bitCorp™

IL RUOLO STRATEGICO DELLA CYBERSECURITY A TUTELA DI AZIENDE E LAVORATORI

- Milano, 17 giugno 2021

INDICE

INTRODUZIONE

Il tema della sicurezza informatica, detta anche Cybersecurity[1], è stato particolarmente sentito nel tempo, specie a seguito della digitalizzazione[2] della civiltà che ha portato dati, informazioni, cose e persone, ad essere sempre più vulnerabili.

Se nel suo complesso Internet[3] rappresenta un bene al servizio di tutti, ma il risvolto nefasto della sua stessa medaglia risiede nella proliferazione di minacce cyber: spionaggi, frodi, furti, attacchi terroristici, disordini sociali, guerre a colpi di bit.

Sappiamo quanto geniale possa essere il potere di un computer, ma abbiamo anche cognizione di quanto possa rivelarsi distruttivo se posto nelle mani sbagliate. In questo quadro di pericoli, rivolgersi ad esperti di sicurezza informatica può fare davvero la differenza!

CYBERCRIME E CYBERSECURITY: FOCUS SULLE MINACCE GLOBALI

L' Associazione Italiana per la Sicurezza Informatica ha più volte dimostrato che i crimini informatici rappresentano la prima vera **minaccia globale**, riversandosi sulle faglie di numerose categorie di enti, aziende e settori. I rischi riscontrati in ambienti motivi, GDO, aziende farmaceutiche, imprese manifatturiere, e-commerce e non solo, sono proliferati a seguito dell'avvento di Internet.

Alla luce delle crescenti minacce di Cybercrime diviene fondamentale intervenire per tempo, realizzando infrastrutture atte a ridurre la vulnerabilità dei sistemi.

La Cybersecurity svolge un ruolo centrale nella tutela di aziende e persone, grazie a soluzioni mirate ed efficienti che permettono di prevenire e risolvere ogni fragilità sistemica.

CHE COS'È IL CYBERCRIME: DEFINIZIONE

Il termine Cybercrime sintetizza la più nota espressione di "**Reato Informatico**". Rientrano in questa definizione tutte quelle azioni realizzate con l'uso di nuove tecnologie, aventi finalità di danneggiamento o distruzione, sanzionate dall'ordinamento penale. Si tratta dunque di attività illecite, generalmente realizzate per mezzo di una connessione a Internet e un computer, che possono arrivare ad arrecare danni incredibili.

LE QUATTRO PRINCIPALI CATEGORIE DI CYBERCRIME

Ogni reato informatico appartiene ad una precisa categoria. Le più note e principali categorie di Cybercrime sono così riassumibili:

[1] https://innovazione.gov.it/notizie/articoli/il-ruolo-strategico-della-cybersecurity/
[2] https://it.wikipedia.org/wiki/Digitalizzazione
[3] https://argomenti.ilsole24ore.com/internet.html?refresh_ce=1

1. reati contro l'integrità di dati e sistemi informatici
2. reati contro la riservatezza di informazioni informatiche
3. reati di falsificazione
4. reati di frode

Ognuna di queste aree racchiude una mole di sotto categorie che danno vita a precise operazioni offensive ai danni di un'azienda, di un ente, di una o più persone.

CYBERSECURITY E STRATEGIA EUROPEA

Il tema della sicurezza informatica, come abbiamo anticipato all'inizio, è molto sentito, specie in quelle aree gestionali in cui si ingorgano molteplici interessi: dati, informazioni, soldi. L'Unione Europea in tema di Cybersecurity ha mostrato di essere in una posizione "guida". La stessa è stata creata nell'idea di poter configurare un esempio da seguire per il rafforzamento dei punti di vulnerabilità di ciascun ente, o soggetto, interessato da reati cibernetici.

La strategia scelta dall'UE si è fondata su tre pilastri fondamentali:

1. l'implementazione degli strumenti di difesa dei sistemi informatici di tutti gli stati membri
2. attuazione di tecniche di prevenzione di attacchi informatici
3. impiego di misure di difesa e controllo dei canali di condivisione delle informazioni

Il gruppo delle aree di intervento così inteso rappresenta una configurazione standard da attuare sia a livello nazionale che internazionale, passando per il canale privato.

CYBERSECURITY: QUANTO PUÒ FARE PER TUTELARCI DAI RISCHI INFORMATICI?

Alla luce delle crescenti preoccupazioni derivanti dai possibili reati informatici, diviene fondamentale intervenire per fotografare la propria situazione di base e attuare le soluzioni relative al caso concreto. Rivolgersi a specialisti di Cybersecurity può eliminare le criticità in favore di un ambiente sicuro, controllato e protetto.

Le organizzazioni che hanno la necessità di memorizzare dati e informazioni sono all'ordine del giorno e, per loro, un servizio specialistico diverrebbe risolutivo per problemi di:

- spionaggio informatico
- hacking
- ingresso di virus informatici
- spamming
- sottrazione di dati e/o risorse economiche

Si tenga presente, che i reati elencati spesso sono frutto di una concatenazione di azioni criminose, volte al complessivo danneggiamento della propria attività. Talvolta, alla gradualità delle operazioni svolte è possibile associare una proporzionale gravità dei risultati.

CYBERSECURITY A TUTELA DELL' AMBIENTE FISICO E INFORMATICO

Rivolgersi ad un'azienda specializzata in servizi di sicurezza informatica significa tutelarsi da una molteplicità di casi: dalla sicurezza fisica a quella informatica.

Difesa Fisica

Appartiene a questa area di intervento lo sviluppo di soluzioni di controllo di accessi ed uscite di flussi di persone. Gli strumenti utilizzati a questo fine sono di tipo prettamente informatico e di videosorveglianza.

Difesa Informatica

Quest'area di competenza si snoda in una serie di accurati passaggi di analisi delle condizioni iniziali del contesto nel quale si è chiesto l'intervento specialistico. Il percorso di indagine e innesto delle soluzioni è sintetizzabile come segue:

1. **Analisi di Compliance**, volta a verificare il concreto rispetto delle normative attualmente in vigore quali, GDPR, Direttiva NIS, standard ISO/IEC 27001.

2. **Indagine di Risk Management**, mirante alla cristallizzazione di tutte le criticità rilevate dalla Vulnerability Assessment, dai Penetration e Application Test, dall'Asset Inventory, dal Disaster Recovery Plan, dal Business Continuity Plan.

3. **Asset Management**, in grado di rilevare ogni fragilità nel sistema di Email, nei collegamenti mobile aziendali, nella rete Internet aziendale, e in ogni altra sede di passaggio di dati e informazioni.

4. **User Management**, rivolta esclusivamente all'analisi dei passaggi di Accesso ai software. Essa si esprime con le operazioni di Identity Access Management, Access Security e Process Access.

Alla luce di quanto descritto, intervenire all'inizio di qualunque attività intrapresa significa mettersi al riparo da ogni possibile rischio informatico.

Se vuoi una consulenza gratuita, scopri cosa possiamo fare per te. Noi di bitCorp saremo lieti di darti una mano!