CORSO CYBER SECURITY

OBIETTIVI CORSO:

- Imparare a riconoscere gli attacchi più frequenti.
- Fornire gli strumenti da utilizzare per la propria sicurezza.
- Imparare a proteggere i dati con mezzi e strumenti gratuiti.
- Adottare le strategie più idonee alla sicurezza aziendale.

CONTENUTI CORSO:

Introduzione al corso

- Cos'è un ethical hacker
- Cosa sono le certificazioni
- Red Team vs Blue Team

Situazione in Italia

- Cyber Crime
- Attacchi hacker
- La normativa NIS e GDPR
- Il rapporto CLUSIT
- Cyber Security RISKS
- Chi sono Autori degli Attacchi
- Data Breach

Deep e Dark Web

- Cos'è il Deep e Dark Web
- Com'è nato
- Come si naviga nel Dark Web
- TOR Browser

Terminologia Hacker

- Buffer Overflow
- Zero Day

- VA vs PT
- MITM
- HASH - Proxy

Fasi di Attacco

- Capire per potersi difendere
- Quali sono le fasi di un attacco
- Ricerca di una vittima
- Attacchi mirati e attacchi di massa

Information Gathering

- Dove gli hacker trovano le loro vittime
- Siete nel mirino degli hacker?
- Come scoprire se sei stato hackerato
- Strumenti di ricerca hacker

* Verranno mostrati e utilizzati alcuni degli strumenti che gli hacker utilizzano per trovare le proprie vittime - esempi pratici

Siti Web di ricerca

- Esercitazioni pratiche
- Utilizzo di TOR

Network Scanning

- Esercitazioni pratiche

Web Scanning

- Esercitazioni pratiche

Creare la cultura aziendale

- L'uomo è l'anello debole della catena aziendale
- Doveri dell'utente
- Le migliori pratiche da utilizzare

Le Password

- Perché sono importanti
- Come creare una password sicura
- La password che stai utilizzando è sicura?
- Le tecniche da evitare per creare le password
- Esempi e verifiche di password - esempi pratici
- Attacchi alle password - esempi pratici

Social Engineering

- Cos'è?
- Perché funziona
- Panoramica degli attacchi
- Strumenti utilizzati - esempi pratici
- Imparare a riconoscerlo ed evitarlo

Phishing

- Approfondimento del Phishing
- Esempi reali di attacchi
- Come riconoscerlo - esempi pratici
- Imparare a riconoscerlo ed evitarlo

Navigazione Sicura

- Panoramica e concetti di base
- Proxy cos'è e quando utilizzarlo
- Navigazione in incognito
- Utilizzo dei dati personali su internet
- Identikit del sito affidabile
- Pagamenti sicuri su Internet

Malware

- Panoramica e concetti di base
- Cosa sono e quali sono
- Cryptolocker e Cryptominer
- Ransomware Approfondimento - Esempi reali

- Wannacry
- Come difendersi

Macchine Virtuali

- Cosa sono?
- Hypervisor, VMware, Sandboxies, Virtualbox
- Macchine virtuali la sicurezza al nostro servizio
- Quando utilizzarle e perché

Non solo Macchine Virtuali

- Antivirus
- I migliori antivirus e perché
- Browser
- I migliori browser e perché
- Firewall
- Quando utilizzarli
- Quali e perchè

Attacchi RFID

- Cosa sono
- Come avvengono - Come difendersi

Smartphone

- Attacchi agli smartphone
- Android vs iOS quale il più sicuro?
- Le APP dello store sono sicure?
- Attenzione ai permessi
- Codici di sblocco da evitare

IoT - Internet of Thinks

- Cos'è?
- Sono sicuri?
- Panoramica e concetti di base
- Esempi

Wi-Fi

- È sicura?
- Panoramica e concetti
- Attacchi alla Wi-Fi
- WPS è sicuro?

Business Continuity

- La continuità dell'azienda
- Business continuity plan
- Il tempo è denaro ma ridurre i tempi costa
- Business continuity vs Disaster Recovery

Disaster Recovery

- Cos'è?
- Cosa fare
- Come procedere - Gli strumenti

Data Loss Prevention

- Cos'è?
- Gli strumenti
- Come evitarlo

Software

- Quali software utilizzare per il lavoro
- Open Source vs Proprietario
- Esempi e raccomandazioni

Incident Response

- Cos'è?
- Tipologie di incidenti
- Procedura di risposta all'incidente
- Backup Monitoraggio Ripristino

Backup

- Tecniche di backup
- Quale utilizzare – vantaggi e svantaggi
- RAID
- NAS vs Cloud

Altre tecniche di difesa

DMZ

- Cosa sono?
- Quando Utilizzarle

HoneyPot

- Cosa sono?

SaaS - Software as a Service

- Quando utilizzarli

NAC

- Cosa sono ?
- Quando servono

SIEM

- Cosa sono
- Quando servono

Conclusione del corso

- Considerazioni
- Domande

Test Finale

Il test prevede una serie di domande e risposte a tempo.

Al termine del quale con un punteggio di almeno 70% delle risposte corrette verrà rilasciato un attestato di frequenza.