CYBERCRIME, I PERICOLI DEL WEB
Corso avanzato sulla sicurezza informatica

Data: Martedì 30 maggio 2017 (8 ore)

Sede: Federmanager Reggio Emilia, Via Paolo Borsellino 2, 42124 Reggio Emilia (RE)

Orario: 9.00-18.00

Per informazioni e iscrizioni:

Federmanager Academy: Marialuisa Lusetti
Tel. 0644070231
Tel. 3391262280
e-mail: marialuisa.lusetti@federmanageracademy.it; info@federmanageracademy.it

Federmanager Reggio Emilia
Tel. 0522 280385
e-mail: segreteria@federmanager.re.it

PREMESSA

Pur non essendovi propedeuticità, **il corso avanzato** sulla sicurezza informatica **si pone in continuità con** la giornata formativa curata dall'Ing. Giorgio Sbaraglia che si terrà presso **Federmanager Bologna** il **12/5/2017** dal titolo **"IL WEB È DIVENTATO UN LUOGO PERICOLOSO? POSSIAMO DIFENDERCI!"**.

CONTENUTI

Come è cambiato il Cybercrime negli ultimi anni

- Il 2016 è stato l'annus horribilis per la cyber security.
- 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 attacco cyber

- 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.
- I Keylogger.
- La vulnerabilità dei siti web: i rischi di WordPress e dei CMS open source.

Phishing, Ransomware e 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.
- Cos'è il Social Engineering.
- Gli attacchi ai devices mobili. Gli Spyware.
- La vulnerabilità delle reti WI-FI.

Email e sistemi di Messaggistica istantanea (IM)

- Gli attacchi attraverso la posta elettronica.
- La truffa "The Man in the Mail".
- L'email non è uno strumento sicuro: lo spoofing.
- La crittografia dell'email: PGP (Pretty Good Privacy).
- Messaggistica istantanea: WhatsApp, Telegram, Messenger, Signal.

La crittografia

- 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).
- Funzioni di hash: MD5, SHA-1 e SHA-2.

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.

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.
- Acquisire Consapevolezza: la miglior difesa è sempre l’uomo.

Approfondimenti ad hoc, definiti in sede di workshop in base alle richieste dei partecipanti

OBIETTIVI

In questo corso verranno trattati argomenti avanzati di Sicurezza Informatica, per utenti evoluti.
Nessuno oggi può prescindere dal considerare la Cyber Security come elemento strategico per la difesa dei dati della propria azienda o del proprio studio professionale. Perché se un’azienda perde i propri dati non è più nulla.
L’evoluzione del cybercrime ha sostituito l’hacker con vere e proprie organizzazioni criminali dotate di grandi mezzi ed in grado di portare attacchi a chiunque. Non è un problema di sapere “se verremo attaccati” ma solo “quando saremo attaccati”. Non importa se siamo grandi o piccoli: prima o poi ci attaccheranno.
I mezzi per difenderci già esistono: quello che manca è la consapevolezza del problema e la conoscenza degli strumenti più idonei da adottare per proteggerci. I principali obiettivi della giornata formativa sono:

- Imparare a riconoscere le modalità di cyberattacco più frequenti
- Fornire ad utenti già esperti la conoscenza degli strumenti da utilizzare per la propria sicurezza informatica.
- Imparare a proteggere i dati con una gestione evoluta delle password.

DESTINATARI: Manager, Imprenditori, Professionisti, Responsabili IT, Security Manager e quanti operano nella gestione dei dati informatici e telematici riservati e/o critici per l’erogazione dei servizi o del business.

DOCENTE: **Giorgio Sbaraglia**, Ingegnere, ha ricoperto per molti anni la funzione di Direttore Acquisti presso una grande società di costruzioni e, precedentemente, presso

aziende metalmeccaniche e manifatturiere del territorio. Appassionato e conoscitore dei temi di sicurezza informatica in azienda, svolge attività di consulenza aziendale ed in collaborazione con diverse società di formazione, tiene corsi di formazione in materia di Cyber Security. È membro del CLUSIT (Associazione Italiana per la Sicurezza Informatica).