kod szkolenia: BS.IT BS / PL AA 2,5h

Bezpieczny Samorząd - wykłady Cyber Awareness

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

Przeznaczenie szkolenia

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

Korzyści wynikające z ukończenia szkolenia

- 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,

Oczekiwane przygotowanie słuchaczy

Znajomość podstawowej obsługi komputera.

Język szkolenia

- Szkolenie: polski
- Materiały: polski

Szkolenie obejmuje

Metoda szkolenia

- wykład

Czas trwania

1 dni / 2 godzin

Agenda szkolenia

1. Studium przypadków ataków na dane.
- Wyjaśnienie podstawowych pojęć w branży bezpieczeństwa IT.
- Zapoznanie uczestników z przykładami największych wycieków danych w historii – Equifax (USA), OPM(USA), Morele.net i ich konsekwencje finansowe dla firmy.
- Aspekty prawne
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. urzędnika 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 urzędów 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.