność kierownika i osoby, której powierzono obowiązki,
- Opracować strukturę dokumentacji wymaganej przez UKSC i NIS 2,
- Wskazać, które wymagane dokumenty i procesy już funkcjonują w organizacji,
- Wykonać zgłoszenie incydentu poważnego w wymaganych terminach wraz z wymaganymi sprawozdaniami,
- Określić wymagania wobec dostawców, w tym odpowiednie zapisy umowne,
- Zaplanować audyt bezpieczeństwa zgodny z art. 15 UKSC,
- Wskazać sposób połączenia wymagań cyberbezpieczeństwa, odporności podmiotu krytycznego i obowiązkowej ochrony,
- Rozpoznać zakres osobistej odpowiedzialności kierownika i osób wykonujących obowiązki wynikające z UKSC.

Powyższe umiejętności są rozwijane poprzez odpowiednio zaprojektowane ćwiczenia, analizę dokumentacji oraz pracę na rzeczywistym przykładzie organizacji.

RAMOWY PROGRAM:

- Wprowadzenie do NIS 2 i UKSC
- Kwalifikacja podmiotu – podmiot kluczowy, ważny lub pozostający poza regulacją,
- Wpis do wykazu oraz obowiązki związane ze zmianą i aktualizacją danych,
- Określenie zakresu systemu zarządzania bezpieczeństwem informacji,
- Środki zarządzania ryzykiem i sposób ich doboru,
- Role i podział odpowiedzialności: kierownik, pełnomocnik, osoby realizujące zadania,
- Dokumentacja normatywna i operacyjna,
- Struktura zespołu cyberbezpieczeństwa oraz kanały zgłoszeń,
- Klasyfikacja i obsługa incydentów,
- Terminy zgłoszeń: wczesne ostrzeżenie, zgłoszenie i sprawozdania,
- Bezpieczeństwo łańcucha dostaw i wymagania wobec dostawców,
- Model własny i outsourcing usług cyberbezp.,
- Audyt bezpieczeństwa,
- Nadzór organów oraz odpowiedzialność i kary,
- Zbieg wymagań NIS 2/UKSC z CER, ochroną fizyczną i innymi reżimami bezpieczeństwa.

TRENER:

Grzegorz Krzemiński - doradca ds. cyberbezpieczeństwa i zgodności. Ponad 30 lat praktyki w bezpieczeństwie wielodomenowym, od 1995 r. - od wdrożeń systemów zarządzania po ponad tysiąc audytów u dostawców usług ICT, w bankowości, transporcie i logistyce, przemyśle, infrastrukturze komunalnej i ochronie zdrowia.

Pracuje na styku: ochrony fizycznej, ochrony przeciwpożarowej, ATEX, bezpieczeństwa informacji, ciągłości działania i cyberbezpieczeństwa. NIS 2 pokazuje nie jako przepis do odczytania, ale jako wymaganie, które trzeba uzgodnić między specjalistami różnych obszarów i uczy, jak z nimi rozmawiać.

Autor Metodyki Audytu Bezpieczeństwa, metody PIWJ atomizacji przepisów na weryfikowalne wymagania jednostkowe. Uczestnik prac normalizacyjnych nad normami z serii ISO/IEC 27001 i ISO 22301, w tym ISO 22316 o odporności organizacyjnej. Autor książek: "Audyt bezpieczeństwa – praktyczny poradnik" i "Zarządzanie bezpieczeństwem – sztuka czy rzemiosło".

CERTYFIKAT:

Szkolenie zakończone jest uzyskaniem dwujęzycznego certyfikatu ukończenia szkolenia z zakresem tematycznym. Certyfikat stanowi udokumentowanie udziału w szkoleniu w rozumieniu art. 8e ust. 3 UKSC.

ĆWICZENIA:

- Sprawdzenie kwalifikacji podmiotu i kompletności wpisu,
- Określenie zakresu systemu zarządzania bezpieczeństwem informacji,
- Identyfikacja ról, odpowiedzialności oraz ewentualnych luk organizacyjnych,
- Opracowanie struktury dokumentacji wymaganej w organizacji,
- Przygotowanie treści kanału zgłoszeń i komunikatu dla użytkowników,
- Wypełnienie wczesnego ostrzeżenia dotyczącego incydentu,
- Przygotowanie sprawozdania końcowego z incydentu,
- Opracowanie wymagań i klauzul dla dostawców,
- Ocena dostawcy pod kątem ryzyka,
- Przygotowanie planu audytu bezpieczeństwa,
- Analiza jednego obiektu pod kątem równoległego stosowania różnych reżimów bezpieczeństwa.

MATERIAŁY SZKOLENIOWE:

Materiał szkoleniowy składa się z 2 części, dostarczonych przed i po szkoleniu:

- Część I złożoną z materiału merytorycznego oraz zestawu ćwiczeń uczestnik otrzymuje przed szkoleniem.
- Część II złożoną z norm, aktów prawnych, wypełnionych Trenerem ćwiczeń, prezentacji oraz materiałów dodatkowych uczestnik otrzymuje do 7 dni po zakończeniu szkolenia.

CENA SZKOLENIA 1 OS:

Szkolenie on-line: 2900 zł netto
Szkolenie stacjonarne: 3200 zł netto

CZAS TRWANIA

2 dni / (12 godzin)

ZAPISY:

biuro@szkoleniazbezpieczenstwa.pl