COS'E' LA CYBERSICURITY

La Cybersecurity consiste nel difendere computer, server, dispositivi mobili, sistemi elettronici, reti e dati dagli attacchi dannosi. È anche conosciuta come sicurezza informatica o sicurezza delle informazioni elettroniche. La Cybersecurity si applica a vari contesti, dal business al mobile computing, e può essere suddivisa in diverse categorie.

• **Sicurezza di rete:** consiste nella difesa delle reti informatiche dalle azioni di malintenzionati, che si tratti di attacchi mirati o di malware opportunistico.

• **Sicurezza delle applicazioni:** ha lo scopo di proteggere software e dispositivi da eventuali minacce. Un'applicazione compromessa può consentire l'accesso ai dati che dovrebbe proteggere. Una sicurezza efficace inizia dalla fase di progettazione, molto prima del deployment di un programma o di un dispositivo.

• **Sicurezza delle informazioni:** protegge l'integrità e la privacy dei dati, sia quelle in archivio che quelle temporanee.

• **Sicurezza operativa:** include processi e decisioni per la gestione e la protezione degli asset di dati.
Comprende tutte le autorizzazioni utilizzate dagli utenti per accedere a una rete e le procedure che determinano come e dove possono essere memorizzati o condivisi i dati.

• **Disaster recovery e business continuity:** si tratta di strategie con le quali l'azienda risponde a un incidente di Cybersecurity e a qualsiasi altro evento che provoca una perdita in termini di operazioni o dati. Le policy di disaster recovery indicano le procedure da utilizzare per ripristinare le operazioni e le informazioni dell'azienda, in modo da tornare alla stessa capacità operativa che presentava prima dell'evento. La business continuity è il piano adottato dall'azienda nel tentativo di operare senza determinate risorse.

• **Formazione degli utenti finali:** riguarda uno degli aspetti più importanti della Cybersecurity: le persone. Chiunque non rispetti le procedure di sicurezza rischia di introdurre accidentalmente un virus in un sistema altrimenti sicuro. Insegnare agli utenti a eliminare gli allegati e-mail sospetti, a non inserire unità USB non identificate e ad adottare altri accorgimenti importanti è essenziale per la sicurezza di qualunque azienda.

L'importanza delle minacce informatiche

A livello globale, le minacce informatiche continuano a evolversi rapidamente e il numero di data breach aumenta ogni anno. La maggior parte delle violazioni, imputabili a criminali malintenzionati, ha colpito servizi medici, rivenditori ed enti pubblici. Alcuni di questi settori sono particolarmente interessanti per i cybercriminali, che raccolgono dati medici e finanziari, ma tutte le aziende connesse in rete possono essere colpite da violazioni dei dati, spionaggio aziendale o attacchi ai clienti.

Tipologie di cyberminacce

La Cybersecurity ha lo scopo di contrastare tre diversi tipi di minacce:

1. Cybercrimine: include attori singoli o gruppi che attaccano i sistemi per ottenere un ritorno economico o provocare interruzioni nelle attività aziendali.

2. Cyberattacchi: hanno spesso lo scopo di raccogliere informazioni per finalità politiche.

3. Cyberterrorismo: ha lo scopo di minare la sicurezza dei sistemi elettronici per suscitare panico o paura.

Di seguito sono illustrati alcuni dei metodi comunemente utilizzati per minacciare la Cybersecurity:

Malware

Malware è la contrazione di "malicious software" (software malevolo). Il malware, una delle minacce informatiche più comuni, è costituito da software creato da cybercriminali o hacker con lo scopo di danneggiare o provocare il malfunzionamento del computer di un utente legittimo. Spesso diffuso tramite allegati e-mail non richiesti o download apparentemente legittimi, il malware può essere utilizzato dai cybercriminali per ottenere un guadagno economico o sferrare cyberattacchi per fini politici. Esistono numerosi tipi di malware, tra cui:

• **Virus:** è un programma capace di replicarsi autonomamente, che si attacca a un file pulito e si diffonde nell'intero sistema informatico, infettandone i file con il suo codice malevolo.

• **Trojan:** è un tipo di malware mascherato da software legittimo. I cybercriminali inducono gli utenti a caricare Trojan nei propri computer, dove possono causare danni o raccogliere dati.

• **Spyware:** è un programma che registra segretamente le azioni dell'utente, per consentire ai cybercriminali di sfruttare tali informazioni a proprio vantaggio. Ad esempio, lo spyware può acquisire i dati delle carte di credito.

• **Ransomware:** malware che blocca l'accesso ai file e ai dati dell'utente, minacciandolo di cancellarli se non paga un riscatto.

• **Adware:** software pubblicitario che può essere utilizzato per diffondere malware.

• **Botnet:** reti di computer infettati da malware, utilizzate dai cybercriminali per eseguire task online senza l'autorizzazione dell'utente.

Immissione di codice SQL

L'immissione di codice SQL (Structured Language Query) è un tipo di cyberattacco con lo scopo di assumere il controllo di un database e rubarne i dati. I cybercriminali sfruttano le vulnerabilità nelle applicazioni data-driven per inserire codice malevolo in un database tramite un'istruzione SQL dannosa, che consente loro di accedere alle informazioni sensibili contenute nel database.

Phishing

In un attacco di phishing, i cybercriminali inviano alle vittime e-mail che sembrano provenire da aziende legittime, per richiedere informazioni sensibili. Gli attacchi di phishing hanno solitamente lo scopo di indurre gli utenti a fornire i dati della carta di credito o altre informazioni personali.

Attacco Man-in-the-Middle

Un attacco Man-in-the-Middle è una minaccia informatica in cui un cybercriminale intercetta le comunicazioni fra due persone allo scopo di sottrarre dati. Ad esempio, su una rete Wi-Fi non protetta, l'autore dell'attacco può intercettare i dati scambiati fra il dispositivo della vittima e la rete.

Attacco Denial of Service

In un attacco Denial of Service i cybercriminali impediscono a un sistema informatico di soddisfare le richieste legittime, sovraccaricando reti e server con traffico eccessivo. In questo modo il sistema risulta inutilizzabile, impedendo all'azienda di svolgere funzioni vitali.

Consigli di Cybersecurity: come proteggersi dai cyberattacchi

Cosa devono fare aziende e singoli utenti per proteggersi dalle minacce informatiche? I nostri migliori consigli di Cybersecurity sono riportati di seguito:

1. **Aggiornare il software e il sistema operativo**: questo permette di sfruttare le patch di sicurezza più recenti.
2. **Utilizzare software antivirus:** soluzioni di sicurezza come software antivirus sono in grado di rilevare e rimuovere le minacce. Il software deve essere aggiornato regolarmente per garantire il massimo livello di protezione.

3. **Utilizzare password complesse:** assicuratevi di utilizzare password difficili da indovinare.
4. **Non aprire allegati e-mail di mittenti sconosciuti:** potrebbero essere infettati dal malware.
5. **Non fare clic sui link contenuti nei messaggi e-mail di mittenti sconosciuti o in siti web non familiari:** è un metodo comune per diffondere il malware.
6. **Evitare di utilizzare reti Wi-Fi non protette negli spazi pubblici:** le reti pubbliche espongono i dispositivi agli attacchi Man-in-the-Middle.