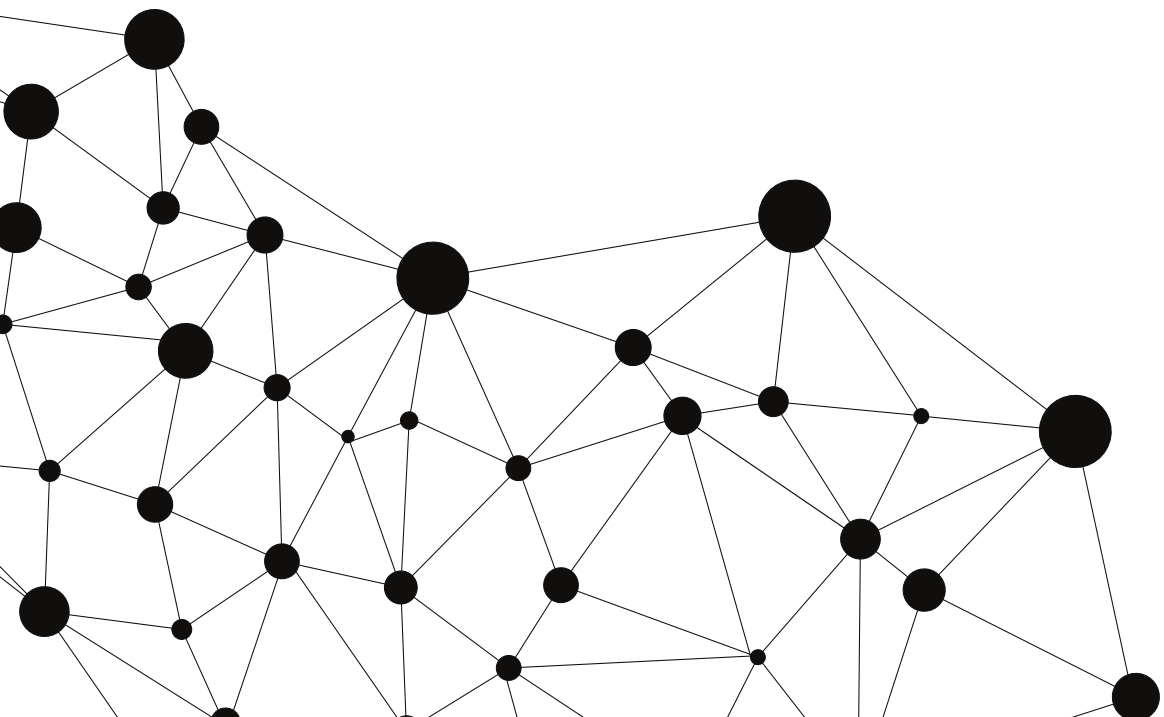
OFERTA

Informacje o szkoleniu

- Organizator: **Polska Platforma Bezpieczeństwa Wewnętrznego**
- Czas trwania szkolenia: **4 godziny zegarowe**
- Forma szkolenia: **online - prezentacja + studium przypadku**

Cel szkolenia

- Wzrost kompetencji kadry w obszarze zagrożeń bezpieczeństwa informacji/cyberbezpieczeństwa– podniesienie poziomu bezpieczeństwa w instytucji.
- Przygotowanie do wdrażania skutecznych rozwiązań organizacyjnych i zachowań podnoszących cyberbezpieczeństwo w urzędzie/instytucji.



OFERTA

Korzyści dla uczestników

- Wzrost świadomości zagrożenia atakiem hackerskim – umiejętność rozróżniania rodzajów i sposobów ataku oraz rozpoznawanie podejrzanych wiadomości, stron, programów.
- Uczestnik pozna własną rolę w procesie ochrony przed zagrożeniami cyberbezpieczeństwa oraz nauczy się odpowiednio oceniać stopień zagrożenia jak również dopasuje do niego odpowiednią reakcję.
- Szkolenie umożliwi podjęcie działań profilaktycznych, których celem będzie wyeliminowanie ryzyka, które potencjalnie może wystąpić w Urzędzie/Instytucji w związku z cyberprzestępczością. Uczestnik szkolenia będzie wiedzieć jak i gdzie zgłaszać próby np.: ataku hakerskiego.
- Umiejętność wykrywania zagrożeń w praktyce przez uczestnictwo w pokazach różnych typów ataków hakerskich przeprowadzonych na wirtualnej maszynie.

Certyfikat

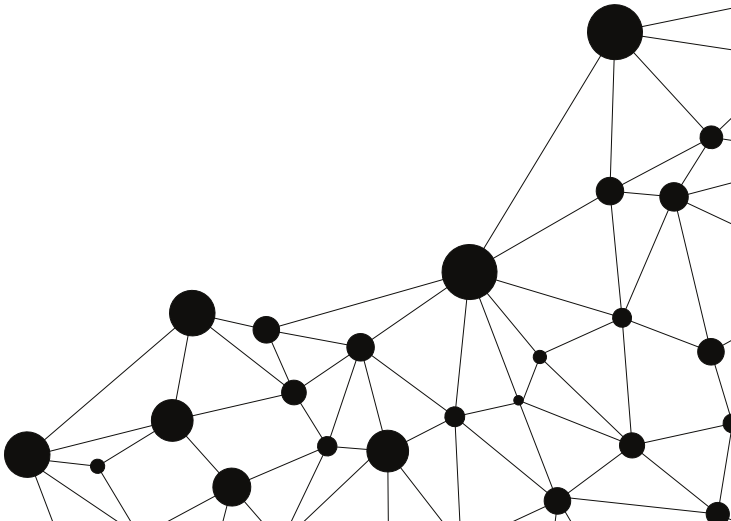
- Certyfikat ukończenia szkolenia wydany przez Polską Platformę Bezpieczeństwa Wewnętrznego oraz materiały szkoleniowe w wersji elektronicznej.

Trener

- Ekspert PPBW z zakresu cyberbezpieczeństwa, od kilku lat zajmuje się ściganiem cyberprzestępczości w jednej z komend wojewódzkich Policji. Specjalista w dziedzinie audytów bezpieczeństwa systemów informatycznych oraz przeprowadzania testów penetracyjnych. Od 2020 roku zaangażowany jest w programy zamkniętych szkoleń z zakresu zwalczania cyberprzestępczości dla jednostek organizacyjnych Policji i Prokuratur. Ukończył specjalistyczne szkolenia dotyczące cyberbezpieczeństwa organizowane między innymi przez firmę Cisco oraz TryHackMe Ltd. oraz zamknięte szkolenia z zakresu social engineering. Uczestnik niezliczonej ilości szkoleń między innymi w zakresie zaawansowanych narzędzi systemów Linux, programowania w języku Python oraz bezpieczeństwa informatycznego instytucji publicznych.

Kontakt

Aneta Jabłońska
Starszy specjalista ds. organizacji szkoleń
tel. +48 61 861 24 46
kom. +48 695 386 963
e-mail: **aneta.jablonska@ppbw.pl**



PROGRAM SZKOLENIA

1

BLOK TEMATYCZNY
9:00-9:45

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 - 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.

10:45-11:00

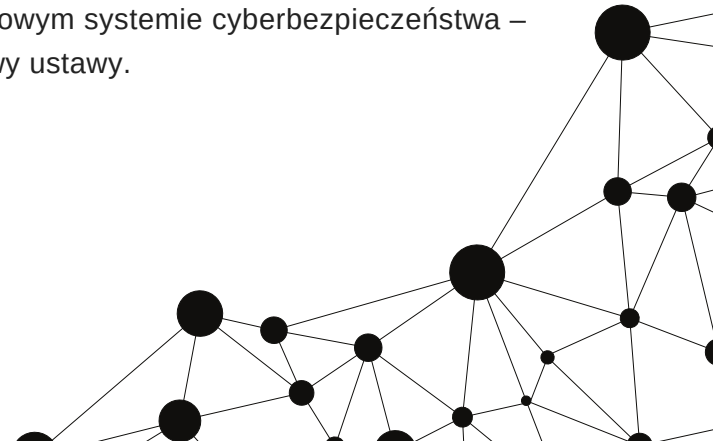
Przerwa

2

BLOK TEMATYCZNY
11:00-12:00

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

3

BLOK TEMATYCZNY
12:00-12:30

Reagowanie w przypadku rozpoznania 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
12:30-13:00

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

Bezpieczeństwo pracy zdalnej:

- Zasady stosowania pracy zdalnej
- Ochrona danych osobowych w pracy zdalnej
- Zasady bezpiecznego korzystania ze zdalnego dostępu do organizacji
- Katalog zabezpieczeń w pracy zdalnej

Podsumowanie, dyskusja