Wektor Wiedzy
Kierunek Twojego rozwoju.

Bezpieczeństwo informacji – aktualne zagrożenia cyberprzestępczością

Wektor Wiedzy
Kierunek Twojego rozwoju.

Program kursu

Temat 1: Podstawy Bezpieczeństwa teleinformatycznego i klasyfikacja zagrożeń.

1. **Podstawy bezpieczeństwa teleinformatycznego**
   - Czy w świecie cyfrowym jest bezpiecznie?
   - Podstawowe narzędzia cyberbezpieczeństwa
   - Aktualność problemu bezpieczeństwa teleinformatycznego – Socjotechnika i manipulacje przestępców
   - Z czego składa się system cyberbezpieczeństwa?
   - Powszechność zagrożeń
   - Co ryzykujemy zaniedbując cyberbezpieczeństwo?
2. **Ataki „na człowieka" tzw. SOCJOTECHNIKA (stosowane techniki manipulacji)**
   - Czym jest socjotechnika?
   - Dlaczego człowiek jest najsłabszym ogniwem
   - Przykłady podstępów socjotechnicznych – wyłudzenia dokumentów, loginów, haseł
   - Jak i skąd atakujący zbierają dane na twój temat
   - Miejsca, w których zostawiamy swoje dane świadomie i nieświadomie - jak świadomie udostępniać informacji w sieci.
3. **Klasyfikacja zagrożeń dla sieci teleinformatycznej i ich źródeł (System i jego podatność)**
   - Antywirus i firewall
   - Niebezpieczeństwo ataków firmę/instytucję
   - Co zrobić, gdy zidentyfikujemy atak?
   - Podatność systemu
   - Sposoby atakowania sieci, rodzaje włamań sieciowych
   - Niebezpieczny system
   - Niebezpieczne aplikacji i źródła
   - Podatność na ataki w związku z przelewami i bankowością
4. **Monitorowanie incydentów bezpieczeństwa teleinformatycznego**
   (Zbieranie danych, diagnozowanie incydentów, podejmowanie działań naprawczych)

Temat 2: Metody i środki bezpieczeństwa technicznego i organizacyjnego

1. **Mechanizmy i programy ochrony przed zagrożeniami cyberbezpieczeństwa**
   - Jakie emocje wykorzystują oszuści w wyłudzeniach danych i finansów?
   - Keyloggery – jak działają, jak się bronić?
   - Malware i Spyware
   - Zagrożenia i zabezpieczenia laptopów i dysków
   - VPN – co to i kiedy korzystać?
2. **Bezpieczeństwo haseł**
   - Bezpieczne hasła
   - Skuteczne organizowanie i zabezpieczanie haseł
   - Uwierzytelnianie dwuskładnikowe
   - Wrażliwe dostępny o które należy zadbać?
   - Jak pracować z pocztą elektroniczną?

3. **Metody i środki bezpieczeństwa**
   - Bezpieczeństwo fizyczne
   - Kopie zapasowe i redundantność
   - Ochrona Danych Osobowych i zagrożenia
   - Kontrola dostępu
   - Zasady ochrony urządzeń mobilnych
   - Polityka stosowania rozwiązań kryptograficznych i szyfrowanie informacji
   - Przedsięwzięcia organizacyjne
   - Zarządzanie uprawnieniami użytkowników systemów informatycznych, kontrola dostępu
4. **Atak „na komputery" - demonstracje wraz z objaśnieniem metod ochrony**
   - Przegląd aktualnych ataków komputerowych wykorzystywanych przez cyberprzestępców, typowe błędy zabezpieczeń wykorzystywane przez atakujących
   - Ataki przez sieci bezprzewodowe (WiFi, Bluetooth, NFC)
   - Ataki przez pocztę e-mail (fałszywe e-maile)
   - Ataki przez strony WWW - jak nie dać się zainfekować, fałszywe strony
   - Ataki przez komunikatory (Skype, Facebook)
   - Ataki przez telefon (fałszywe SMS-y, przekierowania rozmów, itp.)
   - Ataki APT, phishing, smishing, spear-phishing, pharming, spoofing, spam, spim, scam

Temat 3: Rodzaje ataków sieciowych i systemowa organizacja bezpieczeństwa

1. **Cyberprzestępczość - najpowszechniejsze rodzaje ataków i zagrożeń – praktyczne case study przypadków**
   - Phishing i inne odmiany ataków socjotechnicznych
   - Pozostałe zagrożenia dla bezpieczeństwa sieci teleinformatycznej
   - Cracking
   - Sniffing
   - Metoda salami
   - Fałszywe powiadomienia z mediów społecznościowych
   - Oszustwo na „nigeryjskiego księcia"
   - Skimming
2. **Organizacja bezpiecznej sieci teleinformatycznej i bezpieczeństwa informacji – rozwiązania systemowe i wymagania prawne w Polsce**
   - Norma ISO 27001:2017
   - Rozporządzenie o Ochronie Danych Osobowych
   - Rozporządzenie o Krajowych Ramach Interoperacyjności
   - Projektowanie bezpiecznej sieci teleinformatycznej
   - Narzędzia do weryfikacji bezpieczeństwa teleinformatycznego
3. **Dobre praktyki związane z bezpiecznym wykorzystaniem firmowych zasobów**
   - Polityka haseł, zarządzanie dostępem i tożsamością - jakie hasło jest bezpieczne, jak nim zarządzać, zasady udzielania dostępu do zasobów informacyjnych
   - Bezpieczeństwo fizyczne - urządzenia, nośniki danych, dokumenty, „czyste biurko"
   - Bezpieczeństwo danych osobowych kadrowych
   - Bezpieczna praca z urządzeniami mobilnymi (smartfon, tablet, laptop)
   - Problem aktualnego oprogramowania i kopii zapasowych
   - Bezpieczna praca z pakietem biurowym Microsoft Office
   - Bezpieczna praca z programem pocztowym
   - Bezpieczna praca z przeglądarką internetową
   - Zastosowanie technik kryptograficznych (szyfrowanie, certyfikaty

4. Aspekty prawne

- Odpowiedzialność pracownika przed pracodawcą za ujawnienie informacji
- Nieautoryzowane użycie systemów komputerowych
- Rażące zaniedbania związane z wykorzystywaniem sprzętu komputerowego
- Dane osobowe i dane wrażliwe
- Jakie działania związane z cyberatakami kwalifikowane są jako przestępstwa?
- Jakie kary grożą za popełnianie cyberprzestępstw?
- Jakie prawa ma ofiara, która padła ofiarą cyberprzestępstwa?
- Nieautoryzowane użycie komputera.