Firewall perimetrale e sicurezza informatica a 360 gradi

Come possiamo proteggere la nostra rete dagli attacchi esterni ed interni ?

Sentiamo spesso parlare di firewall, antivirus, backup etc etc, ma davvero sappiamo cosa sono e in che modo possono aiutarci ?

Iniziamo a parlare delle minacce che ci provengono dall'esterno.

Il web, e internet in generale, è sempre di più uno strumento ed un partner fondamentale per l'attività di ogni azienda. Per farsene un'idea basti pensare al rapporto con clienti e fornitori, tramite tramite email e form di contatto, alla gestione degli ordini, fatturazione elettronica, formazione a distanza, telelavoro etc etc…

Quello che spesso ci dimentichiamo è che, **ogni volta che comunichiamo con un server esterno, permettiamo allo stesso server esterno di comunicare a sua volta con noi**. Sembra una considerazione scontata e banale ma se ci riflettete un attimo scoprirete che non è affatto così.

> ***Ogni volta che apro una connessione con l'esterno permetto a qualcosa di esterno di entrare nella mia rete***

E cosa si intende con "aprire una connessione verso l'esterno" ?

Per aprire una connessione con l'esterno è sufficiente aprire un sito web, scaricare le email, cliccare su un link, leggere le news, partecipare ad un webinar etc etc. Come potete vedere sono tutte attività che fanno parte della nostra vita quotidiane e che fanno parte ormai della normalità.

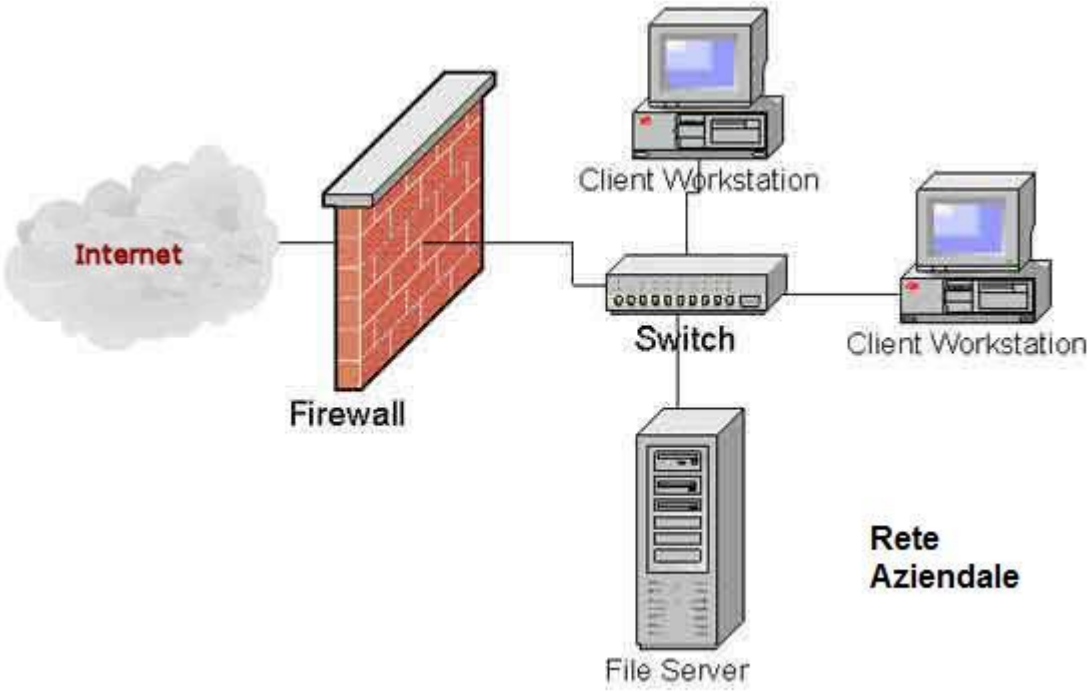
In questo caso le minaccie possono essere varie e molteciplì:

- Un qualcosa che ci viene iniettato tramite una comunicazione.

- Un soggetto che, spacciandosi per qualcun altro, ci invita a compiere delle operazioni **(PHISHING)**.
- Il tentativo di prendere il controllo delle nostre macchine e della nostra rete e usare le nostre risorse per attaccare altre reti **(BOTNET)** o per provocare una interruzione del servizio **(Denial Of Service).**
- L'installazione di cryptovirus per chiedere un successivo riscatto **(Ransomware).**
- L'installazione dei **virus miner** che utilizzano la potenza di calcolo delle macchine della tua rete per estrarre crypto valuta.

e potremmo andare avanti per ore ad elencare tutti i pericoli ai quali ci esponiamo **con un semplice click.**

Per proteggersi dalle minacce che arrivano dall'esterno è necessario dotarsi di un firewall perimetrale. Il **Firewall perimetrale**, a differenza del personal firewall che è installato sulle singole macchine, viene posizionato come **una vera e propria sentinella** tra la nostra rete e la rete internet. Il suo compito è proprio quello di analizzare ogni singolo pacchetto che entra o esce dalla nostra rete e verificare che non contenga minacce, che il mittente ed il destinatario siano chi dicono di essere, che il traffico di rete non nasconda comportamenti maliziosi etc.



Nel corso degli anni, grazie anche all'evolversi dell'hardware, il **firewall perimetrale** è diventato un vero e proprio provider di sicurezza aggiunto. Grazie al software e alle licenze che può gestire, funziona anche da motore antivirus, antispam, anti-intrusione, terminatore di VPN per garantire connessioni protette, sistema di web-filtering per bloccare determinate categorie di siti internet, gestione

e discriminazione degli accessi ai social network, gestione e protezione della rete wifi e molto altro ancora.

Il tutto basandosi sul principio che, essendo l'unico punto di accesso e di transito di pacchetti, da e verso la rete, è il solo apparato ad avere la totale visibilità della situazione.

Parliamo adesso delle minacce che provengono dall'interno della nostra rete.

Il firewall perimetrale, pur essendo uno strumento indispensabile a garantire la sicurezza contro gli attacchi informatici, si limita a proteggere, come si deduce dal suo nome, il perimetro esterno della nostra rete locale LAN.

Le statistiche rilevano che la maggior parte delle minacce, concretizzate poi in un danno informatico, derivano da attacchi partiti dall'interno della rete.

Dipendenti scontenti o tecnicamente superficiali e/o impreparati, periferiche usb infette, sistemi operativi non aggiornati o non aggiornabili, accesso alle informazioni con apparati di proprietà dell'utente come smartphone o tablet **(BYOD)**, sono solo alcune delle situazioni che si possono incontrare in ogni azienda.

Oltre alla formazione degli operatori, diventa quindi indispensabile adottare un valido **sistema antivirus**, il quale deve essere leggero, facilmente gestibile, possibilmente dotato di una console centralizzata e con pochi falsi positivi. Sottolineo il fatto dei falsi positivi perchè, la presenza degli stessi, può spingere l'utente a disabilitare il prodotto considerandolo un ostacolo anzichè un aiuto.

Per quanto riguarda la gestione delle periferiche BYOD, nelle realtà più importanti esistono delle soluzioni che permettono di censire ed autorizzare solo quelle consentite dalle policy aziendali.

Onestamente non mi sento di consigliare l'installazione dei **personal firewall**, spesso inclusi nei sistemi operativi (es: windows firewall) o nelle suite antivirus, in quanto abbastanza noiosi da configurare e spesso causa di problemi. Consiglio di disabilitarli, tranne nei casi in cui si voglia, per esempio, consentire l'accesso ad una risorsa condivisa mettendo dei filtri a livello di indirizzi IP.

Quindi adesso siamo al sicuro ?

hem, premesso che nessuno è mai al sicuro, come dice la celebre frase:

L'unico computer sicuro è un computer spento.

Nessuna strategia di sicurezza informatica può prescindere da una valida **soluzione di backup.** Il backup è la nostra ultima spiaggia e **l'unica vera garanzia che i nostri dati siano sempre disponibili e recuperabili** in caso di problemi di natura sia fisica che logica, come guasti hardware, cancellazioni involontarie o maliziose, intrusioni, infezioni da virus etc etc.

Ovviamente il backup deve essere eseguito e pianificato in modo corretto, rigorosamente conservato al sicuro e su una condivisione protetta da password e, naturalmente, non nello stesso locale del server. Ricordatevi anche che la locazione fisica può essere importante; nel caso vi sia un incendio o qualcosa di simile nella stanza del server non vorremmo mai che compromettesse anche il nostro prezioso backup. Inoltre, in caso di furto, cosa succederebbe se, oltre al server, i ladri portassero via anche il NAS con il backup ?

Queste sono solo alcune e brevi considerazioni. Non dimenticatevi inoltre che, la messa in sicurezza della vostra rete locale e della vostra base dati, è uno dei requisiti fondamentalo per essere a norma con il nuovo Regolamento Europeo per la protezione dei dati personali 2016/679 (GDPR).