Cos'è la Cybersecurity?

La cybersecurity è la pratica di proteggere computer, server, dispositivi mobili, sistemi elettronici, reti e dati da attacchi dannosi. È anche conosciuta come sicurezza informatica o sicurezza delle informazioni elettroniche.
Il termine "cybersecurity" si applica in una varietà di contesti, che spaziano dal mondo aziendale al mobile computing, e può essere suddiviso in alcune categorie comuni.

- **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. Da un report di RiskBased Security emerge che, solo nel 2019, ben 7,9 miliardi di record sono stati esposti a data breach, più del doppio (112%) del numero dei record esposti nel 2018.

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.

Come conseguenza della continua crescita delle minacce informatiche, gli investimenti globali per le soluzioni di cybersecurity stanno aumentando. Gartner prevede che gli investimenti relativi alla cybersecurity raggiungeranno i 188,3 miliardi di dollari nel 2023 e supereranno i 260 miliardi di dollari entro il 2026. I governi di tutto il mondo hanno risposto a questo aumento delle minacce informatiche pubblicando indicazioni per aiutare le aziende a implementare procedure di Cybersecurity efficaci.

Negli Stati Uniti, il National Institute of Standards and Technology (NIST) ha creato un framework di Cybersecurity. Per contrastare la proliferazione del codice malevolo e agevolarne l'individuazione precoce, questo framework raccomanda il monitoraggio continuo e in tempo reale di tutte le risorse elettroniche.

L'importanza del monitoraggio dei sistemi è ribadita anche nel documento "10 steps to cyber security" fornito dal National Cyber Security Centre del governo britannico. In Australia, il Australian Cyber Security Centre (ACSC) pubblica regolarmente indicazioni per contrastare le nuove minacce alla Cybersecurity all'interno delle aziende.

Tipi di attacchi informatici

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.

Ma come fanno questi malintenzionati a ottenere il controllo di un sistema informatico? 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 scaricare il 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 attività 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.

Principali minacce informatiche al giorno d'oggi

Quali sono le nuove minacce informatiche da cui aziende e utenti devono proteggersi? Di seguito sono riportate alcune delle minacce informatiche più recenti segnalate dai governi di Regno Unito, Stati Uniti e Australia.

Malware Dridex

Nel dicembre 2019, il dipartimento di giustizia (DoJ, Department of Justice) statunitense ha accusato il leader di un'organizzazione cybercriminale di aver partecipato a un **attacco con malware Dridex** sferrato a livello globale. Questa campagna malevola ha colpito il pubblico, i governi, le infrastrutture e le aziende di tutto il mondo.

Dridex è un Trojan finanziario con varie capacità. Diffuso fin dal 2014, infetta i computer tramite e-mail di phishing o malware esistente. È in grado di rubare password, dati bancari e informazioni personali, che possono essere utilizzati per transazioni fraudolente, e ha causato enormi perdite finanziarie, dell'ordine delle centinaia di milioni di dollari.

Per rispondere agli attacchi Dridex, il National Cyber Security Centre britannico consiglia al pubblico di "assicurarsi che i dispositivi siano dotati di patch, verificare che l'antivirus sia attivato e aggiornato ed eseguire un backup dei file".

Truffe a sfondo sentimentale

Nel febbraio 2020 l'FBI ha invitato i cittadini statunitensi a prestare attenzione al furto di informazioni riservate da parte di cybercriminali che utilizzano siti, chat room e app di appuntamenti. I malintenzionati approfittano di persone in cerca di nuovi partner, inducendo le vittime a fornire i propri dati personali.

Secondo i **report dell'FBI**, nel 2019 le minacce informatiche a sfondo sentimentale hanno colpito 114 vittime nel New Mexico, producendo perdite finanziarie per 1,6 milioni di dollari.

Malware Emotet

Alla fine del 2019, l'Australian Cyber Security Centre ha segnalato alle organizzazioni nazionali la diffusione di una minaccia informatica globale basata sul malware Emotet.

Emotet è un sofisticato Trojan in grado di rubare dati e di caricare altro malware. Emotet sfrutta le password più elementari. Questo ci ricorda l'importanza di creare una password sicura per proteggersi dalle minacce informatiche.

Protezione dell'utente finale

La protezione dell'utente finale, o endpoint security, è un aspetto cruciale della Cybersecurity. Dopo tutto, sono spesso le persone (gli utenti finali) a scaricare accidentalmente malware o altri tipi di minacce informatiche nei propri pc, computer portatili o dispositivi mobili.

Quindi, in che modo le misure di Cybersecurity proteggono gli utenti finali e i loro sistemi? La Cybersecurity utilizza protocolli crittografici per crittografare messaggi e-mail, file e altri dati importanti. Oltre a proteggere le informazioni in transito, questo consente anche di tutelarsi contro perdite o furti.

Inoltre, il software di sicurezza degli utenti finali esegue la scansione del computer per rilevare il codice dannoso, metterlo in quarantena e successivamente rimuoverlo dal sistema. I programmi di sicurezza possono addirittura rilevare e rimuovere il **codice malevolo nascosto nel Master Boot Record** (MBR) e sono progettati per crittografare o cancellare i dati sul disco rigido del computer.

I protocolli di sicurezza elettronica si prefiggono inoltre di **rilevare il malware** in tempo reale. Molti di essi utilizzano l'analisi euristica e comportamentale per monitorare il comportamento di un programma e del suo codice, al fine di proteggersi da virus o Trojan che cambiano forma a ogni esecuzione (malware polimorfico e metamorfico). I programmi di sicurezza possono confinare i programmi potenzialmente dannosi in una bolla virtuale separata dalla rete dell'utente, per analizzarne il comportamento e determinare come rilevare più efficacemente le nuove infezioni.

I programmi di sicurezza continuano a sviluppare nuove difese, a mano a mano che gli esperti di Cybersecurity identificano nuove minacce e nuovi modi per combatterle. Per ottenere il massimo dal software di sicurezza degli utenti finali, occorre insegnare ai dipendenti come utilizzarlo. Soprattutto, mantenendolo costantemente in funzione e aggiornandolo di frequente, è possibile proteggere gli utenti dalle nuove minacce informatiche.

Consigli di Cybersecurity: come proteggersi dagli attacchi informatici

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 Kaspersky Total Security 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.

Articoli correlati:

- Cos'è il cybercrimine: rischi e prevenzione
- Come evitare molti tipi di cybercrimini
- Minacce alla sicurezza provenienti dalla Internet of Things
- Cosa sono gli spam e le truffe di phishing