kod szkolenia: NIS2 / PL DL1d NIS2

Dyrektywa NIS2 i strategie Analizy Ryzyka

Jednodniowe szkolenie, w trakcie którego zapoznamy uczestników z kluczowymi aspektami wynikającymi z Dyrektywy NIS2.

Oferta skierowana jest do osób zainteresowanych wymogami wynikającymi z wprowadzenia dyrektywy NIS2, zarówno w kontekście samej dyrektywy, jak i obowiązujących przepisów prawa w Polsce.

Szkolenie łączy teorię z praktyką, zapewniając uczestnikom solidną wiedzę i umiejętności niezbędne do skutecznego zarządzania ryzykiem w erze nowych regulacji.

Udział w szkoleniu to inwestycja w bezpieczeństwo organizacji i zwiększenie jej odporności na współczesne zagrożenia cybernetyczne.

Dyrektywa NIS2

Unijne przepisy rozszerzają zakres przepisów dotyczących cyberbezpieczeństwa. Przedsiębiorcy objęci regulacją NIS2, wynikającą z ustawy o krajowym systemie bezpieczeństwa, będą objęci obowiązkiem stosowania produktów, usług bądź procesów, objętych tymi schematami certyfikacyjnymi.

Sprawdź, czy Twoja firma będzie objęta dyrektywą NIS2

Przeznaczenie szkolenia

Szkolenie skierowane jest do osób zarówno bezpośrednio, jak i pośrednio odpowiedzialnych za cyberbezpieczeństwo w firmach oraz instytucjach.

Dedykowane jest szczególnie dla tych, którzy:

- Chcą podnieść świadomość na temat ochrony organizacji przed zagrożeniami cybernetycznymi,

- Potrzebują zrozumienia wymogów wynikających z obowiązującej dyrektywy UE NIS2 oraz przepisów prawa w Polsce,
- Poszukują praktycznych narzędzi i wiedzy do skutecznego wdrażania procedur bezpieczeństwa w swoich organizacjach.

Szkolenie dostarcza zarówno wiedzy teoretycznej, jak i praktycznej, aby wspierać uczestników w dostosowaniu ich organizacji do aktualnych standardów i regulacji z zakresu cyberbezpieczeństwa.

Korzyści wynikające z ukończenia szkolenia

1. Zrozumienie wymogów prawnych:
- Dogłębne poznanie dyrektywy UE NIS2 oraz przepisów prawa polskiego dotyczących cyberbezpieczeństwa.
- Jasne wskazówki, jak dostosować organizację do nowych regulacji.
2. Podniesienie poziomu bezpieczeństwa organizacji:
- Lepsza identyfikacja i minimalizacja zagrożeń cybernetycznych.
- Wdrożenie skuteczniejszych procedur ochrony danych i systemów IT.
3. Praktyczne umiejętności:
- Analiza rzeczywistych incydentów na bazie case studies.
- Ćwiczenia z wykorzystaniem dedykowanej aplikacji VR, umożliwiające symulację scenariuszy zagrożeń i testowanie reakcji na nie.
4. Zwiększenie świadomości w zespole:
- Wzmocnienie świadomości cyberzagrożeń wśród kluczowych osób odpowiedzialnych za bezpieczeństwo w organizacji.
6. Konkretne wskazówki i rozwiązania:
- Gotowe rekomendacje, które można bezpośrednio wdrożyć w firmie lub instytucji.

Oczekiwane przygotowanie słuchaczy

Aby w pełni skorzystać z treści i praktycznych ćwiczeń podczas szkolenia, uczestnicy powinni znać:

1. Podstawowa wiedza o IT:
- Rozumieć podstawowe pojęcia z zakresu technologii informacyjnych i systemów IT używanych w organizacji.
2. Znajomość struktur organizacyjnych:
- Mieć ogólne pojęcie o funkcjonowaniu procesów w swojej organizacji, zwłaszcza tych związanych z bezpieczeństwem i IT.
3. Podstawowa świadomość zagrożeń cybernetycznych:

- Znać główne typy cyberzagrożeń, np. phishing, ransomware, ataki DDoS, oraz ich potencjalne skutki dla organizacji.

4. Ogólne informacje o regulacjach prawnych:

- Posiadać orientację w podstawowych wymogach prawnych dotyczących bezpieczeństwa w swojej branży (np. RODO, ustawa o krajowym systemie cyberbezpieczeństwa).

5. Otwartość na nowe technologie:

- Być gotowym do korzystania z nowych technologii innych cyfrowych narzędzi wykorzystywanych w szkoleniu.

6. Doświadczenie zawodowe w obszarze bezpieczeństwa lub IT (opcjonalne):

- Mile widziana praktyka w zarządzaniu bezpieczeństwem IT, choć nie jest to wymóg konieczny.

Uwaga: Szkolenie jest dostosowane również do osób bez zaawansowanego przygotowania technicznego, dzięki czemu może być wartościowe zarówno dla specjalistów, jak i menedżerów czy administratorów odpowiedzialnych za cyberbezpieczeństwo.

Język szkolenia

Szkolenie: polski
Materiały: polski

Szkolenie obejmuje

- dzień pracy z trenerem
- Nadzór trenera
- Kontakt ze społecznością
- Podręcznik w wersji elektronicznej
- Środowisko laboratoryjne

Metoda szkolenia

- wykład
- warsztaty

Czas trwania

1 dni / 7 godzin

Agenda szkolenia

1. Wprowadzenie do Dyrektywy NIS2:
   - Kluczowe zmiany w porównaniu do poprzedniej dyrektywy NIS.
   - Nowe wymagania i obowiązki dla operatorów usług kluczowych oraz dostawców usług cyfrowych.
2. Wymagania techniczne:
   - Standardy i normy techniczne wymagane przez Dyrektywę NIS2.
   - Praktyczne aspekty implementacji zabezpieczeń technicznych w systemach informatycznych.
3. Wyzwania przed pracownikami:
   - Identyfikacja i analiza głównych wyzwań związanych z cyberbezpieczeństwem w sektorze.
   - Przykłady najlepszych praktyk i studia przypadków z innych organizacji z branży.
4. Praktyczne ćwiczenia i symulacje:
   - Scenariusze incydentów cybernetycznych i reakcje na nie.
   - Ćwiczenia z zakresu oceny ryzyka i zarządzania kryzysowego.