Data Privacy e Data Protection nelle Infrastrutture Critiche nazionali

Il trattamento, la riservatezza e la protezione dei dati personali, sensibili, particolari o comunque "critici" per le infrastrutture nazionali presenta rischi elevati e specifici. La normativa che tutela la privacy i diritti e le libertà fondamentali, le leggi in materia di sicurezza nazionale, antiterrorismo, antifrode, anticontraffazione si trovano sovente in parziale sovrapposizione. Se poi tali informazioni risiedono all'interno di asset e infrastrutture nazionali ecco che queste ultime divengono obiettivi "sensibili" del cyber crime. La giurisprudenza italiana, le leggi promulgate e modificate in virtù di emergenze nazionali (cfr. terrorismo, crimini informatici, ecc.), il prossimo "Regolamento Europeo in materia di protezione dei dati", individuano misure da applicare a protezione di Cyber attacchi sempre più sofisticati e diversificati. Il fenomeno dei social network e la geolocalizzazione dei terminali impone nuove metriche e strumenti per proteggere ambienti e asset tangibili e virtuali.

Agenda (3 giorni)

Quadro di riferimento:

infrastrutture critiche nazionali e loro interdipendenza
normativa nazionale in materia di riservatezza e trattamento delle informazioni
direttiva e regolamento europeo per la protezioni dei dati
reati informatici : Terminologie e tipologie di attacchi
CyberSecurity: scenari evolutivi, Minacce e Vulnerabilità
rapporto tra terminali e reti
differenze tra Architetture Informatiche

Home Protection, Work Protection
Social Media ed entertainment (web reputation, digital identity)
payment (phone, Laptop, Smartphone, tablet)
sicurezza delle applicazioni
criteri di protezione e livello di controllo tecnologico utilizzato nei processi
gestione del rischio , conformità e governo delle infrastrutture
misure di sicurezza logiche, fisiche e organizzative.

Obiettivi

Individuare le Infrastrutture Critiche Nazionali e i Centri preposti al controllo (CERT, CSIRT, ecc.).

Acquisire le conoscenze di base della normativa in materia di riservatezza e protezione dei dati.

Analizzare gli scenari tecnologici evolutivi e le tipologie di attacchi.

Confrontare i principali criteri di protezione con il livello di rischio residuo accettato.

Destinatari e Prerequisiti

A chi è rivolto

Chief Security Officer, Data Protection Officer, Consultant Privacy, Responsabili IT, Security Manager, Incaricati al trattamento, e quanti operano nella gestione dei dati informatici e telematici.

Prerequisiti

Conoscenze di base di informatica e di telecomunicazioni.

Iscrizione

Quota di Iscrizione: 1.640,00 € (+ 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