Sicurezza informatica aziendale: si parte dalla consapevolezza (di tutti)

Con l'aumentare degli attacchi hacker ai danni delle aziende e delle pubbliche amministrazioni di tutto il mondo, il tema della sicurezza dei sistemi e delle reti informatiche ha cominciato a rivestire un ruolo di primaria importanza per molti dirigenti. La parola d'ordine in questo caso è sicurezza informatica (indicata anche con il termine inglese "*cyber security*")

In questo articolo vedremo:

- ☞ **Cosa si intende per sicurezza informatica;**
- ☞ **Perché è importante proteggere la propria infrastruttura IT;**
- ☞ **Come ridurre i rischi legati al mondo digitale.**

Cosa si intende per sicurezza informatica

Per **sicurezza informatica** si intendono una serie di tecnologie e mezzi volti alla protezione dei sistemi informatici aziendali e dei dati sensibili, in termini di:

- **disponibilità,**
- **integrità dei dati,**
- **autenticità e**
- **riservatezza delle informazioni.**

Perché la sicurezza informatica è importante?

Ancora oggi la maggior parte delle PMI sostiene di non trattare dati aziendali tali da giustificare un possibile attacco informatico. **Purtroppo la strategia vincente di chi attacca e danneggia fa leva sulla mancanza di prevenzione e NON si limita alle grandi aziende o alla Pubblica Amministrazione**. Spesso, infatti, i bersagli sono piccole e medie imprese, proprio perché più vulnerabili.

Gli **effetti collaterali di un attacco informatico** posso essere molteplici:

- Pc rallentato e conseguente rallentamento dei processi aziendali
- Compromissione di server aziendali
- Perdita, furto o fuoriuscita di informazioni aziendali e/o di dati sensibili
- Danneggiamento dell'attività aziendale (Business Continuity)
- Danno all'immagine
- Conseguenze legali (*GDPR*)

*Il **regolamento generale sulla protezione dei dati** (RGPD, in inglese GDPR, General Data Protection Regulation- Regolamento UE 2016/679) è un Regolamento con il quale la Commissione europea intende rafforzare e rendere più omogenea la protezione dei dati personali di cittadini dell'Unione Europea e dei residenti nell'Unione Europea, sia all'interno che all'esterno dei confini dell'Unione europea (UE).*

*Il testo, pubblicato sulla Gazzetta Ufficiale Europea il 4 maggio 2016 ed entrato in vigore il 25 maggio dello stesso anno, inizierà ad avere efficacia **il 25 maggio 2018**.*

Fonte: https://it.wikipedia.org/wiki/Regolamento_generale_sulla_protezione_dei_dati

Come ridurre i rischi legati al mondo digitale?

Partendo dal presupposto che una sicurezza totale garantita al 100% è un'utopia, è comunque sempre bene ricordare che occorre attuare una vera e propria strategia proattiva.

Ciò significa che non è pensabile per un'impresa che voglia proteggere i propri asset guardare alla sicurezza informatica come un'attività "one time" ma come un insieme di attività che tenga conto per esempio di azioni quali:

- **l'identificazione delle aree critiche**
- **la gestione dei rischi dei sistemi e della rete, delle vulnerabilità e degli incidenti**
- **il controllo degli accessi**
- **la gestione della privacy e della compliance**
- **la valutazione dei danni, ecc**

Le possibili modalità di cyber attack sono molteplici, servono dunque politiche che predispongano azioni organizzative e scelte tecniche tali da coprire tutte le aree della security, interponendo barriere fra l'attaccante e l'obiettivo.

Quali sono le principali misure di sicurezza (hardware o software) da implementare nella propria azienda per ridurre i rischi di un attacco informatico?

☞ **Antivirus**: è un software programmato per prevenire, rilevare ed eventualmente rendere inoffensivi codici dannosi, noti anche come malware. Su internet si possono facilmente trovare numerosi antivirus gratis; al giorno d'oggi, tuttavia, un "classico" Antivirus non è in grado di proteggere un computer da tutte le minacce esistenti. Spesso infatti non proteggono da attacchi cibernetici, criptolocker, advanced persistent threat (APT), botnets, DDoS attack, phishing, scams, social engineering e nemmeno dall'odioso spam.

☞ **Firewall**: Un firewall è un componente per la sicurezza informatica con lo scopo di controllare gli accessi alle risorse di un sistema filtrando tutto il traffico che tale sistema scambia con l'esterno. Il sistema, che si suppone sicuro e attendibile, protetto dal firewall può essere un singolo computer o una rete di computer (detta rete interna o rete locale o rete privata) mentre l'ambiente esterno con cui interagisce è tipicamente una rete che si suppone sconosciuta, insicura e non attendibile (detta rete esterna o rete pubblica).

☞ **Backup**: L'attività di backup è un aspetto fondamentale della gestione di un computer: in caso di guasti, manomissioni, furti, smarrimenti, attacchi da parte di malware, ecc., ci si assicura che esista una copia dei dati, assicurando quindi una ridondanza logico/fisica dei dati. Anche se i backup rappresentano una semplice forma di disaster recovery e dovrebbero sempre essere all'interno di un piano di questo tipo, un semplice backup non è considerabile come piano di disaster recovery completo. La ragione per questa affermazione è che non tutti i sistemi di backup sono in grado di ricostruire interamente un sistema informatico o un'altra configurazione complessa come un computer cluster, server directory attivo o server database semplicemente con il ripristino dei dati.

☞ **Disaster Recovery**: si intende l'insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture IT a fronte di gravi emergenze che intacchino la regolare attività aziendale (business continuity). L'impatto di tali emergenze è tale che si stima che la maggior parte delle imprese che hanno subito disastri con pesanti perdite di dati, circa il 43% non ha più ripreso l'attività, il 51% ha chiuso entro due anni e solo il 6% è riuscita a sopravvivere nel lungo termine. I disastri informatici con ingenti perdite di dati nella maggioranza dei casi possono provocare il fallimento dell'impresa o dell'organizzazione, ragion per cui investire in opportune strategie di recupero diventa una scelta quasi obbligata.

In conclusione, l'obiettivo della sicurezza informatica è preservare il patrimonio di conoscenza dell'azienda e garantire la continuità operativa.

La sicurezza informatica non è un prodotto ma è un processo aziendale che coinvolge persone e macchine, PC e software: la raccomandazione è di definire prima il processo e poi selezionare con cura strumenti e prodotti necessari a supportarlo.