NEXTON

Business Digital Coaching

WORKSHOP

Information Security

Protezione del Patrimonio Informativo Aziendale e del suo Business

Obiettivo del Workshop

In questo corso verranno trattati argomenti alla base della Sicurezza Informatica e dunque del business.
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. 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.
Non serve essere dei "geni" dell'informatica per riuscire a difendersi: basta acquisire la consapevolezza ("awareness") dei rischi e saperli riconoscere. In una parola: "usare la testa".

In particolare:

- Fornire strumenti e strategie per la sicurezza informatica in azienda e nella pratica di ogni giorno, anche per non specialisti IT, ma semplici utilizzatori.
- Conoscere le tecniche di social engineering ed il phishing (attraverso computer e smartphone).
- Imparare a riconoscere i ransomware e malware più comuni oggi sul web e ad evitarli.
- Imparare a scegliere ed usare le password per proteggere i dati.

A chi è rivolto

Il seminario è rivolto a responsabili dei sistemi informativi, responsabili dell'information security, direttori dell'organizzazione, risk manager, direttori dell'ufficio legale, membri del board, membri dell'organismo di vigilanza, direttori generali, amministratori delegati, e più in generale a tutte le figure apicali con funzioni di responsabilità.

Modalita'

- Location: presso sede del Cliente
- Ambiente: predisposizione di PC, proiettore
- Durata: 8 ore
- Materiali: i contenuti presentati saranno rilasciati in formato PDF.

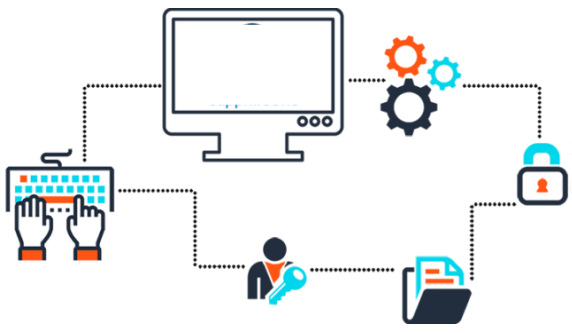
Docente

Giorgio Sbaraglia

Ingegnere, dopo esser stato per molti anni dirigente in una grande società di costruzioni italiana, svolge oggi attività di consulenza e formazione per la sicurezza informatica, ISO 27001, Risk Management e per il GDPR.
Tiene corsi su questi temi per molte importanti società italiane di formazione, tra le quali la Business School de Il Sole 24 Ore.
È membro del CLUSIT (Associazione Italiana per la Sicurezza Informatica) e certificato "Innovation Manager" da RINA.
È autore dei libri: "GDPR kit di sopravvivenza" (Editore GoWare) e "Cybersecurity kit di sopravvivenza. Il web è un luogo pericoloso. Dobbiamo difenderci!" (Editore GoWare).
Scrive per CYBERSECURITY360 testata specialistica del gruppo Digital360 per la cybersecurity.

Contenuti

- **L'evoluzione del Cybercrime**
  - I dati del crimine informatico nell'Italia e nel mondo: il rapporto CLUSIT 2018.
  - Cyberwarfare, la guerra cibernetica: casi famosi.
  - Deep Web, Dark Web, rete TOR e Bitcoin: cosa sono e perché ci riguardano.
  - I danni economici generati alle aziende.
  - I problemi ed i rischi nelle PMI e negli studi professionali.
- **Social Engineering, Phishing e Ransomware**
  - Cos'è il Social Engineering.
  - La crescita esponenziale del phishing e lo Spear phishing: le tecniche d'attacco.
  - I Ransomware: cosa sono e come ci attaccano.
  - Alcuni attacchi famosi: da WannaCry a Petya.
  - Come difendersi dai Ransomware.
  - Sono stato colpito da un Ransomware: cosa fare ora?
  - Implicazioni giuridiche per le vittime dei ransomware.
- **Gli attacchi attraverso i dispositivi mobili**
  - Gli attacchi ai devices mobili. Gli Spyware.
  - I sintomi: come capire se il telefono è stato violato.
  - La vulnerabilità delle reti WI-FI.
  - Messaggistica istantanea: WhatsApp, Telegram, Messenger, Signal. Ci possiamo fidare?
- **I rischi e le vulnerabilità delle email**
  - Gli attacchi attraverso la posta elettronica.
  - La 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: che cosa è la PGP (Pretty Good Privacy).
- **Imparare ad usare le Password**
  - Gli strumenti (sempre più potenti) degli hackers: alcuni famosi casi di attacchi e "data breach".
  - La sicurezza di un Account dipende dalla forza della password.
  - Le regole per una Password sicura e gli errori da evitare.
  - Le "domande di (in)sicurezza".
  - I Password Manager.
  - L'autenticazione a due fattori (MFA: Multi factor authentication).
- **Mettere in pratica la Cyber Security**
  - Il tramonto degli Antivirus: ormai non ci proteggono più. Il polimorfismo.
  - I sistemi di protezione avanzata più efficaci: User Behavior Analytics (UBA).
  - L'importanza del Backup: 3-2-1 Backup Strategy.
  - La Sicurezza Informatica come "Gioco di squadra".



NEXTON

Business Digital Coaching

Milano, Bologna, Ravenna, Modena, Mantova

www.next-on.eu

contact@next-on.eu