INTRODUZIONE ALLA CYBERSECURITY

PREMESSA

In un'azienda di oggi la gestione della sicurezza ICT non si può limitare soltanto ai sistemi informatici, ma tenere conto del fatto che la maggior parte di tutte le operazioni, sia amministrative, sia di produzione, si svolgono grazie ai sistemi ICT. Diventa quindi fondamentale che manager, decisori e operatori d'ufficio siano adeguatamente resi consapevoli delle problematiche di sicurezza che coinvolgono il loro lavoro per poter disegnare le procedure operative tese a minimizzare il rischio, che dovranno inserirsi entro il normale modus operandi del loro lavoro, con l'impatto minimo sul business.

OBIETTIVI

Il presente corso parte da una analisi del ruolo delle tecnologie ICT dentro i vari settori dell'azienda. Il corso prosegue con la presentazione delle minacce più importanti degli ultimi anni e con le metodologie operative necessarie per ridurre il rischio ad esse associato. Poi vengono presentati i modelli di difesa, come definiti sia negli standard internazionali come ISO27001, sia nelle direttive italiane di AgID (Agenzia Italia Digitale), per infine calarli nel contesto operativo dell'azienda specifica.

DESTINATARI

Dirigenti, coordinatori d'area, personale operativo che svolge operazioni potenzialmente a rischio di attacco cyber

ARGOMENTI

Le tecnologie in azienda

- Processi e procedure: l'attività quotidiana del lavoro
- Le tecnologie ICT
- Le tecnologie OT
- Le tecnologie IoT
- Il ruolo delle persone rispetto alle tecnologie
- Visione olistica integrata: esempi di dipendenze incrociate

Casistiche di sicurezza

- Obiettivi di un attacco
- Il modello di sicurezza a strati o a cipolla
- Attacco di massa e indiretto
- Attacco diretto
- Rubare le identità elettroniche
- Malware come arma specifica di attacco
- Chi sono gli attaccanti
- Il ruolo del personale interno
- La minaccia del social engineering
- Il modello No-Trust
- I rimedi

Proteggere i dati

- Concetti base di crittografia
- La crittografia simmetrica
- La crittografia asimmetrica
- Applicazioni della crittografia
- Proteggere dalle alterazioni

Controllare i sistemi

- Strumenti tecnici per controllare i sistemi
- Il processo di accounting
- Pianificare controllo e osservazione

Il processo di difesa

- La privacy post GDPR
- Sicurezza globale delle informazioni: ISO27001:2017 e le sue metodologie (ISO27002)
- La protezione dei sistemi: la direttiva EU NIS (D.lgs 65/2018)
- Analisi del rischio: ISO31000:2018
- Vulnerability assessment
- Analisi delle dipendenze incrociate
- Usare il PDCA per il miglioramento continuo
- La sicurezza: un processo di evoluzione continua

DURATA

Un giorno