kod szkolenia: BS.IT BS / PL DL 3,5h

Bezpieczny Samorząd - wykłady Cyber Awerness (AI)

Projekt Cyberbezpieczny Samorząd ma na celu zwiększenie poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego (JST) poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na zdarzenia w systemach informacyjnych.

Zgodnie z założeniami projekt kierowany jest do administracji publicznej: jednostek samorządu terytorialnego wraz z jednostkami podległymi (z wyłączeniem placówek ochrony zdrowia).

Z tego powodu przygotowaliśmy dedykowane szkolenie dla gmin, która pokrywa całą gamę problematyki związanej z cyberbezpieczeństwem!

Bezpieczny Samorząd **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 Handle**
- **Testy penetracyjne**

Odbiorcy szkolenia

Szkolenie skierowane do wszystkich pracowników organizacji korzystających z sieci komputerowych – pracowników biurowych, urzędników, pracowników administracyjnych o profilu nietechnicznym. Wykłady cyberawerness to praktyczne warsztaty, które uświadamiają skalę zagrożeń na jakie jesteśmy narażeni w codziennej pracy.

Korzyści

- Podniesienie świadomości zagrożeń związanych z działaniami cyberprzestępców,
- Podniesienie kompetencji w zakresie bezpieczeństwa informatycznego
- Obniżenie poziomu ryzyka kradzieży lub wyłudzenia poufnych danych,
- Obniżenie poziomu ryzyka utraty ciągłości działania procesów biznesowych,
- Ochrona infrastruktury teleinformatycznej organizacji,

Program szkolenia

1. Studium przypadków ataków na dane.
- Wyjaśnienie podstawowych pojęć w branży bezpieczeństwa.
- Zapoznanie uczestników z przykładami największych wycieków danych w historii – Equifax (USA), OPM(USA), Morele.net i ich konsekwencje finansowe dla firmy.
- Aspekty prawne (NIS2/DORA/ISO/AIACT)
2. Zdobywanie informacji
- OSINT – portale społecznościowe, wycieki danych, analiza danych celem przygotowania ataku socjotechnicznego. POKAZ NA ŻYWO
3. Anatomia ataku
- W tej części szkolenia zostanie wykonany pokaz praktycznego ataku np. pracownika od pozyskania informacji, wykorzystania socjotechnik, poprzez przejęcie kontroli nad komputerem, telefonem i kontem bankowym. Realne pokazanie powiązań wpływu lekceważenia zasad bezpieczeństwa i działania w stresie do utraty tożsamości cyfrowej. POKAZ NA ŻYWO
4. Phishing i spoffing czyli dlaczego jesteśmy podatni.
- Studium przypadków realizacji ataków socjotechnicznych – przykłady z polskich firm i instytucji państwowych. Metody diagnozy ataku i jego naturalizacji.
5. Zabezpieczenie urządzeń końcowych i użytkownika.
- Dobre praktyki dla użytkowników końcowych jak powinni zabezpieczyć sieć WiFi, telefon, komputer, konta internetowe, urządzenia służbowe. Bezpieczne korzystanie z Intrernetu W ramach szkolenia zostanie pokazany sposób wykorzystania sieci do bezpiecznego przechowywania danych oraz

wysyłania szyfrowanych wiadomości przez komunikatory oraz sieci VPN. KONWERSATORIUM.

6. AI – Sztuczna inteligencja w służbie oszustów:
   - Definicja i pokaz praktyczny chatbotów (np. ChatGPT)
   - Wykorzystanie chatbotów do pomocy w codziennej pracy – pokaz praktyczny
   - Zagrożenia związane z chatbotami
   - Phishing związany z AI
   - Wyciek danych / hackowanie ChatGPT
   - Fałszywe tożsamości
   - Wykorzystanie AI do generowania wizerunku
   - Wykorzystanie AI do fałszowania obrazu
   - Wykorzystanie AI do podrabiania głosu
   - Generowanie fałszywych danych
   - Podsumowanie w formie konkretnych rad metod obrony i detekcji

Oczekiwane przygotowanie uczestnika

Znajomość podstawowej obsługi komputera.

Szkolenie obejmuje

Metoda szkolenia

- wykład

Czas trwania

1 dni / 3 godzin

Język

- Szkolenie: polski
- Materiały: polski