

SICUREZZA INFORMATICA NELLE PICCOLE RETI

Obiettivi

Sarebbe sbagliato pensare che una piccola azienda possa accontentarsi di una piccola sicurezza. Anche se le esigenze e le risorse disponibili per le PMI o le aziende SOHO sono molto differenti rispetto ad un ambito corporate, è comunque irrinunciabile poter contare su quel bagaglio di competenze tecnico-informatiche utile a garantire il mantenimento di una standard di sicurezza soddisfacente. Il corso mira a fornire ai tecnici e agli amministratori di rete di queste piccole realtà le competenze di base per affrontare tutte le più frequenti minacce informatiche e renderli in grado di prevenirle erogando servizi sicuri.

Destinatari

Aziende SOHO/SME; tecnici e amministratori di rete di piccole o medie dimensioni.

Prerequisiti

Conoscenze **di base** di sistemi Windows e Linux e del funzionamento delle reti.

Contenuti

- Introduzione al corso
- Il problema della sicurezza
- I servizi di sicurezza
- Sicurezza fisica
- Protocolli e servizi di rete
- Regole di firewalling e routing
- Utilizzo di iptables
- Configurazione di un firewall: esercitazione
- Scansioni e attacchi comuni
- IDS / IPS
- Definizione delle policy aziendali
 - Gestione dei log
 - Protezione degli storage
 - Politiche e strumenti per i backup
 - Gateway applicativi
 - Gestione delle password
- Hardening dei sistemi
 - Criteri locali
 - Personal firewall
 - Amministrazione remota
 - Distribuzione delle patch
- Attacchi nella rete locale e loro individuazione
 - Scansione ed enumerazione
 - Sniffing
 - Man-in-the-middle
- Sicurezza delle reti Wi-Fi
 - Installazione di una WLAN
 - Problemi della tecnologia WiFi
 - Hardening e monitoraggi perimetrali

- Scansioni e attacchi comuni, individuazione e contrasto
- Esercitazione
- Esposizione dei servizi
 - DMZ
 - Accessi tramite VPN
- Attacchi remoti
 - Scansione ed enumerazione
 - Sfruttamento di configurazioni errate
 - Exploiting
 - Social engineering, phishing e pharming
- Virus e worm: descrizione, catalogazione, funzionamento
 - Spyware, Adware e altre minacce
 - Difese, prevenzione, individuazione e rimozione
- Crittografia simmetrica e asimmetrica
- Il funzionamento dei certificati
- Usi della firma digitale
- Esercitazioni pratiche:
 - Installazione e configurazione di un firewall Linux
 - Installazione di una Certification Authority
 - Installazione, configurazione e messa in sicurezza di servizi comuni