LA SICUREZZA NELLE RETI

Reti sicure

Per rendere sicura una rete dobbiamo conoscere sia le opportune misure da intraprendere sia conoscere da chi o da cosa proteggere il sistema. Iniziamo a vedere da cosa dobbiamo proteggerci.

– **Hacker**: si tratta di un individuo o un gruppo di individui il cui obiettivo è accedere ai sistemi per diversi motivi che vanno dal puro divertimento, allo studio, alla curiosità o semplicemente per dimostrare di essere in grado di farlo. Nella maggior parte dei casi l'hacker non causa gravi danni al sistema della vittima.

– **Cracker**: si tratta di un individuo o di un gruppo di individui il cui obiettivo è violare i sistemi di sicurezza informatici per provocare un danno. A differenza degli **hacker**, che possono anche avere intenti etici o di ricerca, i cracker agiscono tipicamente per **Intenzioni malevole**, con lo scopo di causare danni, rubare informazioni, o compromettere la sicurezza.

1. **Tecniche utilizzate**:
    - **Brute force**: Tentano di violare password o chiavi di sicurezza.
    - **Phishing**: Ingannano gli utenti per ottenere credenziali o dati sensibili.
    - **Malware**: Diffondono virus, ransomware (tipologia di malware progettata per bloccare l'accesso a file, dati o interi sistemi informatici della vittima, richiedendo un riscatto (ransom) per ripristinare l'accesso. È una delle minacce informatiche più diffuse e pericolose) o spyware (categoria di malware progettata per **spiare** e raccogliere informazioni sull'utente o sul sistema informatico senza il suo consenso. Questo software può operare in modo nascosto, inviando i dati raccolti a terze parti per scopi dannosi o commerciali)
    - **Exploit**: Sfruttano vulnerabilità nei software o nei sistemi operativi, con l'obiettivo di ottenere un comportamento non previsto, spesso dannoso. Gli exploit sono comunemente utilizzati per compromettere la sicurezza di un sistema
2. **Obiettivi comuni**:
    - Furto di dati sensibili (es. credenziali bancarie, informazioni personali).
    - Sabotaggio (es. defacement di siti web per modificare il contenuto di un sito web, solitamente per motivi di vandalismo digitale, propaganda politica, o come forma di protesta. L'obiettivo principale non è rubare dati o danneggiare il sistema in modo permanente, ma cambiare la sua presentazione pubblica, spesso per attirare l'attenzione, attacchi DDoS **(Distributed Denial of Service)**, è una tecnica malevola che mira a rendere un sistema, un servizio o una rete inutilizzabili sovraccaricandoli con un volume di traffico superiore alla loro capacità.

- Estorsione (es. ransomware).

Si possono dividere in due tipi (Cracker):

• **Outsider**: sono coloro che operano dall'esterno del network che intendono attaccare.

Insider: sono coloro che sono autorizzati all'uso della rete e che cercano di abusarne.

Cracker vs Hacker:

- **Hacker**: Spesso lavora per scopi costruttivi, migliorando la sicurezza o innovando tecnologie (es. **ethical hacker**).
- **Cracker**: Ha obiettivi distruttivi o illegali, cercando di compromettere sistemi senza autorizzazione.

La sicurezza della rete è definita dal livello di **fault tolerance** della stessa rete, ovvero la capacità di un sistema di eseguire normalmente le operazioni malgrado la presenza di errori hardware o software.

La sicurezza di una rete non dipende unicamente dalla sua **struttura fisica** (come il cablaggio, i dispositivi hardware, la topologia) o **logica** (come i protocolli di comunicazione, la segmentazione, le configurazioni software). Anche se questi aspetti influenzano la sicurezza, non sono sufficienti da soli per definire una rete come sicura o insicura.

In pratica, una rete può avere una struttura fisica e logica ben progettata, ma può comunque essere vulnerabile se non sono stati implementati adeguati controlli e misure di sicurezza. Allo stesso modo, una rete con una struttura fisica o logica semplice o non ottimale può essere resa sicura con strategie di protezione adeguate.

Per una azienda i malfunzionamenti sono causa di guai e di conseguenza di costi aggiuntivi. Nelle reti di grandi dimensioni la funzionalità della rete deve essere garantita con bassissimi margini di errore, per raggiungere questo risultato tuttavia le soluzioni sono complesse. Una rete può essere soggetta a malfunzionamenti di vario genere, basti pensare che per esempio un problema ai server di un qualsiasi ISP può bloccare migliaia di siti web. Per ridurre il rischio di blocchi della rete dobbiamo utilizzare le seguenti strategie:

– bloccare i tentativi di intrusione dall'esterno;

– proteggere la rete da attività di utenti che possono compiere atti dolosi o colposi;

– utilizzare sistemi di controllo e di monitoraggio della rete;

– ampliare il livello di affidabilità e di sicurezza attraverso sistemi di controllo dell’alimentazione, degli impianti, dei locali e delle strutture che li ospitano;

In conclusione, la sicurezza di una rete non dipende unicamente dalla sua struttura fisica o logica, ma dall'integrazione di strumenti, politiche e procedure di sicurezza. Anche una rete fisicamente ben progettata può essere vulnerabile senza misure di protezione adeguate, mentre una rete meno sofisticata può essere resa sicura con controlli adeguati.

Per ridurre il rischio di blocchi della rete dobbiamo utilizzare le seguenti strategie:

– bloccare i tentativi di intrusione dall’esterno;

– proteggere la rete da attività di utenti che possono compiere atti dolosi o colposi;

– utilizzare sistemi di controllo e di monitoraggio della rete;

– ampliare il livello di affidabilità e di sicurezza attraverso sistemi di controllo dell’alimentazione, degli impianti, dei locali e delle strutture che li ospitano;

– utilizzare le tecniche di ridondanza di server e servizi.

Livello di Fault Tolerance di una Rete

Il **fault tolerance** (o tolleranza ai guasti) di una rete è la sua capacità di continuare a funzionare correttamente anche in presenza di guasti o malfunzionamenti. Un livello elevato di fault tolerance indica che la rete può resistere a problemi come guasti hardware, errori software, interruzioni di connessione o malfunzionamenti dei dispositivi senza interrompere i servizi forniti agli utenti.

Elementi chiave della fault tolerance

1. **Ridondanza**
   - Implica l'uso di componenti duplicati (ad esempio, server, router, percorsi di rete) per garantire che, se un componente si guasta, un altro entri in funzione senza interruzioni.
   - **Esempio:** Configurare una rete con percorsi alternativi tra due nodi per evitare problemi se un cavo si rompe.
2. **Failover**
   - Meccanismo che permette di passare automaticamente a un componente o sistema di backup in caso di guasto.
   - **Esempio:** Se un server primario si arresta, un server secondario subentra immediatamente.
3. **Load Balancing**

    - Distribuzione del carico di lavoro tra più componenti per evitare sovraccarichi e migliorare la resilienza.
    - **Esempio:** Utilizzo di bilanciatori di carico per distribuire le richieste tra diversi server web. I **bilanciatori di carico** (in inglese *load balancers*) sono dispositivi hardware o software che distribuiscono il traffico di rete o le richieste di elaborazione tra più server o risorse, al fine di ottimizzare l'uso delle risorse, migliorare le prestazioni e garantire la disponibilità dei servizi.
4. **Rilevamento e ripristino dei guasti**
    - Utilizzo di strumenti di monitoraggio per identificare rapidamente i problemi e attivare le procedure di ripristino.
    - **Esempio:** Sistemi di monitoraggio SNMP che avvertono gli amministratori di rete in caso di guasti. I **sistemi di monitoraggio SNMP** (*Simple Network Management Protocol*) sono strumenti utilizzati per monitorare e gestire dispositivi di rete come router, switch, server, stampanti e altre apparecchiature connesse. Questi sistemi si basano sul protocollo SNMP per raccogliere informazioni sullo stato e sulle prestazioni dei dispositivi e per inviare comandi di configurazione o gestione. SNMP è un protocollo standardizzato per la gestione e il monitoraggio dei dispositivi di rete. Esso consente a un amministratore di rete di:
        1. Monitorare le prestazioni dei dispositivi.
        2. Effettuare modifiche alle configurazioni da remoto.
5. **Architetture distribuite**
    - Progettare reti in modo che le risorse siano distribuite su più nodi, riducendo il rischio di un singolo punto di guasto.
    - **Esempio:** Utilizzo di data center distribuiti geograficamente per garantire l'accesso ai dati anche in caso di interruzioni locali.

Misurazione del livello di fault tolerance

Il livello di fault tolerance di una rete si può valutare considerando:

- **Tempo di inattività tollerabile (MTTR - Mean Time to Repair):** Tempo necessario per riparare un guasto e ripristinare il sistema.
- **Tempo medio tra i guasti (MTBF - Mean Time Between Failures):** Frequenza con cui si verificano i guasti.
- **Percentuale di disponibilità (Uptime):** Rapporto tra il tempo in cui il sistema è operativo e il tempo totale. Una disponibilità del 99,999% (noto come "five nines") equivale a circa 5 minuti di inattività all'anno.

La **percentuale di disponibilità (Uptime)** è una misura chiave per valutare l'affidabilità di un sistema informatico o di un servizio. Si calcola come il rapporto tra il tempo in cui il sistema è stato operativo e il tempo totale previsto di funzionamento, solitamente espresso in percentuale.

Formula per il calcolo dell'Uptime

$$\text{Disponibilità (\%)} = \left(\frac{\text{Tempo operativo}}{\text{Tempo totale}} \right) \times 100$$

Dove:

- **Tempo operativo**: Il tempo in cui il sistema è accessibile e funzionante.
- **Tempo totale**: Il periodo di osservazione (ad esempio un anno).

Cosa significa "Five Nines" (99,999%)?

- Una disponibilità del **99,999%** è considerata altissima affidabilità, spesso richiesta per sistemi critici come data center, servizi bancari o sanitari.
- Questa percentuale si traduce in un **tempo massimo di inattività (downtime)** molto limitato:

Percentuale di Uptime	Downtime annuo massimo
99%	3 giorni, 15 ore
99,9% (Three Nines)	8 ore, 45 minuti
99,99% (Four Nines)	52 minuti, 36 secondi
99,999% (Five Nines)	5 minuti, 15 secondi

Esempio pratico

Se un servizio ha un tempo totale di 1 anno (365 giorni):

- Con un Uptime del **99,999%**, il sistema può avere **5 minuti e 15 secondi di inattività** nell'intero anno.
- Se la disponibilità scende al **99%**, l'inattività potrebbe arrivare a più di **3 giorni** in un anno.

Perché è importante?

- **Sistemi critici**: Per applicazioni mission-critical (es. sanità, aviazione), una disponibilità elevata garantisce che i servizi siano quasi sempre funzionanti.

- **Esperienza utente**: Un'elevata disponibilità riduce il rischio di interruzioni, migliorando la fiducia degli utenti nel servizio.

Tecnologie che migliorano il fault tolerance

1. **RAID (Redundant Array of Independent Disks):**
   - Garantisce la disponibilità dei dati su più dischi rigidi, anche in caso di guasto di uno di essi.
2. **Cluster di server:**
   - Gruppi di server che lavorano insieme per fornire ridondanza e failover (**tecnica di ridondanza** utilizzata per garantire la **continuità del servizio** e la **disponibilità** di sistemi critici quando si verifica un guasto o un malfunzionamento. Il concetto chiave del failover è trasferire automaticamente le operazioni da un sistema primario a un sistema secondario o di backup in caso di errore).

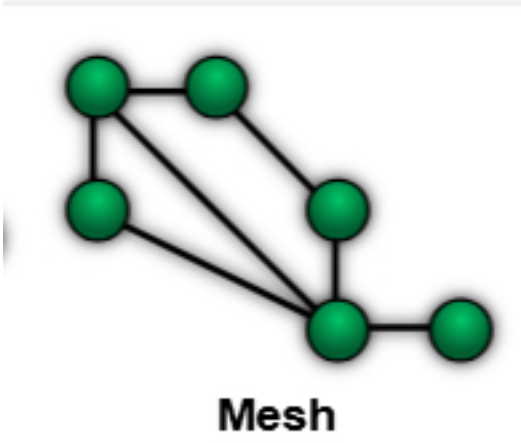
Caratteristiche principali del Failover

1. **Monitoraggio**:
   Il sistema monitora continuamente il funzionamento del componente principale (es. server, rete, applicazione).
2. **Rilevamento del guasto**:
   Quando viene rilevato un problema (es. guasto hardware, crash software), il sistema attiva il failover.
3. **Switch automatico**:
   Il carico di lavoro viene trasferito automaticamente al sistema secondario senza (o con minima) interruzione del servizio.
4. **Continuità operativa**:
   L'utente finale percepisce un'interruzione minima o nulla durante il processo.

3. **Routing dinamico:**
   - Protocolli come OSPF o BGP permettono alla rete di trovare percorsi alternativi in caso di interruzione del percorso principale.
4. **Virtualizzazione:**
   - Le macchine virtuali (Una **VM** è un software che emula l'hardware di un computer, permettendo di eseguire un sistema operativo e programmi come se si trovassero su un hardware dedicato. Questo viene reso possibile grazie a **software di virtualizzazione**.) possono essere spostate rapidamente tra host fisici in caso di guasti hardware.

Esempio pratico

Immaginiamo una rete aziendale con una configurazione a **topologia mesh**, in cui ogni nodo è collegato a più nodi. Se un router smette di funzionare, il traffico viene automaticamente reindirizzato attraverso i percorsi alternativi disponibili, mantenendo la continuità del servizio.



Per la classe:

1. **Esercizio teorico:**
   Perché la ridondanza è importante per il fault tolerance di una rete.
   1. La **ridondanza** è fondamentale per il **fault tolerance** di una rete perché permette di **mantenere operativi i servizi** anche in caso di guasti a componenti critici come collegamenti, dispositivi o server. In altre parole, la ridondanza fornisce percorsi e risorse **alternativi** che subentrano automaticamente se una parte della rete smette di funzionare.

Esempio pratico di ridondanza in una rete

Immaginiamo una **rete aziendale** composta da due **switch** e vari dispositivi collegati:

1. **Scenario senza ridondanza**
   Se un solo switch è collegato a tutti i computer e il collegamento o lo switch smette di funzionare, tutti i dispositivi connessi perderanno l'accesso alla rete.
   - **Conseguenza**: Interruzione totale del servizio fino alla riparazione.
2. **Scenario con ridondanza**
   La rete viene progettata con **collegamenti e dispositivi ridondanti**:
   - I computer sono collegati a **due switch** invece di uno.
   - Gli switch stessi sono interconnessi tramite un **collegamento secondario**.

- Un protocollo come **Spanning Tree Protocol (STP)** gestisce i percorsi per evitare loop.
- **Caso di guasto**: Se uno switch smette di funzionare, il traffico verrà automaticamente **reindirizzato** attraverso il secondo switch grazie alla ridondanza.
- **Conseguenza**: I dispositivi continuano ad accedere alla rete senza interruzioni significative.

La **sicurezza nelle reti** si riferisce alla protezione delle infrastrutture di rete da accessi non autorizzati, attacchi e altre minacce che possono compromettere l'integrità, la disponibilità e la riservatezza dei dati. È un ambito fondamentale per garantire che le informazioni e i sistemi informatici siano protetti da attacchi esterni e vulnerabilità interne. In pratica, la sicurezza nelle reti comprende una serie di tecnologie, politiche e procedure volte a prevenire e gestire le minacce.

Le principali aree di interesse nella sicurezza delle reti includono:

1. **Autenticazione e controllo accessi**: Assicurare che solo gli utenti legittimi possano accedere alle risorse di rete, tramite l'uso di credenziali, autenticazione a più fattori (MFA - Impronta digitale, Scansione della retina, Riconoscimento vocale, Riconoscimento facciale) e tecnologie come VPN e firewall.
2. **Protezione dei dati**: Criptare i dati sia in transito che a riposo per prevenire accessi non autorizzati.
3. **Monitoraggio e rilevamento**: Utilizzo di strumenti per monitorare e analizzare il traffico di rete, identificando comportamenti sospetti o attacchi in corso (es. sistemi IDS / IPS – sistemi di rilevamento delle intrusioni / sistemi di prevenzione delle intrusioni).
4. **Prevenzione degli attacchi**: Difendersi contro minacce come malware, phishing, attacchi DDoS, e spoofing, utilizzando misure come antivirus, firewall, e aggiornamenti regolari.
5. **Ripristino e recupero**: Pianificare soluzioni di backup e disaster recovery in caso di attacco o disastro.

In generale, la sicurezza nelle reti è un processo continuo che richiede aggiornamenti regolari e una consapevolezza costante delle minacce emergenti. L'obiettivo finale è proteggere i dati aziendali e personali, garantendo che le reti siano sicure, affidabili e resistenti agli attacchi.