PROGRAM SZKOLENIA

1

BLOK TEMATYCZNY
10:00-10:45

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
10:45-11:45

Ataki na „komputery” – omówienie wraz z demonstracją

Przegląd najczęstszych ataków komputerowych wykorzystywanych przez cyberprzestępców:

- Ataki przez fałszywe maile - pokaz.
- Kradzież tożsamości, kradzież haseł tzw. oszustwa nigeryjskie - pokaz.
- Ataki dokonywane przez telefony komórkowe (fałszywe SMSY tzw. SMS Premium, przekierowania rozmów) - przykłady.
- Ataki dokonywane przez sieci bezprzewodowe (WIFi, Bluetooth) - pokaz.
- Malware – złośliwe oprogramowanie instalowane na komputerach, tabletach, smartfonach - przykłady.
- Phishing – podszywanie się pod osoby lub instytucje - przykłady.

11:45-12:05

Przerwa kawowa

2

BLOK TEMATYCZNY
12:05-13:00

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.

PROGRAM SZKOLENIA

13:00-13:30

Lunch

3

BLOK TEMATYCZNY
13:30-14:00

Reagowanie w przypadku rozpoznainia cyberprzestępstwa

Gdy instytucja jako ofiarą cyberataku/cyberprzestępstwa - kogo i jak poinformować.

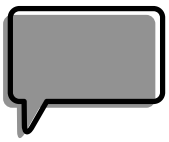
- Sposób postępowania w przypadku zgłaszania popełnienia przestępstwa organom ścigania.
- Współdziałanie z organami ścigania w zakresie rozpoznawania i zwalczania cyberprzestępczości.
- Jak zabezpieczyć dowody cyberprzestępstwa?

POKAZ
14:00-14:45

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 speach) w sieci.



14:45-15:00

Podsumowanie, dyskusja