Program szkolenia „Wprowadzenie do bezpieczeństwa IT”

1. Cyberbezpieczeństwo Definicje

Omówienie podstawowych definicji i słownictwa z zakresu cyberbezpieczeństwa:

- Incydent Cyberbezpieczeństwa;
- Login/hasło mocne, słabe;
- Sieć firmowa/sieć WiFi;
- Program antywirusowy;
- Firewall;
- Węzeł sieci firmowej.

2. Podstawy prawne związane z bezpieczeństwem w IT w administracji:
   - Ustawa o KSC;
   - Inne regulacje prawne: RODO, Ustawa o rachunkowości.

3. Podstawowe rodzaje ataków w cyberprzestrzeni:
   - DDoS;
   - Boty;
   - Phishing;
   - Pharming;
   - Sniffing;
   - Ransomware;
   - Koń trojański;
   - Atak DNS;
   - Ataki przez firmy trzecie.

4. Przykłady udanych ataków hakerskich w Polsce i na świecie:
   - omówienie sposobu ich przeprowadzenia;
   - wskazanie słabych punktów w organizacji.

5. Jak pracownicy mogą wpłynąć na bezpieczeństwo organizacji?
   - obowiązki pracowników dotyczące cyberbezpieczeństwa;
   - dokumenty wewnętrzne dotyczące cyberbezpieczeństwa;
   - procedury;
   - dobre praktyki.

6. Jak organizacje zabezpieczają się przed cyberatakami?
   - szkolenia;
   - audyty;
   - analiza ryzyka;
   - symulowane ataki;
   - analiza podatności i planowanie doskonalenia;
   - wdrazanie zabezpieczeń organizacyjnych i technicznych;
   - wykonywanie tych działań cyklicznie (PDCA).

7. Dokumenty:
   - polityka;
   - regulaminy;
   - procedury;

- dobre praktyki.

8. Podsumowanie:
   - uwagi/pytania;
   - dyskusja.