Cybersecurity, cos'è e perché è importante

(Fonte: https://www.agendadigitale.eu/)

La Cyber Security rappresenta un campo relativo alla **sicurezza informatica**: strumenti e tecnologie la cui funzione è quella di proteggere i sistemi informatici dagli attacchi dall'esterno.
La **sicurezza informatica** si basa sulla protezione della confidenzialità, integrità e disponibilità di un sistema informatico. Caratteristiche cui si aggiunge l'autenticità delle informazioni.
Nella Cyber Security sono presenti elementi giuridici, umani, tecnici e organizzativi in grado di analizzare i punti vulnerabili di un sistema, le minacce e i rischi associati.
La cyber security che rientra nel campo della sicurezza informatica, assume un risvolto particolarmente delicato quando applicata alle aziende e alle imprese più in generale.
Se da un lato i vecchi metodi di sicurezza informatica sono stati concepiti per proteggere i dati locali, le strategie di sicurezza informatica aziendale includono un controllo dei flussi di dati che viaggiano tra dispositivi wireless e server cloud.
Ciò significa che la sicurezza informatica aziendale basa la protezione dell'infrastruttura on-premise nel cloud, nonché sul controllo di fornitori di terze parti e sulla protezione del numero crescente di endpoint connessi alla rete tramite l'Internet of Things (IoT).
In questo canale tutti gli articoli relativi al tema della sicurezza informatica. Leggi anche gli approfondimenti sul sito Cybersecurity360.

Che cos'è la sicurezza informatica aziendale?

La sicurezza informatica aziendale è la pratica di **protezione dei dati** e delle risorse aziendali dalle minacce informatiche. Utilizza i tradizionali metodi di sicurezza informatica per proteggere i dati a livello locale ed estende tale idea al trasferimento di dati attraverso reti, dispositivi e utenti finali.
La sicurezza informatica aziendale affronta problemi di sicurezza comuni come **attacchi DoS Denial-of-Service (DoS) o DDos (Distributed Denial of Service)**, ingegneria sociale e vulnerabilità del software, ma tiene anche conto del modo in cui i dati vengono trasferiti tra dispositivi e reti all'interno dell'organizzazione nel suo insieme.

Cosa si intende per Cyber Security?

Quando pensiamo alla sicurezza informatica solitamente ci soffermiamo sulla sicurezza dei dati personali e a come proteggere i nostri dispositivi. Tuttavia, c'è un altro modo di intendere la sicurezza informatica che include tutto il mondo aziendale.
Per stabilire il confine entro cui finisce la sicurezza informatica e inizia la cyber security, possiamo partire dal tipo di dati che dovranno essere protetti.

La cyber security si occupa della protezione dei dati da accessi non autorizzati mentre la sicurezza informatica, si occupa di proteggere i dati più in generale e dunque anche da accessi legali e autorizzati.
Per le aziende, queste due forme di sicurezza, informatica e cyber security sono egualmente importanti. Difatti, circa un terzo di tutte le aziende di tutte le dimensioni ha subito violazioni negli ultimi anni.

Quali sono gli obblighi in materia di Nis 2 e Cybersecurity?
La Direttiva NIS2 (Direttiva (UE) 2022/2555) rappresenta un aggiornamento fondamentale nella legislazione dell'Unione Europea per la cybersecurity. È entrata in vigore il 17 gennaio 2023 e mira a stabilire una strategia comune di sicurezza informatica tra gli Stati membri. Questo aggiornamento è stato necessario per **affrontare le minacce informatiche che sono diventate sempre più sofisticate e pervasive negli ultimi anni**.
La NIS2 prevede requisiti più stringenti rispetto alla precedente Direttiva NIS, ampliando il suo ambito di applicazione a un maggior numero di settori considerati critici. Include, tra gli altri, fornitori di servizi cloud, data center e servizi sanitari. La direttiva stabilisce anche un quadro dettagliato per le misure di sicurezza, richiedendo un approccio multirischio e la segnalazione tempestiva di incidenti significativi alle autorità competenti.
Le organizzazioni soggette alla Direttiva NIS2 devono adottare diverse misure, tra cui la **gestione dei rischi**, la continuità operativa, la sicurezza della supply chain, e l'uso di soluzioni di autenticazione a più fattori. La direttiva enfatizza anche l'importanza della governance della sicurezza informatica e della formazione continua per i dipendenti.
La conformità alla NIS2 non è solo un obbligo legale, ma rappresenta anche un'opportunità strategica per le organizzazioni per migliorare la loro sicurezza informatica, rafforzare la fiducia dei consumatori e aumentare la competitività sul mercato.
La **Direttiva NIS 2** (Network and Information Security Directive) rappresenta un importante passo avanti nell'ambito della cybersecurity in Europa. È stata introdotta per migliorare la sicurezza delle reti e dei sistemi informativi in tutta l'Unione Europea. Ecco alcuni punti chiave:

- Protezione rafforzata: **La NIS 2 mira a rafforzare la sicurezza** delle infrastrutture critiche, come energia, trasporti, salute e finanza, richiedendo agli Stati membri di garantire un elevato livello di sicurezza informatica.
- Obblighi per le aziende: **Le aziende sono obbligate a implementare la Nis 2** per ottenere misure di sicurezza adeguate e a segnalare gli incidenti di sicurezza alle autorità competenti. Questo include la gestione dei rischi, la sicurezza della supply chain e la condivisione di informazioni sulle minacce.
- Amplia la portata: Rispetto alla prima direttiva NIS, la NIS 2 amplia la portata includendo più settori e servizi digitali, come i **fornitori di servizi cloud** e le piattaforme online.

- Collaborazione e condivisione delle informazioni: La direttiva promuove la cooperazione e la condivisione delle informazioni tra gli Stati membri per migliorare la capacità di risposta agli incidenti di sicurezza informatica.
- Sanzioni per chi non applica la Nis 2: Sono previste sanzioni severe per le aziende che non rispettano le misure di sicurezza richieste dalla Nis 2, incentivando così l'adozione di pratiche di sicurezza più rigide.

FAQ: Tutto su Cyber Security

Quali sono le principali minacce alla cybersecurity?

Perché la cybersecurity è importante per le aziende?

Quali sono le principali normative sulla cybersecurity in Europa?

Come proteggere un'azienda dalle minacce informatiche?

Qual è il ruolo del fattore umano nella cybersecurity?

Quali sono i framework di cybersecurity più utilizzati?

Come formarsi per lavorare nel settore della cybersecurity?

Quali sono le principali lacune nella cybersecurity in Italia?

Come sta evolvendo la cybersecurity in Italia?

Che cos’è la sicurezza informatica aziendale?

Cosa si intende per Cyber Security?

Quali sono gli obblighi in materia di Nis 2 e Cybersecurity?

FAQ generate con l'AI, a cura della Redazione