kod szkolenia: BS.IT KZ / PL DL 1d NIS2

Cyberbezpieczny Samorząd - Cyberbezpieczeństwo dla kadry zarządzającej

Celem szkolenia jest zwiększenie świadomości kadry kierowniczej Urzędu w zakresie problematyki związanej z bezpieczeństwem informacji, rozwinięcie umiejętności strategicznego zarządzania cyberbezpieczeństwem oraz zrozumienie przepisów prawnych i ich implementacji.

W wyniku szkolenia kadra kierownicza będzie w stanie efektywnie zarządzać cyberbezpieczeństwem w urzędzie, podejmować strategiczne decyzje dotyczące ochrony danych oraz promować kulturę bezpieczeństwa wśród pracowników. Dzięki temu urząd będzie lepiej przygotowany na ewentualne zagrożenia i incydenty.

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

Sprawdź swoją wiedzę z zakresu:

- **CompTIA CySA+**
- **CompTIA Security+**
- **CompTIA Network+**
- **OSINT - Biały Wywiad, czyli jak dotrzeć do cennych informacji**
- **CEH - Certified Ethical Hacker**
- **ECIH - Certified Incident Handler**
- **Testy penetracyjne**

Odbiorcy szkolenia

Szkolenie jest przeznaczone dla kadry kierowniczej urzędów oraz jednostek samorządu terytorialnego i dotyczy zagadnień związanych z bezpieczeństwem informacji oraz wymogami w zakresie cyberbezpieczeństwa.

Korzyści

1. Podniesienie umiejętności związanych z:
   - rozpoznawaniem zagrożeń i reagowanie na nie,
   - analizą rzeczywistych incydentów
   - zarządzaniem w sytuacjach kryzysowych
2. W wyniku szkolenia kadra kierownicza będzie w stanie:
   - efektywnie zarządzać cyberbezpieczeństwem w urzędzie,
   - podejmować strategiczne decyzje dotyczące ochrony danych oraz promować kulturę bezpieczeństwa wśród pracowników.
3. Pozwoli to na zwiększenie gotowości urzędu na wystąpienie zagrożeń oraz skuteczniejsze zarządzanie incydentami.

Program szkolenia

1. Podstawy cyberbezpieczeństwa (podstawowe pojęcia i zasady działania).
2. Ocena ryzyka, w tym metody identyfikacji i analizy ryzyka związanego z IT, środki zaradcze w celu minimalizacji ryzyka.
3. Audyt wewnętrzny (cyberbezpieczeństwa) i raportowanie zgodności z przepisami.
4. Przegląd najpopularniejszych zagrożeń (w tym rodzaje ataków, ransomware i malware, phishing, oszustwa i wyłudzenia z uwzględnieniem oszustwa typu Business E-mail Compromise, atak telefoniczny, spoofing, atak odwrócony – zmuszenie ofiary do szukania pomocy u atakującego, przekręt nigeryjski, wyłudzenia BLIK, oszustwo na dyrektora/prezesa).
5. Znaczenie cyberbezpieczeństwa dla jednostki samorządu terytorialnego.
6. Przegląd aktualnych zagrożeń i trendów w cyberprzestrzeni.
7. Analiza przepisów rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2024 poz. 773) i ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2024 poz. 1077 z późn. zm.).
8. Zasady postępowania w razie wprowadzenia stopni alarmowych CRP dotyczących zagrożeń w

cyberprzestrzeni.
9. Obowiązki jednostek samorządu terytorialnego wynikające z przepisów.
10. Metody identyfikacji i oceny ryzyka.
11. Tworzenie i implementacja polityk ochrony danych.
12. Standardy i najlepsze praktyki postępowania w celu zapewnienia cyberbezpieczeństwa w urzędzie, cyberhigiena.
13. Profilaktyka cyberbezpieczeństwa w urzędzie, standardy i najlepsze praktyki w tym w zakresie bezpieczeństwa urządzeń i bezpieczeństwa fizycznego.
14. Sposoby podnoszenia świadomości pracowników Urzędu w zakresie cyberbezpieczeństwa i testowania odporności Urzędu na różnego rodzaju ataki.
15. Umiejętność skutecznej komunikacji z zespołem, z innymi komórkami urzędu i jednostek podległych oraz z interesariuszami zewnętrznymi w sprawach cyberbezpieczeństwa.
16. Procesy i procedury zarządzania incydentami oraz role poszczególnych pracowników.
17. Rola kadry kierowniczej w zakresie cyberbezpieczeństwa (w tym w sytuacjach kryzysowych).
18. Incydenty w kontekście zachowania ciągłości działania urzędu.
19. Przywództwo, motywowanie zespołu i promocja kultury bezpieczeństwa w urzędzie.

Ćwiczenia praktyczne

- Rozpoznawaniem zagrożeń i reagowaniem na nie.
- Analizą rzeczywistych incydentów (studia przypadków).
- Zarządzaniem w sytuacjach kryzysowych (scenariusze codziennych zagrożeń).

Oczekiwane przygotowanie uczestnika

Podstawowa znajomość obsługi komputera.

Szkolenie obejmuje

- 1 dzień pracy z trenerem
- Nadzór trenera
- Kontakt ze społecznością
- Materiały w wersji elektronicznej

Czas trwania

1 dni / 7 godzin

Język

- Szkolenie: polski
- Materiały: polski