Cyber Security: Minacce e Criteri di Protezione

Il cyberspace è oggi il termine più utilizzato per indicare le dimensioni digitali della società dall'avvento di Internet. Per chi opera a garanzia degli interessi nazionali di un Paese o di una Industria è necessario impostare una propria politica di cyber security che oltre alle tecnologie affronti aspetti sociali, legali ed economici. Le minacce coinvolgono diversi attori. Istituzioni, Industria privata, Cittadini sono vulnerabili e il Cyber Crime può operare acquisendo informazioni riservate e/o delicate da utilizzare per attaccare infrastrutture critiche di vitale importanza o beni tangibili di singoli. Il cyberspace, secondo l'approccio militare, ha la dimensione di un vero campo di battaglia e come tale ci si muove con tecniche di intelligence (Cyber War). Lo scenario internazionale ed italiano si analizza sia in termini legislativi che di processi organizzativi e tecnologici per il contrasto al crimine, unitamente al livello di consapevolezza da parte dei vari settori sia istituzionali che privati di essere obiettivi sensibili e rischiare di poter subire notevoli perdite in termini economici e tecnologici. Gli elementi in gioco sono le infrastrutture critiche, gli asset esposti ai rischi di attacchi cyber in varie tipologie, i danni causati e potenziali, i valori economici in gioco. La cyber security, infatti, non è solo un'esigenza ma anche un'opportunità in termini di capacità industriali e di ricerca.

Agenda (3 giorni)

Quadro di riferimento:

Cyber Security Standard
infrastrutture critiche nazionali ed estere identificate, team di difesa e loro differenze (CERT, CSIRT, ecc.)
report ed evidenze su tipologia, target e danni economici causati dagli attacchi informatici (cyber attacks)
situazione internazionale in USA, Unione Europea e in Italia anche dal punto di vista normativo
enti e operatori coinvolti nel governo del Cyber Space e nelle misure di protezione e nelle strategie nazionali
misure di protezione, di difesa, di resilience e "proattive" per la prevenzione ed il contrasto del Cyber Crime
indicatori del livello di consapevolezza, difesa, interdipendenza transnazionale e propensione agli investimenti in sicurezza
analisi delle tecniche di protezione tradizionali ed emergenti e delle minacce correlate (CyberCrime).

Obiettivi

Acquisire gli elementi principali sugli aspetti normativi, regolatori, sugli standard di riferimento.

Avere evidenze della situazione internazionale e nazionale in merito dimensione del fenomeno, alle minacce, agli attacchi di tipo Cyber ed ai criteri di protezione.

Analizzare le principali tecniche di attacco e di difesa in funzione del contesto.

Individuare le infrastrutture potenziali obiettivi, le strutture e i centri di prevenzione e di risposta ed il grado di esposizione al rischio degli asset tangibili e non.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili IT, Security Manager, Forze dell'Ordine e quanti operano nella gestione dei dati informatici e telematici riservati e/o critici per l'erogazione dei servizi o del business.

Prerequisiti

Conoscenze di base di informatica e di telecomunicazioni.

Iscrizione

Quota di Iscrizione: 1.790,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza

80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com