La Gestione della Sicurezza delle Informazioni a Tutela del Patrimonio Aziendale

01 GIORNO

OBIETTIVI

Nell'ultimo decennio si è assistito ad un forte trend di "digitalizzazione" di molti processi di business sia interni all'azienda che nell'interazione tra l'azienda e le sue controparti. I processi sono sempre più dipendenti da asset informatici (dati, applicazioni, infrastrutture). In tale contesto il cyber risk inizia ad essere considerato uno dei rischi più critici ed impattanti per le aziende. Un rischio da comprendere, gestire e trasformare in leva competitiva, con una strategia di consapevolezza diffusa all'interno di tutta l'organizzazione aziendale e non più unicamente demandato ai soli direttori tecnici. Il corso analizza lo scenario dei rischi cyber a cui le aziende sono esposte, il profilo degli attaccanti, il potenziale impatto, le azioni strategiche e tattiche da attuare per la corretta gestione di essi.

"Non possiamo azzerare la probabilità di un incidente ma possiamo ridurla e renderne il suo impatto accettabile!"
PAMELA PACE

PROGRAMMA

Il valore delle informazioni
- Il valore delle informazioni nella storia
- Il valore della conservazione delle informazioni
- Il valore economico delle informazioni
- Il potere delle informazioni
- Le informazioni quale asset aziendale
- Il Secolo delle informazioni
- Le informazioni: un patrimonio da proteggere

I rischi a cui le aziende sono esposte
- Il cyber risk nel panorama dei rischi mondiali
- Il profilo degli attaccanti:
  - chi sono
  - come agiscono
  - quali sono i loro obiettivi
  - le motivazioni
  - i bersagli
  - i ritorni
  - la provenienza "geografica"
  - i costi di un attacco
- Le tipologie di attacchi:
  - Social Engineering
  - Fake news
  - Malware, Spyware etc.
  - Spionaggio industriale
  - Hacking
  - Activism
  - Insider

Miti da sfatare
- Perché dovrebbero attaccare proprio noi che riteniamo di non avere asset sensibili
- Esternalizziamo i servizi (es. affidarsi al cloud)
- Proteggersi è inutile
- La cyber security è un problema tecnologico
- A cosa serve la compliance

Perché è sicuro che saremo attaccati
- Diffusione sempre più massiccia del digitale nei processi di business
- Dipendenza sempre più diffusa dalle tecnologie in ogni ambito operativo, produttivo, privato, ecc.
- Insufficiente conoscenza del tema nelle organizzazioni
- Scarsa sensibilità del top management
- Mancanza di coscienza dei rischi a cui si è esposti
- The hacking economy

Gli impatti
- Rischi a cui si è esposti
- Il brand
- Perdite e danni diretti e indiretti
- Gli aspetti legali
- I profili di responsabilità dell'azienda, del board, degli amministratori, dei direttori tecnici

Le azioni strategiche e tattiche da intraprendere
- Nosce te ipsum
- Misurati
- Identifica e indirizza il percorso
- Diffondi competenze, metodo e consapevolezza
- Technology focused vs Risk driven
- Cyber risk management strategy e framework della cyber security

IN COLLABORAZIONE CON
Objectivc Technology

PARTECIPANTI

Il seminario è rivolto a responsabili dei sistemi informativi, responsabili dell'information security, direttori finance, 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.

EDIZIONI

2019

Milano, 15 Febbraio
Milano, 17 Maggio
Milano, 15 Novembre

ISCRIZIONI

SINGOLA € 600 (+IVA)
per l'iscrizione di un partecipante

MULTIPLA -15% a persona per:
- 2 o più iscritti alla stessa edizione del corso
- 9 o più iscrizioni nell'arco di 12 mesi a diversi corsi a catalogo

COME ISCRIVERSI

+39 02 38010666
+39 02 38010871
www.scuoladipaloalto.it
informazioni@paloaltoscuola.it