Szkolenie:

„Aktualne zagrożenia cyberbezpieczeństwa”

Plan szkolenia

Wstęp - Powszechność zagrożeń cyberprzestępczości

- Jak powszechne są cyberprzestępstwa – statystyki
- Kim jest cyberprzestępca?
- Socjotechnika i manipulacje
- Na jakich emocjach działają oszuści
- Przykłady ogłoszeń w darknecie
- Czym ryzykujemy zaniedbując cyberbezpieczeństwo?

Moduł nr 1. Człowiek jako najsłabsze ogniwo

- Przykładowe ataki z pominięciem narzędzi cyberbezpieczeństwa
- Dlaczego najsłabszym ogniwem jest człowiek
- Kogo wybiera cyberprzestępca

Moduł nr 2. – System cyberbezpieczeństwa

- Podstawowe narzędzia cyberbezpieczeństwa
- Z czego powinien składać się skuteczny system cyberbezpieczeństwa
- Jak go zbudować?

Moduł nr 3. Najpowszechniejsze zagrożenia w sieci

- Rodzaje zagrożeń sieciowych
- Wirusy
- Koń trojański i bomba logiczna
- Exploity
- Robaki
- Rokity
- Spyware

Moduł nr 4. Zagrożenia sieciowe jak się bronić?

- Skąd się bierze złośliwe oprogramowanie – przykłady
- Jak je rozpoznać?
- Jak je usuwać?
- Jak się bronić przed złośliwym oprogramowaniem

Lekcja nr 5. Bezpieczna praca w firmie

- Rodzaje zagrożeń w codziennej pracy w firmie
- Zasady czystego biurka
- Zasady czystego ekranu
- Co należy szczególnie chronić

Lekcja nr 6. Podejrzane urządzenia elektroniczne

- Zagrożenia urządzeń elektronicznych
- Przykłady zagrożeń laptopy, pendrive, smartfony
- Jak się przed tym chronić?

Lekcja nr 7. Zagrożenia sieci WiFi

- Publiczne i nie sprawdzone hotspoty – zagrożenia
- Case study – przykładowych zagrożeń
- Bezpieczna praca z WiFi

Lekcja nr 8. Ransomware

- Ransomware jako najczęstszy rodzaj ataków na firmy i instytucje
- Przykłady ataków i konsekwencji
- Jak się chronić i na co zwracać uwagę

Lekcja nr 9. Spyware i Keylogger

- Rodzaje zagrożeń związanych z keylogger i spyware
- Przykłady ataków – utrata danych, podmiany kont bankowych
- Skąd je mamy?
- Jak się przez tym bronić?

Lekcja nr 10. Niebezpieczeństwo aplikacji

- Jakie aplikacje są niebezpieczne
- Zagrożenia związane z niebezpiecznymi aplikacjami
- Jak się bronić i na co zwracać uwagę

Lekcja nr 11. Niebezpieczeństwo komunikatorów i social mediów

- Jak podszyć się pod kogoś w social mediach
- Niebezpieczeństwo komunikatorach i social mediach
- Przykłady ataków

- Jak się przed tym bronić?

Lekcja nr 12. Bezpieczna praca z pocztą elektroniczną

- Zagrożenia związane z pocztą elektroniczną
- Przykłady fałszywych e-maili
- Jak pracować bezpiecznie z poczta elektroniczną?

Lekcja nr 13. Phishing jak się nie dać złowić, na co zwracać uwagę

- Phishing – czym jest, jak działa?
- Przykłady zagrożeń związanych z Phishingem
- Jak zidentyfikować Phishing?
- Jak się bronić przed Phishingiem?

Lekcja nr 14. Bezpieczeństwo haseł

- Skąd cyberprzestępcy mają nasz hasła?
- Jak zweryfikować możliwość utraty haseł?
- Jak bezpiecznie tworzyć i organizować hasła – przykładowe narzędzia
- Jak zapewnić 99,99% bezpieczeństwo dla swoich dostępów

Lekcja nr 15. Bezpieczeństwo pracy zdalnej

- Zagrożenia w pracy zdalnej
- Przykłady możliwych ataków
- Bezpieczeństwo danych
- Jak bezpiecznie pracować na odległość – podstawowe zasady