kod szkolenia: BS.IT KZ / PL DL 2d NIS2

Cyberbezpieczeństwo dla kadry zarządzającej (AI)

Szkolenie „CyberBezpieczeństwo dla kadry zarządzającej” przygotowuje liderów do podejmowania świadomych decyzji w obszarze ochrony danych, zarządzania ryzykiem oraz reagowania na incydenty cybernetyczne. Uczestnicy poznają najnowsze trendy i technologie w zakresie bezpieczeństwa IT, OT oraz AI, a także aktualne regulacje prawne — w tym NIS2 oraz Cybersecurity Act — które wpływają na obowiązki i odpowiedzialność przedsiębiorstw. Program łączy wiedzę strategiczną, technologiczną i prawną, umożliwiając budowanie odporności organizacji na współczesne zagrożenia oraz skuteczne ograniczanie ryzyka finansowego i reputacyjnego.

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 przeznaczone jest dla osób, które odpowiadają za strategiczne i operacyjne decyzje w zakresie bezpieczeństwa informacji, w tym:

- kadry zarządzającej i członków zarządów,
- menedżerów średniego i wyższego szczebla,
- właścicieli firm i przedsiębiorców,
- dyrektorów działów IT, bezpieczeństwa i compliance,
- osób odpowiedzialnych za wdrażanie polityk bezpieczeństwa w organizacji.

Korzyści

1. Zwiększenie świadomości o cyberzagrożeniach – poznasz, jak identyfikować i minimalizować ryzyka związane z atakami w środowisku IT, OT oraz AI, co pozwoli skuteczniej chronić dane i systemy przedsiębiorstwa.
2. Poznanie technik ofensywnych i obronnych – dowiesz się, jak działają cyberprzestępcy, jakie metody ataków stosują (m.in. socjotechnika, MITM, deep fake AI) oraz jak skutecznie przeciwdziałać takim incydentom w organizacji.
3. Zrozumienie regulacji prawnych – nauczysz się, jak interpretować i wdrażać przepisy RODO, NIS2 i Cybersecurity Act, aby ograniczyć ryzyko odpowiedzialności finansowej i prawnej.
4. Przygotowanie na zarządzanie kryzysowe – odkryjesz, jak opracować i wdrożyć procedury reagowania na incydenty, by zminimalizować skutki naruszeń oraz zapewnić ciągłość działania przedsiębiorstwa.
5. Budowanie kultury bezpieczeństwa – nauczysz się, jak tworzyć w organizacji środowisko sprzyjające odpowiedzialnemu zarządzaniu informacją i zwiększysz odporność zespołów na manipulacje i błędy ludzkie

Program szkolenia

1. Jak rozumieć CyberBezpieczeństwo w erze informacji
   - Wprowadzenie do tematyki CyberBezpieczeństwa, czym się ono różni od bezpieczeństwa IT oraz bezpieczeństwa informacji, jakich obszarów działalności firm i organizacji dotyczy, czy można analizować kwestie CyberBezpieczeństwa w organizacji w oderwaniu od kontekstu społecznego i geopolitycznego.
2. Przegląd głównych zagrożeń związanych z CyberBezpieczeństwem w kontekście stosowanych technologii i obszaru działania organizacji
   - Zagrożenia wewnętrzne (insider threats), wybrane obszary zagrożeń związanych ze stosowaniem technologii IT, zagrożenia w obszarze OT, zagrożenia związane z łańcuchem dostaw.

3. Przybliżenie wybranych technik ofensywnych stosowanych w CyberAtakach AI
   - Socjotechnika, scenariusz ataku typu MITM krok po kroku, caller ID spoofing, deep fake.
4. Przegląd podstawowych regulacji krajowych i unijnych, dotyczących kwestii związanych z CyberBezpieczeństwem
   - Prawo ogólne, ochrona danych osobowych aka RODO/GDPR, podmioty na które nałożono szczególne obowiązki czyli KSC oraz NIS/NIS2, o przyszłości CyberBezpieczeństwa w UE czyli Cybersecuirty AI Act, regulacje branżowe (np. DORA, rekomendacje KNF)
5. Konsekwencje prawne (i nie tylko) dla firm oraz osób zarządzających związane z naruszeniami i zaniedbaniami w obszarze Cyber Bezpieczeństwa
   - Odpowiedzialność kodeksowa (osobista kadry zarządzającej), kary finansowe nakładane na organizacje, dodatkowa odpowiedzialność odszkodowawcza, konsekwencje pozaprawne.
6. Anatomia zaawansowanych ataków celowanych (ang. Advanced Persistent Threat)
   - Omówienie etapów modelowego ataku celowanego oraz możliwości przeciwdziałania takim atakom na podstawie autorskiego rozwinięcia koncepcji Cyber Kill Chain.
7. Kilka słów podsumowania
   - Podsumowanie jak współcześnie należy podchodzić do CyberBezpieczeństwa, podstawowe reguły mające zastosowanie w adresowaniu zagrożeń związanych z CyberBezpieczeństwem, dyskusja oraz potencjalne kolejne kroki.

Oczekiwane przygotowanie uczestnika

Podstawowa znajomość obsługi komputera

Szkolenie obejmuje

- 2 dni pracy z trenerem
- Nadzór trenera
- Kontakt ze społecznością
- Podręcznik w wersji elektronicznej

Czas trwania

2 dni / 14 godzin

Język

- Szkolenie: polski
- Materiały: polski