FORMAT S.R.L.
CENTRO STUDI RICERCHE E FORMAZIONE

CYBER SECURITY AWARENESS

PROGETTO AZIENDALE

Obiettivo del progetto è fornire al personale, sia pubblico che privato, le competenze necessarie per identificare e trattare le minacce associate all'uso delle tecnologie informatiche

Collaborano con noi

Avv. Michele Iaselli - Docente Informatica Giuridica Luiss, Membro LES, Coordinatore Comitato Scientifico di Federprivacy

Dr. Alfredo Visconti - Presidente ANDIP, Amministratore della Brain-It, Esperto di data quality e trattamento dei dati personali

Articolazione delle attività

Attività di servizi tecnico-consulenziali

❖ **Campagna di phishing, spear phishing, smishing, vishing**

Campagna di phishing, spear phishing, smishing, vishing simulato sulla popolazione aziendale al fine di valutare i rischi legati a questa tecnica di cyberattacco e il livello di sicurezza informatica dell'Azienda/Ente

❖ **Attività di valutazione della vulnerabilità**

La valutazione delle vulnerabilità consiste in un processo di revisione sistematica dei punti deboli della sicurezza riconoscendo, analizzando e dando priorità alle vulnerabilità esistenti nei sistemi o nei dispositivi IT, tracciando le minacce prevalenti nell'ambiente e raccomandare metodi di riparazione e mitigazione. Con le informazioni appropriate a portata di mano, i fattori di rischio possono essere facilmente determinati e possono essere definiti con competenza senza alcun ritardo.

1. Vulnerability assessment: ha lo scopo di individuare le vulnerabilità nell'infrastruttura informatica
2. Report vulnerabilità: produzione del documento con le vulnerabilità rilevate e valutazione delle remediation da mettere in atto.

Viene richiesta la possibilità di installare la piattaforma Net-Audit di Cybonet che poi verrà disinstallata al termine dell'attività.
Si richiede accesso remoto per un nostro specialista

❖ **Attività di Penetration Test**

È una strategia di valutazione delle minacce che prevede la simulazione di attacchi reali per valutare i rischi associati a potenziali violazione della sicurezza e viene definito anche hacking etico.

Attività Formazione

- 2 ore di formazione in webinar asincrono
- 2 ore di formazione in webinar live (si consigliano massimo 25/30 partecipanti)

Contenuti della formazione

✓ Cosa si intende per cybersecurity
✓ Il rischio informatico
✓ I reati informatici
✓ Le truffe informatiche: social engineering, phishing e spear phishing, smishing, vishing
✓ Le diverse tipologie di virus
✓ Cos'è un malware
✓ Come difendersi dai rischi provenienti dal web
✓ L'utilizzo di più dispositivi mobile: computer, portatile, telefono
✓ Le regole di sicurezza previste dal GDPR
✓ Le regole di sicurezza per il mondo internet e posta elettronica