CAPITOLO 8 – SICUREZZA DELLE RETI INFORMATICHE

Obiettivi del Capitolo

Al termine di questo capitolo il corsista sarà in grado di:

- Comprendere i principi fondamentali della sicurezza informatica.
- Identificare le principali minacce alle reti.
- Comprendere il funzionamento di malware e attacchi informatici.
- Conoscere le tecnologie di protezione delle infrastrutture.
- Comprendere il ruolo di firewall, VPN, IDS e IPS.
- Applicare le principali buone pratiche di cybersecurity.
- Analizzare semplici scenari di sicurezza aziendale.

8.1 Introduzione alla sicurezza delle reti

La sicurezza informatica comprende tutte le misure tecniche, organizzative e procedurali adottate per proteggere:

- dati;
- dispositivi;
- applicazioni;
- reti;
- servizi digitali.

Negli ultimi anni l'aumento delle minacce informatiche ha reso la cybersecurity una priorità strategica per aziende, pubbliche amministrazioni e organizzazioni di qualsiasi dimensione.

Un incidente informatico può causare:

- perdita di dati;
- interruzione delle attività;
- danni economici;
- danni reputazionali;
- sanzioni normative.

8.2 La triade CIA

Uno dei concetti fondamentali della sicurezza informatica è la triade CIA.

CIA significa:

- Confidentiality
- Integrity
- Availability

Riservatezza (Confidentiality)

Garantisce che le informazioni siano accessibili soltanto agli utenti autorizzati.

Esempi:

- password;
- crittografia;
- controllo accessi.

Integrità (Integrity)

Garantisce che i dati non vengano alterati in modo non autorizzato.

Esempi:

- firme digitali;
- hash crittografici;
- controlli di integrità.

Disponibilità (Availability)

Garantisce che servizi e informazioni siano accessibili quando necessario.

Esempi:

- ridondanza;
- backup;
- alta affidabilità.

8.3 Minacce alla sicurezza delle reti

Una minaccia è qualsiasi evento che possa compromettere la sicurezza di un sistema.

Le minacce possono essere:

- accidentali;
- intenzionali;
- interne;
- esterne.

Minacce accidentali

Sono causate da errori involontari.

Esempi:

- cancellazione di file;
- configurazioni errate;
- guasti hardware.

Minacce intenzionali

Derivano da azioni deliberate.

Esempi:

- furto di dati;
- sabotaggio;
- attacchi informatici.

8.4 Vulnerabilità

Una vulnerabilità è una debolezza che può essere sfruttata da un attaccante.

Esempi:

- software non aggiornato;
- password deboli;
- configurazioni errate;

- servizi esposti inutilmente.

Una vulnerabilità non implica necessariamente un attacco, ma aumenta il rischio che esso possa verificarsi.

8.5 Rischio informatico

Il rischio rappresenta la probabilità che una minaccia sfrutti una vulnerabilità causando un danno.

Formula semplificata:

Rischio = Minaccia × Vulnerabilità × Impatto

Ridurre una vulnerabilità significa ridurre il rischio.

8.6 Malware

Il termine malware deriva da:

Malicious Software

Indica qualsiasi software progettato per causare danni o svolgere attività non autorizzate.

8.7 Virus

Un virus informatico necessita generalmente di un file ospite per diffondersi.

Caratteristiche:

- si replica;
- infetta altri file;
- può danneggiare il sistema.

8.8 Worm

Un worm è un malware autonomo.

Può propagarsi automaticamente attraverso la rete.

Caratteristiche:

- elevata velocità di diffusione;
- sfruttamento delle vulnerabilità;
- saturazione delle risorse di rete.

8.9 Trojan Horse

Il Trojan (Cavallo di Troia) si presenta come un software legittimo.

Una volta installato:

- apre accessi non autorizzati;
- ruba informazioni;
- installa ulteriori malware.

8.10 Ransomware

Il ransomware cifra i dati della vittima e richiede un riscatto per il ripristino.

Conseguenze:

- blocco delle attività;
- perdita di dati;
- gravi danni economici.

Negli ultimi anni è diventato una delle minacce più diffuse.

8.11 Spyware

Lo spyware raccoglie informazioni senza il consenso dell'utente.

Può registrare:

- attività online;

- credenziali;
- dati personali.

8.12 Adware

L'adware mostra pubblicità indesiderata.

Sebbene spesso meno pericoloso di altri malware, può:

- rallentare il sistema;
- compromettere la privacy;
- facilitare ulteriori infezioni.

8.13 Phishing

Il phishing è una tecnica di ingegneria sociale.

L'attaccante cerca di convincere la vittima a fornire:

- password;
- dati bancari;
- informazioni riservate.

Generalmente utilizza:

- email;
- SMS;
- siti web contraffatti.

8.14 Spear Phishing

È una forma avanzata di phishing.

L'attacco è personalizzato verso una persona o un'organizzazione specifica.

L'efficacia è spesso maggiore rispetto al phishing tradizionale.

8.15 Attacchi DoS e DDoS

DoS (Denial of Service)

L'obiettivo è rendere indisponibile un servizio.

DDoS (Distributed Denial of Service)

L'attacco proviene da numerosi sistemi compromessi.

Effetti:

- saturazione della banda;
- blocco dei server;
- indisponibilità dei servizi.

8.16 Man in the Middle

In questo attacco un soggetto malevolo si inserisce tra due sistemi che comunicano.

Obiettivi:

- intercettare dati;
- modificarli;
- rubare informazioni.

Per questo motivo è fondamentale utilizzare protocolli cifrati.

8.17 Brute Force

L'attaccante tenta numerose combinazioni di password fino a individuare quella corretta.

La protezione richiede:

- password robuste;
- blocco degli account;
- autenticazione multifattore.

8.18 Ingegneria Sociale

Molti attacchi sfruttano il comportamento umano piuttosto che vulnerabilità tecniche.

Esempi:

- telefonate fraudolente;
- email ingannevoli;
- falsi supporti tecnici.

La formazione degli utenti rappresenta una delle difese più efficaci.

8.19 Firewall

Il firewall controlla il traffico di rete.

Può:

- consentire;
- limitare;
- bloccare

le comunicazioni secondo regole predefinite.

8.20 Segmentazione della rete

La segmentazione consiste nel suddividere la rete in aree separate.

Tecnologie utilizzate:

- VLAN;
- subnet;
- firewall interni.

Vantaggi:

- riduzione della superficie di attacco;
- isolamento dei problemi;
- maggiore sicurezza.

8.21 DMZ

DMZ significa:

Demilitarized Zone

È una rete separata che ospita servizi esposti a Internet.

Esempi:

- server web;
- server di posta;
- portali pubblici.

La DMZ riduce i rischi per la rete interna.

8.22 VPN

VPN significa:

Virtual Private Network

Permette di creare un tunnel cifrato tra due punti.

Vantaggi

- protezione dei dati;
- accesso remoto sicuro;
- riservatezza delle comunicazioni.

Utilizzi tipici

- smart working;
- collegamento tra sedi;
- accesso remoto ai server aziendali.

8.23 IDS e IPS

IDS

Intrusion Detection System

Monitora il traffico e segnala attività sospette.

IPS

Intrusion Prevention System

Interviene automaticamente per bloccare gli attacchi.

8.24 Autenticazione

L'autenticazione verifica l'identità dell'utente.

Può basarsi su:

Qualcosa che conosci

Password.

Qualcosa che possiedi

Token o smartphone.

Qualcosa che sei

Biometria.

8.25 Multi-Factor Authentication (MFA)

La MFA richiede almeno due fattori di autenticazione.

Esempio:

- Password
- Codice temporaneo sul telefono

Vantaggi:

- maggiore protezione;
- riduzione del rischio di compromissione.

8.26 Principio del Minimo Privilegio

Ogni utente deve possedere esclusivamente i permessi necessari per svolgere le proprie attività.

Benefici:

- riduzione dei rischi;
- limitazione dei danni;
- maggiore controllo.

8.27 Backup

Il backup consiste nella copia dei dati.

Tipologie:

- completo;
- incrementale;
- differenziale.

Un backup efficace rappresenta una delle principali difese contro ransomware e guasti.

8.28 Aggiornamenti e Patch Management

Molti attacchi sfruttano vulnerabilità note.

Per questo motivo è fondamentale:

- aggiornare i sistemi;
- applicare le patch;

- mantenere software supportati.

8.29 Modello Zero Trust

Zero Trust si basa sul principio:

"Never Trust, Always Verify"

Nessun utente o dispositivo viene considerato automaticamente affidabile.

Ogni accesso deve essere verificato.

Vantaggi

- maggiore controllo;
- riduzione dei rischi;
- migliore protezione degli ambienti distribuiti.

8.30 Caso di studio

Un'azienda di 200 dipendenti implementa:

- Firewall NGFW;
- VLAN separate;
- VPN per il lavoro remoto;
- MFA per tutti gli utenti;
- backup giornalieri;
- monitoraggio IDS/IPS.

Dopo l'implementazione:

- diminuiscono gli incidenti di sicurezza;
- aumenta la protezione dei dati;
- migliora la conformità normativa.

Riepilogo

In questo capitolo abbiamo studiato:

- Triade CIA;
- Minacce e vulnerabilità;
- Malware;
- Phishing;
- DoS e DDoS;
- Firewall;
- DMZ;
- VPN;
- IDS e IPS;
- MFA;
- Backup;
- Patch Management;
- Zero Trust.

La sicurezza delle reti non dipende da una singola tecnologia ma dall'integrazione di processi, strumenti e comportamenti corretti.

Domande di verifica

1. Cosa rappresenta la triade CIA?
2. Qual è la differenza tra minaccia e vulnerabilità?
3. Cos'è un ransomware?
4. Come funziona un attacco phishing?
5. Quali differenze esistono tra DoS e DDoS?
6. Cos'è una VPN?
7. Qual è il ruolo di un firewall?
8. Quali differenze esistono tra IDS e IPS?
9. Cos'è la Multi-Factor Authentication?
10. Quali principi caratterizzano il modello Zero Trust?