Corso: RICONOSCERE LE E-MAIL PERICOLOSE E AGIRE IN SICUREZZA

(Guida alla "sicurezza" informatica)

CORSO A CURA DI **ASSET MANAGEMENT S.r.l. –** DOCENTE **GIORGIO SBARAGLIA**

DURATA ORE 9,00 – 18,00

28 NOVEMBRE2018

DOVE SI TIENE IL CORSO

Sede ASSET – GI GROUP Milano, Palazzo Del Lavoro, Piazza 4 Novembre 5 (zona Stazione Centrale)

OBIETTIVI

Il corso permette di imparare a riconoscere le modalità di cyber attacco più frequenti; fornisce a utenti già esperti la conoscenza degli strumenti da utilizzare per la propria sicurezza informatica. Consente inoltre di imparare a proteggere i dati con una gestione evoluta delle password.
Metodologia attiva intervallata da lecture interattive e esercitazioni pratiche.

PROGRAMMA

Come è cambiato il Cybercrime negli ultimi anni

- Panoramica sul cyber crime: la crescita del Phishing e del Social Engineering.
- Il Cyber warfare, la guerra cibernetica: i casi Natanz (Iran) e Ucraina
- Il Deep Web, il Dark Web, i black market, la rete TOR e il Bitcoin: cosa sono e come vengono usati
- Hacker, cracker, black hat, white hat: che differenza c'è? Cosa vogliono da noi i criminali informatici

Panoramica sulle principali tecniche di cyber attacco

- Gli attacchi DDoS e le Botnet
- IoT: il lato vulnerabile dell'Internet delle Cose
- APT (Advanced Persistent Threat)
- Attacchi "man-in-the-middle". Il protocollo HTTPS
- La vulnerabilità dei siti web: i rischi di WordPress e dei CMS open source

Phishing, Ransomware e Social Engineering

- Cos'è il Social Engineering
- La crescita esponenziale del phishing e lo Spear phishing
- I Ransomware: la minaccia oggi più temibile
- Cosa fare se siamo stati colpiti da un ransomware: le opzioni possibili

- Implicazioni giuridiche per le vittime dei ransomware
- Responsabilità per il dipendente che causa un attacco ransomware aziendale

I rischi sui device mobili

- Gli Spyware negli smartphone: alcuni attacchi famosi
- Come operano gli spyware
- I sintomi: come capire se il telefono è stato colpito
- Gli strumenti per violare gli smartphone: come viene fatta l'estrazione dei dati da un dispositivo
- L'acquisizione attraverso il backup
- La vulnerabilità delle reti WI-FI

Email e sistemi di Messaggistica istantanea (IM)

- Gli attacchi attraverso la posta elettronica
- Business Email Compromise (BEC): che cosa è e quanti danni sta causando nelle aziende. Le truffe "The Man in the Mail" e "CEO fraud"
- L'email non è uno strumento sicuro: lo spoofing
- La crittografia dell'email: PGP (Pretty Good Privacy)
- PEC e posta crittografata: caratteristiche, utilizzi e differenze
- Messaggistica istantanea (IM): WhatsApp, Telegram, Messenger, Signal. Quali sono gli strumenti di Messaggistica più sicuri

La crittografia

- Perché la crittografia ci riguarda tutti
- Un po' di storia: dal cifrario di Cesare alla macchina Enigma ad Alan Turing
- Crittografia simmetrica (a chiave singola)
- Crittografia asimmetrica a chiave pubblica/privata (Diffie-Hellman)
- Advanced Encryption Standard (AES)

L'importanza delle Password

- Come gli hacker riescono a violare i nostri account (più facilmente di quello che crediamo)
- La corretta gestione delle Password sicura e gli errori da evitare
- Le "domande di sicurezza"
- I Password Manager: quali scegliere e come usarli. Il Password management nelle aziende
- L'autenticazione a due fattori: una sicurezza ulteriore
- Come gestire correttamente il Backup. NAS e sistemi RAID: cosa sono e come usarli per conservare in sicurezza i nostri dati

I rischi aziendali

- La "deperimetralizzazione": il "Teorema del Fortino"
- Il pericolo arriva soprattutto dall'interno
- I rischi causati dagli utenti interni: malicious insider, utenti compromessi e accidentali

Conclusioni: come possiamo difenderci

- I sistemi più avanzati per proteggerci: l'analisi comportamentale
- L'importanza degli aggiornamenti di sicurezza
- Le verifiche periodiche di sicurezza: Vulnerability Assessment e Penetration Test

- Che cos'è la ISO/IEC 27001 e come si collega e si integra con il GDPR (General Data Protection Regulation)
- Acquisire Consapevolezza: la miglior difesa è sempre l'uomo

DESTINATARI

Il corso è destinato a tutti coloro che hanno necessità di acquisire competenze di base nell'ambito della sicurezza informatica.

QUOTE

Il costo del corso per i Non Soci è di 300 euro + IVA
Per i Soci Assologistica e Assologistica Cultura e Formazione come da condizioni previste

La quota include materiali didattici e invio per e-mail delle slide di approfondimento

Per diventare Soci Assologistica o Assologistica Cultura e Formazione
chiedere info : tel.02/6691567 - 02/6690319 email: culturaformazione@assologistica.it

SI PREGA DI VISIONARE IL REGOLAMENTO CORSI SU:
WWW.ASSOLOGISTICACULTURAEFORMAZIONE.COM
- SEZIONE CORSI -