

CYBERSECURITY

The image features a blue gradient background. On the right side, there is a series of approximately seven parallel white diagonal lines that extend from the bottom left towards the top right corner. The word "CYBERSECURITY" is centered in the middle of the image in a white, uppercase, sans-serif font.


INTRODUZIONE

- ▶ Uno dei primi obiettivi delle aziende è la **sicurezza** della rete aziendale e per la tutela delle informazioni aziendali.
- ▶ Per **sicurezza** di un sistema informatico si intende la salvaguardia di:
 - **Affidabilità** → i dati devono essere sempre accessibili agli utenti **autorizzati**. (Esempio di violazione affidabilità: mancanza di alimentazione elettrica e rottura di un componente hardware)
 - **Integrità** → i dati non devono essere corrotti. (Esempio di integrità: cancellazione o modifica di un file)
 - **Riservatezza** → i dati devono essere accessibili solo a chi è autorizzato ad utilizzarli (Esempio di riservatezza: intercettazione dei dati durante la loro trasmissione e accesso non autorizzato ai dati sul server)
 - **Autenticità** → i dati devono essere autentici dal mittente al destinatario (Esempio di autenticità: spedizione di email da parte di pirata informatico che si maschera per il mittente)
 - **Non Ripudio** → chi invia/riceve non può negare di averlo fatto. (Esempio di non ripudio: email falsa – carta intestata falsa – firma falsa)


CIA: CONFIDENTIALITY – INTEGRITY - AVAILABILITY

- ▶ Un sistema si definisce sicuro quando le informazioni contenute sono garantite contro le violazioni degli aspetti di sicurezza.
- ▶ Un'azienda deve attuare un'adeguata **politica di sicurezza** quindi definire ed organizzare la riservatezza e l'integrità informatica gestendone tutti gli aspetti (tecnici, di management, di business)

INTRODUZIONE

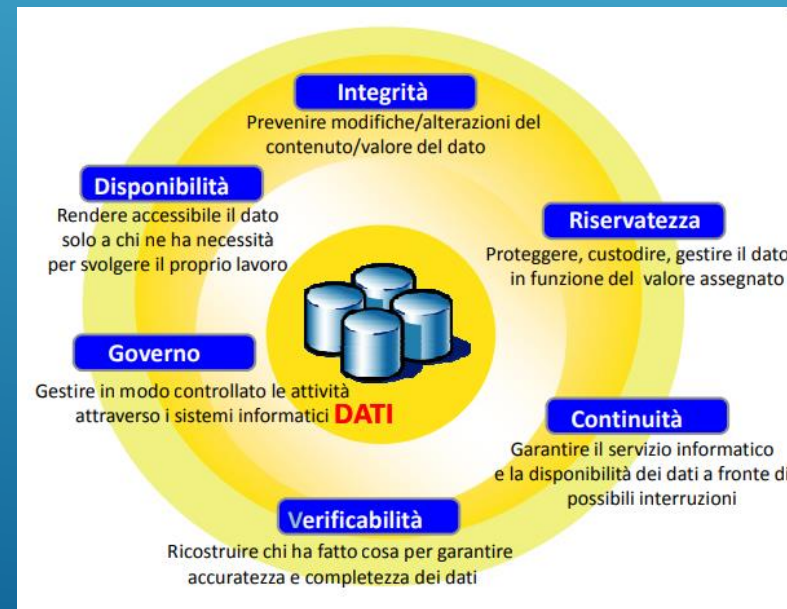
- ▶ La sicurezza di un sistema non può essere considerata qualcosa di statico ma deve essere un **processo continuo** → definizione delle politiche di sicurezza, delle regole di comportamento, analisi e gestione del rischio, piano operativo, formazione del personale.
 - ▶ **VULNERABILITA'** → debolezza del sistema.
 - ▶ **MINACCIA** → evento di natura dolosa o accidentale che sfruttando una vulnerabilità del sistema, potrebbe provocare un danno
 - ▶ **RISCHIO** → l'eventualità che una minaccia si trasforma in danno
- 
- A series of three parallel white diagonal lines are positioned in the bottom right corner of the slide, extending from the middle of the right edge towards the bottom left.

ALCUNE DEFINIZIONI

- ▶ **VULNERABILITA'** → debolezza del sistema.
 - ▶ **MINACCIA** → evento di natura dolosa o accidentale che sfruttando una vulnerabilità del sistema, potrebbe provocare un danno
 - ▶ **RISCHIO** → l'eventualità che una minaccia si trasforma in danno
 - ▶ **SALVAGUARDIA** → contromisura che consente di intraprendere delle azioni per ridurre le vulnerabilità
- 
- A series of three parallel white diagonal lines in the bottom right corner of the slide, extending from the middle of the right edge towards the bottom left.

CONCETTO GIURIDICO DI SICUREZZA INFORMATICA

- ▶ E' collegato a tutti gli accorgimenti tecnici ed organizzativi che tutelano i beni giuridici della confidenzialità o riservatezza, dell'integrità e della disponibilità delle informazioni registrate.
- ▶ L'accesso non autorizzato ad un sistema informatico da parte di qualcuno può essere paragonato alla violazione di domicilio. (REATO!)
- ▶ Copiare i dati oppure i programmi può essere considerato come violazione dei diritti d'autore.



INTEGRITA'

- ▶ Per l'integrità dei dati, le minacce possono essere **NATURALI** o **UMANE**.
- ▶ Quelle NATURALI (calamità imprevedibili) sono impossibili da prevedere. Per questi attacchi è possibile effettuare un' **ANALISI DEI RISCHI** perché potrebbero causare lunghi periodi di inattività lavorativa (prevedere dei piani di ripristino con operazioni di **DISASTER RECOVERY**).
- ▶ Quelle UMANE sono dovute a persone che vogliono danneggiare il sistema dell'azienda. Possono essere dipendenti interni all'azienda (**attacco interno**) che, conoscendo le password per accedere ai sistemi, riescono a danneggiarli. Questi si chiama **CRACKER**, coloro che si introducono nei sistemi senza essere autorizzati. Oltre all'attacco interno, si può avere **attacco esterno** creato da persone esterne all'azienda che ne vogliono danneggiare l'organizzazione, accedendo ai sistemi senza autorizzazione (**HACKER**).

RISERVATEZZA

- ▶ Per la riservatezza, è necessario limitare l'accesso degli utenti.
- ▶ Per far ciò, è necessario un meccanismo di **AUTENTICAZIONE**
- ▶ **AUTENTICAZIONE** → processo di riconoscimento di un utente tramite conoscenza di un segreto (utilizzo di username e password) oppure tramite possesso di un oggetto (smart card) oppure tramite strumento di riconoscimento biometrico (impronta digitale, screen viso, screen iride).
- ▶ Dopo essersi autenticato, un utente deve essere **autorizzato**; alcune cose le può fare ed altre no.

ATTACCHI

SNIFFING → intercettare i dati in rete utilizzando lo sniffer cioè un programma che permette ad un computer di leggere automaticamente tutti i pacchetti che attraversano la rete alla quale è connesso, estraendo le informazioni più interessanti.

La tecnica di difesa per lo sniffing consiste nel crittografare i pacchetti spediti, utilizzare connessioni sicure, evitare di trasmettere dati sensibili su reti pubbliche.

SPOOFING → introdursi nella rete per modificare l'indirizzo IP del mittente e facendo credere al destinatario che provengono da un'altra origine (**Spoofing di indirizzi IP**)

Spoofing dei dati → consiste nel prendere il controllo del canale di trasmissione e nell'inserire, modificare, cancellare i dati trasmessi. La tecnica di difesa consiste nell'utilizzo di tecniche di autenticazione e di verifica di integrità.

Mac Spoofing → clonazione degli indirizzi MAC

Email Spoofing → falsificazione del mittente delle email

La tecnica di difesa per lo spoofing consiste nell'applicare tecniche di autenticazione a più fattori, tecniche di verifica dell'integrità dei pacchetti.

ATTACCHI

PHISHING → chi attacca si finge un'entità affidabile ed invia email/messaggi per adescare tramite link chiedendo dati sensibili

La tecnica di difesa per il phishing consiste nel verificare autenticità del mittente, controllare la URL, non cliccare sui link sospetti, utilizzare filtri anti phishing.

MAN IN THE MIDDLE → intercettazione attiva delle comunicazioni tra 2 parti per leggere/modificare messaggi (scambio di messaggi tramite WiFi non sicuro)

La tecnica di difesa per lo MITM consiste nell'utilizzo di connessioni cifrate, verifica certificati digitali, uso di VPN.

DENIAL OF SERVICE → attacco che rende inutilizzabile la rete facendo entrare enorme quantità di dati, saturando la rete (attacco ad uno shop online inserendo elevatissimo numero di richieste al secondo fino a bloccare il sito)

La tecnica di difesa per il DOS consiste nell'utilizzo di software di prevenzione

ATTACCHI

SPAMMING → invio massivo di email indesiderate

La tecnica di difesa per lo spamming consiste nell'utilizzare filtri anti spam, black list.

NUKING → attacchi mirati per causare crash dei sistemi

La tecnica di difesa per il nuking consiste nell'utilizzo di aggiornamenti di sicurezza, configurazione dei firewall.


ATTACCHI IoT → attacco tramite i dispositivi IoT (sono potenziali porte di accesso ai sistemi)

La tecnica di difesa consiste nel cambio di password iniziale obbligatorio,

CICLO DI VITA DEGLI ATTACCHI

- 1) **Recupero delle informazioni sulle vulnerabilità** (vulnerabilità software – valutazione degli accessi – dipendente insoddisfatto)
- 2) **Compromissione iniziale** (accesso al sistema sfruttando le vulnerabilità)
- 3) **Comando e controllo** (dentro il sistema, installazione di software dannoso)
- 4) **Escalation di privilegi** (diventare amministratore del sistema attaccato)
- 5) **Spostamento laterale** (trovare nuovi obiettivi all'interno del sistema attaccato)
- 6) **Raggiungimento del target** (accesso agli obiettivi raggiunti)

MISURE DI SICUREZZA

- 1) **PREVENTION** (implementare misure per prevenire lo sfruttamento delle vulnerabilità del sistema)
 - 2) **DETECTION** (rilevare prontamente il problema per intraprendere delle azioni prima che questo si diffonda)
 - 3) **AUTOMATION** (se possibile, automatizzare le azioni di prevention e detection)
 - 4) **RESPONSE** (sviluppare un piano di intervento in caso di violazione con individuazione delle responsabilità e delle azioni da intraprendere)
- 
- A series of white diagonal lines of varying lengths and thicknesses, located in the bottom right corner of the slide, creating a modern, abstract graphic element.

PROTEZIONE DEI DATI

- Gli **STORAGE** sono tutti i supporti hardware e software per proteggere grandi quantità di dati, capaci di garantire la sicurezza delle informazioni conservate.
- Possono essere:
 - ✓ **NAS (Network Attached Storage)**: il dispositivo è collegato a più computer messi in rete tra loro. Questo sistema permette di centralizzare la memorizzazione dei dati in un'unità accessibile da tutta la rete ma la grande quantità di dati che viaggiano in rete può rallentare il sistema.
 - ✓ **DAS (Direct Attached Storage)**: dispositivo di memorizzazione collegato direttamente ad un server, non avendo collegamento in rete. Con questo sistema, è difficile condividere i dati tra più computer e l'espansione dello spazio è complessa
 - ✓ **SAN (Storage Area Network)**: sistema di memorizzazione che rende disponibili i dati a computer connessi ad alte velocità tramite fibra ottica.

PROTEZIONE DEI DATI

- Il **BACKUP** dei dati è una copia di riserva dei dati da poter recuperare in caso di perdita accidentale.
- Dovrebbe essere fatto spesso
- Può essere:
 - **COMPLETO**: memorizza sempre tutti i dati.
 - **INCREMENTALE**: memorizza solo le modifiche fatte rispetto all'ultimo backup
 - **DIFFERENZIALE**: memorizza solo le modifiche rispetto all'ultimo backup completo.