Zarządzanie ryzykiem: Strategie Analizy Ryzyka z użyciem narzędzia IT

Jednodniowe szkolenie, w trakcie którego zapoznamy uczestników z kluczowymi aspektami wynikającymi z Dyrektywy NIS2. Uczestnicy kursu pozyskają wiedzę na temat spełnienia wymogów cyberbezpieczeństwa. Podczas wykładów oraz praktycznych ćwiczeń warsztatowych zdobędą umiejętności związane z kluczowymi elementami dyrektywy NIS2. W szczególności pod kątem realizacji obowiązków związanych z analizą ryzyka, wykorzystując do tego dedykowane narzędzie informatyczne.

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 przeznaczone jest dla osób odpowiedzialnych za cyberbezpieczeństwo w organizacji zatrudnionych na każdym szczeblu organizacyjnym, ze szczególnym uwzględnieniem pracowników objętych wymaganiami Dyrektywy NIS2.

KORZYŚCI WYNIKAJĄCE Z UKOŃCZENIA SZKOLENIA

- Zwiększenie świadomości dotyczącej cyberbezpieczeństwa: Szkolenie powinno zwiększyć świadomość uczestników na temat zagrożeń związanych z cyberbezpieczeństwem i potrzeby ochrony systemów i danych przed atakami cybernetycznymi.
- Zrozumienie dyrektywy NIS2: Uczestnicy powinni zrozumieć kluczowe elementy dyrektywy NIS2, w tym jej cele, zasady i wymogi dotyczące ochrony infrastruktury krytycznej i usług istotnych.
- Identyfikacja i zarządzanie ryzykiem cybernetycznym: Szkolenie powinno pomóc uczestnikom w identyfikacji i ocenie ryzyka cybernetycznego oraz w opracowywaniu i wdrażaniu skutecznych strategii zarządzania ryzykiem.
- Środki bezpieczeństwa w zakresie ciągłości działania: Szkolenie powinno zapewnić wiedzę w zakresie obowiązków podmiotów w zakresie wdrożenia odpowiednich środków, które zapewnią ciągłość działania w przypadku incydentów cyberbezpieczeństwa i umożliwią zminimalizowanie potencjalnych szkód oraz przywrócenie normalnego funkcjonowania systemów.
- Zgodność z przepisami: Szkolenie powinno pomóc uczestnikom zrozumieć, jak spełniać wymogi prawne związane

z cyberbezpieczeństwem, w tym wymogi dyrektywy NIS2, oraz jak unikać potencjalnych sankcji prawnych.

OCZEKIWANE PRZYGOTOWANIE SŁUCHACZY

- Ogólna wiedza dotycząca cyberbezpieczeństwa
- Podstawowa znajomosc obsługi komputera

AGENDA SPOTKANIA

Sala szkoleniowa

- Co to jest NIS2? Kogo dotyczy? – cel i zakres.
  - Przyczyny powstania, zakres oraz wpływ na poziom cyberbezpieczeństwa organizacji.
- Najważniejsze zmiany i obowiązki, które wprowadza NIS2.
  - Omówienie głównych zmian w odniesieniu do obecnie obowiązującej dyrektywy NIS i jej zasięgu.
- Kogo obowiązuje nowa dyrektywa NIS2 i do kiedy mają zostać przeprowadzone zmiany? Podmioty kluczowe a podmioty ważne.
  - Omówienie jakie organizacje są objęte wymogami dotyczącymi bezpieczeństwa w ramach NIS2.
- NIS2 z perspektywy organizacji – Jakie działania trzeba podjąć?
  - Obowiązki podmiotów kluczowych i podmiotów ważnych.
  - Omówienie najważniejszych aspektów i obowiązków w ujęciu organizacji.
- Analiza ryzyka w ramach NIS2 z wykorzystaniem dedykowanej aplikacji – warsztat
  - Przeprowadzenie warsztatów związanych z obszarem zarządzania ryzykiem w ramach Dyrektywy NIS2 z wykorzystaniem aplikacji pozwalającej na automatyzacje działań. Praca na narzędziu z wykorzystaniem ryzyk referencyjnych, pozwalających na podniesienie świadomości uczestników szkolenia.
  - Warsztat pozwoli uczestnikom zrozumieć specyfikę oraz wymagania dotyczące analizy ryzyka w obszarze Dyrektywy NIS2. W ramach tego etapu szkolenia omówione zostaną takie zagadnienia jak:

a) Omówienie procesu zarządzania ryzykiem z wykorzystaniem przykładów w dedykowanej aplikacji

b) Omówienie środków zarządzania ryzykiem w cyberbezpieczeństwie z wykorzystaniem przykładów w dedykowanej aplikacji.

- Tworzenie zintegrowanych systemów zarządzania ryzykiem z wykorzystaniem aplikacji – warsztat .
  - Praca warsztatowa związana z budową zintegrowanego systemu zarządzania ryzykiem w różnych obszarach. Ćwiczenia realizowane z wykorzystaniem dedykowanego narzędzia informatycznego.
  - Warsztat pozwoli na omówienie specyfiki dotyczącej tworzenia w organizacjach zintegrowanego systemu zarządzania ryzykiem w odniesieniu do zarządzania ryzykiem operacyjnym kontekstu bezpieczeństwa informacji, cyberbezpieczeństwa oraz ciągłości działania.

Kod szkolenia	NIS2 / PL AA 1d
Czas trwania	1 dni
Poziom	Podstawowy
Autoryzacja	PBSG