Program szkolenia

Cyberbezpieczeństwo w administracji publicznej - aspekty prawne, organizacyjne i techniczne

1

BLOK TEMATYCZNY
09:00-9:45

Wstęp do zagadnienia cyberbezpieczeństwa:

Jak należy rozróżniać czym jest cyberbezpieczeństwo i cyberprzestrzeń?

Podstawy bezpieczeństwa w instytucji – tworzenie wdrażanie i utrzymanie polityki bezpieczeństwa:

- Polityka bezpieczeństwa informacji - czym jest w organizacji polityka bezpieczeństwa i jaka jest jej rola.
- Incydenty bezpieczeństwa.
- Norma 27001 – jako powszechne rozwiązanie i standard bezpieczeństwa.
- Audyt systemów komputerowych w tym testy penetracyjne.

POKAZ
9:45-10:45

Ataki na „komputery" – omówienie wraz z demonstracją:

Przegląd najczęstszych ataków komputerowych wykorzystywanych przez cyberprzestępców:

- Ataki przez fałszywe maile.
- Kradzież tożsamości, kradzież haseł tzw. oszustwa nigeryjskie.
- Ataki dokonywane przez telefony komórkowe (fałszywe SMSY tzw. SMS Premium, przekierowania rozmów) - przykłady.
- Ataki dokonywane przez sieci bezprzewodowe (WIFi, Bluetooth).
- Malware – złośliwe oprogramowanie instalowane na komputerach, tabletach, smartfonach - przykłady.
- Phishing – podszywanie się pod osoby lub instytucje - przykłady.
- Oszustwa inwestycyjne – wykorzystanie zdalnego pulpitu w procederach przestępczych.
- Urządzenia mobilne i komunikatory internetowe – podstawy bezpiecznego użytkowania.
- Spoofing telefoniczny – zagrożenia wynikające z możliwości podszywania pod cudzy numer telefonu.

Program szkolenia

Cyberbezpieczeństwo w administracji publicznej - aspekty prawne, organizacyjne i techniczne

10:45-11:00

Przerwa

2

BLOK TEMATYCZNY
11:00-12:00

Socjotechnika, czyli ataki na „człowieka” – omówienie wraz z demonstracją. Jak rozpoznać, że jest się celem ataku socjotechnicznego. Przykłady ataków socjotechnicznych:

- Ataki dokonywane z użyciem Social Media (Facebook, Instagram) w tym przez komunikatory (Messenger, Skype).
- Miejsca, gdzie zostawiamy swoje dane – działania świadome i nieświadome.
- Stalking – uporczywe nękanie przy użyciu e-maili i smsów.
- Mowa nienawiści (hate speech) w sieci.

Sztuczna Inteligencja – najnowsze zagrożenia:

- Zagrożenia wynikające z możliwości generowania obrazów i wizerunków.
- Generowanie głosu przez AI i możliwości złośliwego wykorzystania.
- Tworzenie złośliwego oprogramowania i skryptów obchodzących zabezpieczenia systemów.
- Wykorzystanie sztucznej inteligencji przez oszustów.

Program szkolenia

Cyberbezpieczeństwo w administracji publicznej - aspekty prawne, organizacyjne i techniczne

3

BLOK TEMATYCZNY
12:00-13:00

Aspekty prawne:

- Jakie działania związane z cyberatakami kwalifikowane są jako przestępstwa?
- Jakie kary grożą za popełnianie cyberprzestępstw?
- Jakie prawa ma ofiara, która padła ofiarą cyberprzestępstwa?
- Odpowiedzialność pracownika za ujawnienie informacji.
- Nieautoryzowane użycie komputera.
- Ustawa z dnia 5 lipca 2018 o krajowym systemie cyberbezpieczeństwa – zakres przedmiotowy i podmiotowy ustawy.

Reagowanie w przypadku rozpoznania cyberprzestępstwa:
Gdy instytucja pada ofiarą cyberataku/cyberprzestępstwa - kogo i jak poinformować.

- Sposób postępowania w przypadku zgłaszania popełnienia przestępstwa organom ścigania.
- Współdziałanie z organami ścigania w zakresie rozpoznawania i zwalczania cyberprzestępczości.
- Jak zabezpieczyć dowody cyberprzestępstwa?

Podsumowanie i dyskusja.