Sicurezza di rete: firewall, IPS e VPN

Uno dei problemi più importanti nei sistemi informativi aziendali è la protezione del proprio sito da attacchi esterni provenienti da Internet. Le prime azioni di difesa sono affidate ai "Firewall", che controllando i punti di accesso minimizzano il rischio di accessi non autorizzati. Per integrare le funzionalità del Firewall e soprattutto per ridurre il rischio di attacchi provenienti dall'interno si può aggiungere il controllo eseguito dagli IDS/IPS, che esaminano il traffico alla ricerca di azioni illecite e/o di codice malevolo.Il corso si conclude con l'esame delle diverse soluzioni di reti private virtuali che, utilizzando una infrastruttura pubblica, permettono di interconnettere i siti su base geografica.Il corso offre una visione d'insieme delle tematiche connesse alla sicurezza dei sistemi e delle reti.

Agenda (4 giorni)

La sicurezza in Internet/Intranet: analisi dei principali requisiti di sicurezza e delle minacce delle reti TCP/IP.

Tecnologie di firewalling e meccanismi di funzionamento:

descrizione delle funzionalità di base di un firewall
progettazione della politica di sicurezza di un firewall
tipologie di firewall (Packet filter, Application proxy, stateful) e loro campi di impiego.

Funzionalità accessorie di un firewall:

Network Address Translation (NAT), Port Address Translation (PAT)
Virtual Private Network (VPN)
High availability, load balancing.

Selezione di prodotti di firewalling:

Rassegna dei principali prodotti di firewalling commerciali
Rassegna dei principali prodotti in libera distribuzione
Linee guida sulla selezione di un prodotto di firewalling.

Architetture implementative di firewalling:

modelli architetturali per la protezione di una Intranet da reti esterne interconnesse (Internet, altri Sistemi informativi)
modelli architetturali per la realizzazione di aree protette all'interno della Intranet
architetture per l'alta affidabilità/load balancing.

Intrusion prevention system:

IDS ed IPS
descrivere come i sensori possono limitare gli attacchi
conoscere i parametri di sistema essenziali
analizzare gli eventi e sintonizzare un sensore.

Reti private Virtuali (VPN):

protocollo IPSec, tunnel e transport mode, main e aggressive mode.

Obiettivi

Al termine del corso i partecipanti sono in grado di comprendere e saper utilizzare gli apparati di rete per garantire il livello di sicurezza richiesto.

Destinatari e Prerequisiti

A chi è rivolto

Tecnici che operano nell'ambito della protezione delle reti e dei sistemi di elaborazione, personale preposto alla pianificazione e/o progettazione di sistemi di sicurezza informatica.

Prerequisiti

Buona conoscenza della suite di protocolli TCP/IP.

Iscrizione

Quota di Iscrizione: 1.840,00 € (+ 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

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