CyberSA-B-25 - PNRR 1.5 - Cybersecurity: strategie e azioni di rafforzamento (Webinar)

Durata

4 ore

Modalità

In aula virtuale

Programma

Il Corso si inquadra nelle iniziative di Formazione e Security Awareness finanziate con risorse PNRR, Missione 1, Componente 1, Investimento 1.5 "Cybersecurity". Il Corso è destinato alle figure che hanno il compito di indirizzare e promuovere le azioni di rafforzamento della sicurezza informatica nell'ambito dell'Amministrazione.

Modulo 1: Contesto PA - Cybersecurity

Costo attuale del cybercrime:

- L'Italia sempre più nel mirino del cybercrime (tipologie di attacco più diffuse secondo il Rapporto Clusit 2024)
- Presentazione e analisi di casi noti di attacchi andati a segno in ambito Pubbliche Amministrazione - Case Study:
- Perché le PA sono nel mirino degli hacker?

Modulo 2: Phishing e Social Engineering

- Cos'è il Social Engineering
- Il Phishing e le sue varianti smishing, vishing e Qrishing
- Case Study: Elementi chiave per riconoscere una mail di Phishing attraverso la proposta di diversi esempi (simulazione interattiva in aula)

Modulo 3: Cyber Hygiene

- Clean Desk e Clear Screen
- La tutela degli asset aziendali
- Sicurezza dei laptop e dei dispositivi mobili (Dos and Don'ts)
- Sicurezza delle comunicazioni

Modulo 4: Esposizione e trattamento dei rischi

- Identificazione e gestione dei rischi
- Minacce interne – human factor
- Minacce esterne – attacco cyber malware/data breaches

Modulo 5: Identità Digitale

- Social Network, tutela identità digitale e dati personali (Video)
- Il ruolo delle password nella sicurezza informatica
- Dos and Don'ts
- Gestione delle Password
- Multifactor Authentication

Modulo 6: Normativa di riferimento

- NIS / NIS 2 – Soggetti coinvolti e Incident Reporting
- Misure minime di sicurezza ICT per le pubbliche amministrazioni (AgID)
- Nuovo Regolamento UE su Cybersicurezza e disegno Legge n. 1717/2024

Quiz di verifica dell'apprendimento