



Bezpieczeństwo informacji – aktualne zagrożenia cyberprzestępczością

Program kursu:

Temat 1: Podstawy Bezpieczeństwa teleinformatycznego i klasyfikacji zagrożeń

1. Podstawy bezpieczeństwa teleinformatycznego

- Główne pojęcia i zagadnienia związane z bezpieczeństwem sieci teleinformatycznych
- Aktualność problemu bezpieczeństwa teleinformatycznego
- Zarządzanie i utrzymywanie infrastruktury sieciowej
- Współczesne techniki zapewniania bezpieczeństwa informacji w sieci teleinformatycznej

2. Klasyfikacja zagrożeń dla sieci teleinformatycznej i ich źródeł

- Podatności sieci teleinformatycznej na ataki
- Sposoby atakowania sieci, rodzaje włamań sieciowych, rodzaje ataków sieciowych

3. Monitorowanie incydentów bezpieczeństwa teleinformatycznego

- Diagnostowanie incydentów
- Zbieranie danych dotyczących incydentów
- Analiza danych dotyczących incydentów
- Podejmowanie działań naprawczych

Temat 2: Organizacyjne i techniczne środki bezpieczeństwa teleinformatycznego

1. Mechanizmy ochrony przed zagrożeniami bezpieczeństwa sieci teleinformatycznej

- Narzędzia i aplikacje do zabezpieczania sieci
- Systemy wykrywania włamań i ataków
- Zapory sieciowe
- Bezpieczna konfiguracja narzędzi do zarządzania i monitorowania urządzeń sieciowych

2. Metody i środki ochrony informacji

- Bezpieczeństwo fizyczne
- Bezpieczeństwo programowe
- Podstawowe zasady ochrony komputerów służbowych
- Kopie zapasowe i redundancja
- Polityka stosowania rozwiązań kryptograficznych i szyfrowanie informacji
- przedsięwzięcia organizacyjne
- Zarządzanie uprawnieniami użytkowników systemów informatycznych, kontrola dostępu

Temat 3: Cyberbezpieczeństwo i systemy bezpieczeństwa teleinformatycznego

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

Więcej informacji na temat szkolenia znajdziesz na: <https://wektorwiedzy.pl>