Sicurezza dei sistemi e delle reti - Implementazione

Protezione efficace di hardware e dati

A distanza

5 giorni (35 Ore)

Open : 2.995,00 € +IVA
Packaged in azienda : 6.890,00 € +IVA +10% di Project Management (Quota riferita ad un gruppo di 10 pax max)
Customized : Su richiesta

WebCode: IT.22

La protezione dei dati aziendali richiede una politica di sicurezza in grado di **resistere a tutte le minacce esterne.** Lungi dall'essere un campo specifico, la sicurezza deve essere presa in considerazione sia per le apparecchiature di rete che per i sistemi. Pur non essendo un esperto, l'amministratore non deve infatti ignorare i rischi e deve essere in grado di **implementare un'architettura di sicurezza** che soddisfi i requisiti dell'azienda.

A chi è rivolto

Per chi

Chi si occupa della sicurezza di un sistema informativo o opera in rete o predispone server aziendali

Prerequisiti

Nessuno

Programma

1 - L'ambiente

- Il perimetro (reti, sistemi operativi, applicazioni)
- Gli attori (hacker, responsabile della sicurezza, auditor, siti di sicurezza)
- I rischi
- Protezione
- Prevenzione
- Rilevamento

2 - Attacchi

- Intrusioni di livello 2: a livello dello switch di accesso o del punto di accesso wireless
- Intrusioni di livello 3 (IP): IP spoofing, Denial of Service, scan, man-in-the-middle, applicazioni strategiche (DHCP, DNS, SMTP, ecc.), applicazioni rischiose (HTTP/HTTPS, ecc.)
- Attacchi logici: virus, worm, Trojan horse, spyware, phishing, password cracking, ransomware, crypto locker
- Attacchi applicativi: al sistema operativo o alle applicazioni (buffer overflow)

3 - Protezione

- A livello di switch di accesso: port security, utilizzo del protocollo 802.1x (NAC), VLAN Hopping, DHCP Snooping, IP source guard, ARP spoofing, filtro BPDU, root guard
- A livello wireless: implementazione di una chiave WEP, WPA, WPA2, WPA3
- A livello di IP: firewall layer7, firewall specializzati, su router, state full (ispezione dei livelli superiori a 3), UTM, proxy
- Protezione contro gli attacchi logici: antivirus, EDR, XDR, MDR e SOC
- Protezione dagli attacchi alle applicazioni: hardening delle piattaforme Microsoft e Linux, validazione delle applicazioni

4 - Monitoraggio e prevenzione

- Sonde IDS
- Log server/SIAM
- IPS: enclosure dedicate, funzionalità firewall

5 - Esempi di architetture

- Esempio di azienda monosede
- Collegamento di utenti mobile
- Esempio di azienda multisito

6 - Sicurezza degli scambi, crittografia

- Lo scopo della crittografia e le funzioni di base
- Algoritmi simmetrici
- Algoritmi asimmetrici
- Algoritmi hash
- Metodi di autenticazione (pap, chap, Kerberos)
- L'HMAC e la firma elettronica
- Certificati e PKI
- Protocolli IPSEC, SSL
- VPN site-to-site e mobile Zero Trust Network Access (ZTNA)

Obiettivi del corso

- Sapere come progettare e implementare un'architettura di sicurezza appropriata
- Essere in grado di implementare i principali mezzi per proteggere le reti
- Avere un primo approccio alla protezione dei server
- Scoprire come la crittografia sia utile per proteggere gli scambi di informazioni

Esercitazioni

- Una formazione molto **pragmatica**: i partecipanti vengono portati ad implementare la sicurezza di una rete aziendale attraverso tanti esempi pratici
- Un punto preciso sugli **obblighi di legge** in tema di sicurezza
- La rassegna delle **soluzioni** disponibili sul mercato

Date 2026

Ultimi posti Edizione garantita

dal 11 mag al 19 mag
- dal 11 mag al 13 mag
- dal 18 mag al 19 mag

dal 19 ott al 27 ott
- dal 19 ott al 21 ott
- dal 26 ott al 27 ott