COS'E' LA CYBER SECURITY

La Cyber Security (o sicurezza informatica) è il campo che si occupa di proteggere i **sistemi informatici**, le **reti** e i **dati** da accessi non autorizzati, danni, furti o attacchi informatici. L'obiettivo principale della Cyber Security è garantire la **riservatezza**, **integrità** e **disponibilità** delle informazioni e dei sistemi, proteggendo le risorse tecnologiche dalle minacce esterne (come hacker e malware) e interne (come errori o atti malevoli da parte degli utenti).

Perché la Cyber Security è importante?

Con l'aumento dell'uso di internet, dei dispositivi mobili e della digitalizzazione, il numero di attacchi informatici è cresciuto esponenzialmente. La Cyber Security è diventata una necessità per proteggere le informazioni personali, aziendali e governative. Senza una protezione adeguata, le persone e le aziende sono vulnerabili a:

- **Furto di dati sensibili** (ad esempio, numeri di carte di credito, password, documenti riservati).
- **Interruzione dei servizi** (come il downtime di un sito web o di un sistema critico, causato da un attacco DDoS).
- **Danno alla reputazione** (se un'azienda subisce una violazione, la fiducia dei clienti può diminuire).
- **Ransomware** (che cifra i dati e chiede un riscatto per decriptarli).

Le principali aree della Cyber Security:

1. **Sicurezza delle reti (Network Security):**
   Protegge le reti informatiche da accessi non autorizzati, attacchi di malware e traffico dannoso. Include l'uso di firewall, crittografia e VPN.
2. **Sicurezza delle applicazioni (Application Security):**
   Si occupa della protezione delle applicazioni software contro vulnerabilità che potrebbero essere sfruttate da attaccanti. Gli sviluppatori usano tecniche di programmazione sicura e test per ridurre il rischio.
3. **Sicurezza dei dati (Data Security):**
   Si concentra sulla protezione dei dati durante il loro ciclo di vita, dall'archiviazione alla trasmissione. La crittografia e i backup sono strumenti fondamentali in questo ambito.
4. **Sicurezza operativa (Operational Security):**
   Riguarda le pratiche e le politiche utilizzate per proteggere i dati e le risorse aziendali. Ad esempio, i controlli degli accessi, l'autenticazione e l'autorizzazione, e la gestione delle password sono tutti aspetti importanti.
5. **Sicurezza fisica (Physical Security):**
   Protegge l'infrastruttura fisica, come i server e i dispositivi hardware, da furti o danni. Questo può includere l'uso di videocamere, allarmi e controlli di accesso fisici.

6. **Sicurezza dei dispositivi mobili (Mobile Security):**
   Protegge i dispositivi mobili come smartphone e tablet da minacce come malware e accessi non autorizzati.
7. **Gestione delle identità (Identity Management):**
   Si occupa di assicurarsi che solo gli utenti autorizzati possano accedere ai sistemi e alle informazioni sensibili, spesso utilizzando tecniche come l'autenticazione a due fattori (2FA).
8. **Gestione dei rischi e risposta agli incidenti (Risk Management and Incident Response):**
   Identifica i rischi potenziali, pianifica azioni per ridurre il rischio e prepara procedure di risposta in caso di attacco o violazione.

Minacce comuni nella Cyber Security:

- **Malware:** Software dannoso progettato per danneggiare o prendere il controllo di un dispositivo.
- **Phishing:** Attacco che cerca di ingannare l'utente per ottenere informazioni sensibili, spesso tramite email fasulle.
- **Ransomware:** Tipo di malware che cifra i dati dell'utente e chiede un riscatto per decriptarli.
- **Attacchi DDoS (Distributed Denial of Service):** Tentativo di rendere un sistema o sito web non disponibile sovraccaricandolo con richieste di traffico.
- **SQL Injection:** Una tecnica che sfrutta le vulnerabilità nelle applicazioni web per accedere ai database.

Come difendersi dalla Cyber Security?

Le aziende e gli individui devono implementare misure di sicurezza per proteggere i propri dati e dispositivi, tra cui:

- **Utilizzo di software antivirus e firewall.**
- **Aggiornamento regolare dei sistemi e software per evitare vulnerabilità note.**
- **Formazione e sensibilizzazione per prevenire errori umani (ad esempio, riconoscere email di phishing).**
- **Implementazione di una solida gestione delle password e autenticazione a più fattori.**
- **Backup regolari dei dati per prevenire la perdita in caso di attacchi.**

In sintesi, **la Cyber Security è fondamentale** per proteggere tutti gli aspetti digitali della nostra vita personale e professionale da attacchi, danni e minacce che potrebbero compromettere la nostra sicurezza e privacy.

I FONDAMENTI DELLA CYBER SECURITY

I fondamenti della Cyber Security sono essenziali per comprendere come proteggere i sistemi informatici, le reti e i dati da attacchi, danni o accessi non autorizzati. La sicurezza informatica è un campo ampio che include la protezione da minacce interne ed esterne, e viene applicata attraverso misure preventive, rilevamento e risposta agli incidenti.

Ecco una panoramica dei **principali fondamenti della Cyber Security**:

---

1. Riservatezza (Confidentiality)

La **riservatezza** si riferisce alla protezione delle informazioni da accessi non autorizzati. L'obiettivo principale è garantire che solo le persone o i sistemi autorizzati possano accedere ai dati sensibili.

- **Esempio:** Proteggere le informazioni finanziarie di un cliente in una banca. Solo il cliente e i dipendenti autorizzati possono accedere ai dettagli del conto.

Tecniche di protezione:

- **Crittografia:** Codifica dei dati in modo che solo chi possiede una chiave possa decifrarli.
- **Controllo degli accessi:** Utilizzo di password e **autenticazione a due fattori (2FA)** per limitare l'accesso a informazioni riservate.

---

2. Integrità (Integrity)

L'**integrità** assicura che i dati siano accurati e completi e che non siano stati alterati da parte di persone non autorizzate. In pratica, significa che le informazioni non devono essere modificate, corrotte o cancellate durante la trasmissione o l'archiviazione.

- **Esempio:** Se un'azienda conserva una lista di ordini online, l'integrità garantisce che i dettagli dell'ordine non siano cambiati in modo fraudolento durante il processo di pagamento.

Tecniche di protezione:

- **Hashing:** Creazione di un valore unico per ogni dato che può essere confrontato per verificare che non sia stato modificato.
- **Controlli di versione:** Verifica delle versioni dei file per assicurarsi che non ci siano modifiche non autorizzate.

---

3. Disponibilità (Availability)

La **disponibilità** riguarda l'assicurarsi che i sistemi, le reti e i dati siano accessibili e operativi quando richiesti, in modo che le persone autorizzate possano utilizzarli quando ne hanno bisogno.

- **Esempio:** Un sito di e-commerce deve essere attivo e funzionante 24 ore su 24, affinché i clienti possano fare acquisti in qualsiasi momento.

Tecniche di protezione:

- **Backup regolari:** Assicurarsi che i dati siano copiati regolarmente in modo che possano essere recuperati in caso di guasti o attacchi.

- **Ridondanza e failover:** Utilizzo di sistemi duplicati per garantire che se un sistema fallisce, un altro possa subentrare senza interruzioni.

---

4. Autenticazione e Autorizzazione

L'**autenticazione** è il processo di verifica dell'identità di un utente o sistema (ad esempio, attraverso username e password), mentre l'**autorizzazione** è il processo che determina a quali risorse un utente può accedere una volta autenticato.

- **Esempio:** Una banca online autentica l'utente con la password, e poi autorizza l'accesso solo ai dati dell'account di quella persona specifica.

Tecniche di protezione:

- **Autenticazione a due fattori (2FA):** Una seconda forma di verifica oltre alla password, come un codice inviato al telefono dell'utente.
- **Controllo degli accessi basato sui ruoli (RBAC):** Limitazione dell'accesso alle risorse in base al ruolo dell'utente all'interno dell'organizzazione.

---

5. Monitoraggio e Rilevamento delle Minacce

Un aspetto fondamentale della Cyber Security è il monitoraggio continuo dei sistemi per rilevare attività sospette, attacchi o anomalie. La capacità di rilevare un attacco in tempo reale è cruciale per mitigare il danno.

- **Esempio:** Un sistema di monitoraggio potrebbe rilevare accessi insoliti a un server e generare un allarme in caso di tentativi di hacking.

Tecniche di protezione:

- **Sistemi di rilevamento delle intrusioni (IDS):** Monitorano il traffico di rete alla ricerca di attività dannose.
- **Sistemi di gestione delle informazioni e degli eventi di sicurezza (SIEM):** Raccolgono e analizzano i log di eventi da più fonti per identificare potenziali minacce.

---

6. Risposta agli Incidenti e Recupero

La risposta rapida a un attacco informatico è fondamentale per limitare i danni. Inoltre, il recupero delle informazioni e dei sistemi compromessi è essenziale per ripristinare le normali operazioni.

- **Esempio:** Se un'azienda viene colpita da un attacco ransomware, una risposta efficace potrebbe includere l'isolamento del sistema compromesso, l'individuazione della causa e il ripristino dai backup.

Tecniche di protezione:

- **Piani di risposta agli incidenti:** Procedure definite su come reagire a diversi tipi di attacchi.
- **Ripristino di emergenza:** Creazione di backup regolari e testati per recuperare rapidamente i dati dopo un attacco.

---

7. Protezione delle Reti

La protezione delle reti è una delle aree chiave della Cyber Security. Le reti devono essere protette da attacchi come la **sovraccarico** (DDoS), accessi non autorizzati e traffico dannoso.

- **Esempio:** Un firewall aiuta a impedire che traffico non autorizzato entri nella rete aziendale.

Tecniche di protezione:

- **Firewall e VPN:** Filtrano il traffico di rete e proteggono le comunicazioni da accessi non autorizzati.
- **Segmentazione della rete:** Creazione di "zone sicure" per limitare i danni in caso di violazione.

---

8. Educazione e Consapevolezza degli Utenti

L'educazione continua è un fattore cruciale nella Cyber Security. Gli utenti finali (dipendenti, clienti, ecc.) sono spesso il punto debole nella difesa di un sistema informatico. Essere consapevoli delle minacce come il **phishing** o gli **attacchi di social engineering** è fondamentale.

- **Esempio:** Se un dipendente non riconosce una email di phishing, potrebbe inconsapevolmente fornire dati aziendali sensibili.

Tecniche di protezione:

- **Formazione periodica degli utenti:** Insegnare agli utenti come identificare le minacce e proteggere i propri dispositivi.
- **Simulazioni di phishing:** Eseguire esercizi di phishing per testare la consapevolezza degli utenti.

ESEMPIO Email phishing

Ecco un esempio di **email di phishing** ben fatta, che potrebbe ingannare un utente poco attento.

📩 **Oggetto:** 🔴 URGENTE: Il tuo account è stato sospeso!

Da: assistenza-clienti@bancaitalia-support.com

Testo dell'email:

Gentile Cliente,

Abbiamo rilevato un'attività sospetta sul tuo conto bancario. Per garantire la sicurezza del tuo account, abbiamo temporaneamente sospeso l'accesso ai servizi online.

Per riattivarlo, ti invitiamo a verificare immediatamente i tuoi dati cliccando sul link sottostante:

📎 **Verifica il tuo account**

⚠️ Se non confermi le tue credenziali entro 24 ore, il tuo account verrà definitivamente bloccato.

Grazie per la collaborazione,
Servizio Clienti Bancario
📞 800-123-456 | ✉️ support@bancaitalia-support.com

🔍 **Perché questa è un'email di phishing?**

1. **Mittente falso**: sembra ufficiale ma l'indirizzo non è quello della vera banca.
2. **Senso di urgenza**: spinge l'utente ad agire in fretta.
3. **Link ingannevole**: il testo dice "bancaitalia", ma il vero link è sospetto.
4. **Minaccia di blocco**: induce paura per spingere a cliccare.

⚠️ **Mai cliccare su link sospetti o inserire dati personali!**

I PIU' DIFFUSI ATTACCHI INFORMATICI

📌 **1. Phishing**

Cosa è?
Un hacker invia email, SMS o messaggi falsi fingendosi un ente affidabile (banca, posta, social network) per rubare dati sensibili come password e numeri di carta di credito.

📌 **Esempio:**
Ricevi un'email da "support@bancaitalia.com" che ti dice di aggiornare i tuoi dati bancari cliccando su un link (falso).

📌 **2. Malware (Virus, Trojan, Ransomware, Spyware)**

Cosa è?
Un software dannoso che si installa nel tuo dispositivo senza il tuo consenso.

- **Virus**: si diffonde da un file all'altro e può danneggiare il sistema.
- **Trojan**: sembra un programma utile, ma in realtà nasconde una minaccia.
- **Ransomware**: blocca i tuoi file e chiede un riscatto per sbloccarli.
- **Spyware**: spia le tue attività e invia i dati a un hacker.

📌 **Esempio:**
Scarichi un file da un sito non sicuro, e il tuo computer si infetta con un virus che ruba le tue password.

📌 3. Attacco Man-in-the-Middle (MitM)

Cosa è?
Un hacker si inserisce tra due dispositivi che comunicano tra loro, intercettando i dati senza che le vittime se ne accorgano.

📌 Esempio:
Se ti connetti a una rete Wi-Fi pubblica non protetta, un hacker può leggere i tuoi messaggi e le password che inserisci.

📌 4. Attacco DDoS (Distributed Denial of Service)

Cosa è?
Un hacker sovraccarica un sito web o un server con tantissime richieste, fino a mandarlo in tilt e renderlo inaccessibile.

📌 Esempio:
Un attacco DDoS contro un sito di e-commerce può bloccare gli acquisti online per ore.

📌 5. SQL Injection

Cosa è?
Un hacker inserisce comandi malevoli in un sito web vulnerabile per accedere ai database e rubare informazioni.

📌 Esempio:
Un sito di shopping online mal protetto può subire un attacco SQL Injection, permettendo agli hacker di rubare i dati degli utenti.

📌 6. Brute Force Attack

Cosa è?
Un hacker prova tantissime combinazioni di password fino a trovare quella giusta ed entrare in un account.

📌 Esempio:
Se usi una password debole come "123456", un hacker può scoprirla in pochi secondi con un attacco

---

📌 7. Social Engineering

Cosa è?
L'hacker manipola le persone per ottenere informazioni riservate, senza bisogno di hackerare nulla.

📌 Esempio:
Qualcuno chiama fingendosi un tecnico informatico e ti chiede la password per "risolvere un problema".

📌 8. Zero-Day Attack

Cosa è?
Un hacker sfrutta una vulnerabilità di un software **prima** che venga scoperta e corretta dagli sviluppatori.

📌 **Esempio:**
Un bug in un'app di messaggistica potrebbe essere usato dagli hacker per spiare gli utenti prima che venga rilasciato un aggiornamento di sicurezza.

📌 9. Attacco Supply Chain

Cosa è?
Gli hacker attaccano un fornitore di software o hardware per colpire tutte le aziende che lo usano.

📌 **Esempio:**
Se un hacker compromette un aggiornamento di Windows, milioni di computer potrebbero essere infettati.

📌 10. Credential Stuffing

Cosa è?
Un hacker usa combinazioni di email e password rubate da altri siti per entrare nei tuoi account.

📌 **Esempio:**
Se hai usato la stessa password su più siti e uno di questi viene violato, gli hacker possono provare quella password su altri servizi (come Facebook, PayPal, ecc.).

📌 11. Eavesdropping Attack (Intercettazione dati)

Cosa è?
Un hacker ascolta le comunicazioni in rete per rubare informazioni private.

📌 **Esempio:**
Se usi una connessione Wi-Fi non sicura, un hacker può intercettare le tue credenziali di accesso mentre navighi.

📌 12. Clickjacking

Cosa è?
Un sito ingannevole nasconde un pulsante malevolo sotto uno che sembra innocuo, così l'utente clicca senza volerlo.

📌 **Esempio:**
Pensi di cliccare su "Scarica ora", ma in realtà attivi un abbonamento o scarichi un malware.

🔒 Come difendersi?

✓ **Non cliccare su link sospetti** nelle email.
✓ **Usa password complesse e diverse per ogni sito**.

✓ **Attiva l'autenticazione a due fattori (2FA)**.
✓ **Usa solo reti Wi-Fi protette**.
✓ **Mantieni aggiornati i tuoi dispositivi e software**.
✓ **Scarica programmi solo da fonti ufficiali**.

CONSEGUENZE ATTACCHI INFORMATICI (REALI)

1. Attacco WannaCry (2017)

Descrizione: WannaCry è un ransomware che ha infettato oltre 230.000 computer in oltre 150 paesi, bloccando l'accesso ai dati e richiedendo un riscatto in Bitcoin per la loro liberazione. **Impatto:** Ha colpito organizzazioni sanitarie, aziende e governi, causando significative perdite finanziarie e interruzioni dei servizi.

2. Violazione dei dati Equifax (2017)

Descrizione: Equifax, una delle tre grandi agenzie di credito negli Stati Uniti, ha subito una violazione che ha esposto i dati personali di circa 147 milioni di persone. **Impatto:** Informazioni personali come nomi, indirizzi, numeri di telefono e, in alcuni casi, numeri di previdenza sociale sono state compromesse, causando un enorme danno alla reputazione dell'azienda e significative perdite finanziarie.

3. Attacco DDoS su GitHub (2018)

Descrizione: GitHub ha subito un attacco DDoS (Distributed Denial of Service) che ha raggiunto un picco di 1,35 terabit al secondo, uno dei più grandi attacchi di questo tipo mai registrati. **Impatto:** L'attacco ha causato interruzioni temporanee del servizio, ma grazie alle misure di sicurezza implementate, GitHub è riuscito a mitigare l'attacco in poche ore.

4. Phishing su Google (2017)

Descrizione: Un gruppo di hacker ha utilizzato un'email di phishing per ottenere l'accesso a account Google di dipendenti di aziende tecnologiche e di servizi finanziari. **Impatto:** Gli hacker sono riusciti a rubare informazioni sensibili e credenziali, causando potenziali rischi per la sicurezza delle aziende colpite.

5. Attacco NotPetya (2017)

Descrizione: NotPetya è un ransomware che ha colpito aziende in tutto il mondo, causando danni significativi ai sistemi operativi e richiedendo un riscatto per la decriptazione dei dati. **Impatto:** Ha causato danni finanziari enormi, con stime di perdite che superano i 10 miliardi di dollari, e ha colpito aziende come Maersk (azienda di traspoti), Merck (azienda settore chimico) e FedEx.

6. Attacco SYNLAB (2024)

Dettagli dell'Attacco

Tipo di Attacco: Ransomware

Gruppo Criminale: Black Basta

Quantità di Dati Sottratti: Circa 1,5 terabyte di dati sensibili, inclusi dati personali dei pazienti, clienti e analisi mediche.

Impatto: Interruzione dei servizi di prelievo, visite e ritiro dei referti medici. Synlab Italia ha disabilitato tutti i sistemi informatici in via precauzionale e ha istituito una task force per mitigare gli impatti e ripristinare i sistemi2.

Conseguenze

Privacy dei Pazienti: I dati sensibili dei pazienti sono a rischio di pubblicazione e diffusione.

Disagio per i Clienti: Prenotazioni e scaricamenti dei referti medici sono stati sospesi, causando disagi significativi.

Collaborazione con le Autorità: Synlab Italia sta lavorando a stretto contatto con le autorità competenti e le forze dell'ordine per risolvere la situazione.

Synlab Italia ha comunicato che continuerà a fornire aggiornamenti regolari sulla situazione attraverso il proprio sito web e le pagine social. La situazione è ancora in evoluzione e le autorità stanno investigando per identificare e perseguire i responsabili dell'attacco.

COS'E' LA SOCIAL ENGEENERING E COME PROTEGGERSI

La social engineering (ingegneria sociale) è una tecnica utilizzata da hacker o malintenzionati per manipolare le persone al fine di ottenere informazioni confidenziali, accessi non autorizzati o altri dati sensibili. A differenza degli attacchi informatici tradizionali che si concentrano su vulnerabilità tecniche (come virus o malware), la social engineering si concentra sul fattore umano, sfruttando la psicologia e il comportamento delle persone.

Come funziona la Social Engineering?

Gli attacchi di social engineering si basano sulla creazione di situazioni in cui le persone, inconsapevolmente, rivelano informazioni riservate o compiono azioni che mettono a rischio la sicurezza. Alcuni dei metodi più comuni includono:

1. **Phishing:**
   L'attaccante invia un'email che sembra provenire da una fonte affidabile (come una banca o un'azienda) per indurre la vittima a fornire informazioni personali o cliccare su un link che porta a un sito web falso.

2. **Pretexting:**
   L'attaccante si crea una "scusa" (o pretesto) per ottenere informazioni. Ad esempio, potrebbe fingersi un dipendente aziendale e chiedere a un altro dipendente di rivelare dati sensibili, come password o dettagli su una transazione.

3. **Baiting:**
   In questo caso, l'attaccante offre un "esca" per indurre la vittima a compiere un'azione. Ad esempio, potrebbe lasciare un'unità flash USB infetta in un luogo pubblico, sperando che qualcuno la raccolga e la colleghi al proprio computer, infettandolo con malware.

4. **Tailgating (o Piggybacking):**
   L'attaccante cerca di entrare in un'area protetta (come un edificio o una rete) sfruttando la cortesia di qualcun altro. Ad esempio, entra in un ufficio seguendo un dipendente che ha accesso a quella zona, senza che quest'ultimo se ne accorga.

5. **Vishing (Voice Phishing):**
   Simile al phishing, ma viene effettuato tramite chiamate telefoniche. L'attaccante si finge una persona di fiducia (ad esempio, un tecnico di supporto) per ottenere informazioni sensibili da una vittima.

Perché è efficace?

La social engineering sfrutta la fiducia, la curiosità e il comportamento naturale delle persone. Le vittime potrebbero non essere consapevoli dei rischi e possono facilmente cadere in trappole costruite ad arte, come rispondere a un'email che sembra legittima o fornire informazioni senza pensarci due volte.

Come proteggersi dalla Social Engineering?

- **Educazione e consapevolezza:**
  È fondamentale che le persone siano consapevoli dei rischi di social engineering e che imparino a riconoscere i segnali di avvertimento, come messaggi urgenti, richieste inusuali o offerte troppo allettanti.

- **Verifica:**
  Non fidarti mai di comunicazioni non richieste. Se ricevi una richiesta di informazioni sensibili via email, telefono o social media, verifica sempre la sua autenticità contattando direttamente l'organizzazione o la persona coinvolta.

- **Evita di cliccare su link sospetti:**
  Non cliccare su link contenuti in email o messaggi che non ti sembrano legittimi. Controlla sempre l'indirizzo URL prima di inserire qualsiasi informazione personale.

- **Autenticazione a due fattori (2FA):**
  Utilizzare la **verifica in due passaggi** per aggiungere un ulteriore livello di sicurezza ai tuoi account online, rendendo più difficile l'accesso non autorizzato anche se qualcuno riesce a ottenere la tua password.

La social engineering si basa sulla manipolazione psicologica ed è uno dei metodi più efficaci per compromettere la sicurezza di un sistema, quindi è fondamentale essere sempre vigili e non dare mai per scontato che una richiesta sia legittima.

POLITICA "ZERO TRUST"

Ecco i principi chiave delle politiche Zero Trust:

1. **Verifica Continua:** Ogni tentativo di accesso viene verificato e autenticato in tempo reale, senza dare per scontato che un utente o dispositivo sia affidabile solo perché è già all'interno della rete aziendale.
2. **Minimizzazione dei Permessi:** Gli utenti e i dispositivi vengono forniti solo con i permessi minimi necessari per svolgere le loro funzioni. Questo riduce il rischio di danni in caso di compromissione.
3. **Segmentazione della Rete:** La rete aziendale viene suddivisa in segmenti più piccoli e sicuri, in modo che l'accesso a una parte della rete non garantisca automaticamente l'accesso ad altre parti.
4. **Monitoraggio e Analisi:** Le attività e i comportamenti degli utenti e dei dispositivi vengono costantemente monitorati e analizzati per rilevare eventuali anomalie o comportamenti sospetti.
5. **Autenticazione Multifattoriale:** L'implementazione di autenticazione a più fattori (MFA) per aggiungere ulteriori livelli di verifica all'accesso, rendendo più difficile per gli attaccanti compromettere i sistemi.

Adottare Zero Trust significa migliorare la sicurezza aziendale e personale, riducendo la possibilità di attacco e migliorando la protezione dei dati.