Program Seminarium

Cyberbezpieczeństwo

jak skutecznie chronić siebie przez cyberzagrożeniami?

	BLOK TEMATYCZNY NR 1
10:00-11:30	**Wprowadzenie do zagadnienia cyberbezpieczeństwa** **Rodzaje zagrożeń w cyberprzestrzeni, sposoby ochrony i profilaktyka** **Cyberataki** • Malware – złośliwe oprogramowanie instalowane na komputerach, tabletach, smartfonach • Phishing – podszywanie się pod osoby lub instytucje • Ataki typu DDoS – blokowanie stron internetowych i serwerów pocztowych • Pendrive i inne nośniki danych – jako potencjalne źródło przenoszenia złośliwego oprogramowania **Przestępczość ekonomiczna, w tym zagrożenia dla elektronicznych systemów płatności** • Kradzież tożsamości lub haseł • Złośliwe oprogramowanie podmieniające numery kont • Oszustwa na portalach aukcyjnych • Oszustwa z wykorzystywaniem sms-ów premium • Szpiegostwo przemysłowe **Przestępczość przeciwko godności osobistej** • Mobbing elektroniczny (Cyber bullying) – agresywne zachowania wobec osoby podejmowane przez osobę lub grupę osób, przy wykorzystaniu telefonów lub Internetu • Mowa nienawiści (*hate speech)* w sieci
	BLOK TEMATYCZNY NR 2
11:45-13:00	**Socjotechnika jako narzędzie wykorzystywane przez cyberprzestępców – sposoby ochrony (jakich błędów unikać w celu zminimalizowania ryzyka skutecznego cyberataku)** • Najczęstsze i najbardziej skuteczne typu ataków socjotechnicznych (np. fałszywe e-maile) • Wykorzystywanie mediów społecznościowych (np. Facebook) • Ataki typu APT – długotrwałe, złożone i wieloaspektowe działania kierowane przeciwko konkretnym osobom, instytucjom, organizacjom i firmom **Podstawy prawne** • Jakie działania związane z cyberatakami kwalifikowane są jako przestępstwa • Jakie kary grożą za popełnianie cyberprzestępstw • Jakie prawa ma ofiara, która padła ofiarą cyberprzestępstwa **Jesteś 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**

	ZAJĘCIA WARSZTATOWE – STUDIUM PRZYPADKU
13:15-14:00	Podczas zajęć warsztatowych przeprowadzonych zostanie kilka demonstracyjnych prób dokonania cyberataku z wykorzystaniem socjotechnicznych „sztuczek" używanych przez przestępców. Uczestnicy szkolenia sprawdzą swoje zachowania przy próbie cyberataku. Warsztaty będą uwzględniały także kwestie związane z zabezpieczeniem dowodów cyberprzestępstwa oraz poinformowaniem odpowiednich służb.
	BLOK TEMATYCZNY NR 3
14:00-15:00	**Podstawy zarządzania bezpieczeństwem w instytucji pod kątem cyberzagrożeń** • Świadomość zagrożeń i konieczność przeciwdziałania im • Tworzenie, wdrażanie, utrzymanie oraz rozwój polityki bezpieczeństwa • Audyt systemów komputerowych w tym testy penetracyjne **Gdzie szukać informacji na temat skutecznej ochrony przed cyberatakami** • Poradniki i portale internetowe z aktualnymi informacjami o sposobach ochrony przed cyberatakami