STUDIO ROSSI & PARTNERS
Commercialisti & Consulenti del Lavoro
Via F. Ferrucci 6 - 20145 Milano
tel. 02.55187013 - fax. 02.5469729
www.studiorossipartners.it email: info@rossistudio.it

Cyber Security

6 mosse per proteggere la propria Rete Informatica Aziendale

Come mettere in sicurezza la rete aziendale: suggerimenti ed azioni.

STUDIO ROSSI
& PARTNERS
Commercialisti & Consulenti del Lavoro
Via F. Ferrucci 6 - 20145 Milano
tel. 02.55187013 - fax. 02.5469729
www.studiorossipartners.it email: info@rossistudio.it

Che cosa si intende per Cyber Security

La rapida evoluzione delle tecnologie digitali ha avuto un profondo impatto sulla nostra società e sulla vita sia personale che lavorativa degli individui. La privacy non esiste più in termini assoluti.
L'utilizzo dei dispositivi digitali è totalizzante, le persone che usano quei device danno le proprie informazioni alla Rete.

Le Reti Wireless, e non, permettono l'accesso a una mole immensa di informazioni sempre e subito, ma rendono i nostri dispositivi, e noi con loro, molto vulnerabili.

Pensiamo a tutte le informazioni private che conserviamo sui nostri smartphone o sui computer:

- dati personali
- profili sui social network
- accessi ai servizi di online Banking

quello di cui stiamo parlando è subito estremamente più chiaro.

In altre parole l'accesso a internet ci apre al mondo, ma rende le persone, le aziende e le istituzioni potenzialmente esposte a gravi rischi di truffa e sabotaggio.
Tutto questo provoca un bisogno di sicurezza, dal momento in cui la rete fornisce sia vantaggi che insidie.

Il tema della Cyber Security (sicurezza informatica), oggi, è diventato un protagonista chiave sulla scena delle politiche aziendali. Per Cyber Security si intende un approccio mirato alle misure di protezione da attuare in caso di minacce esterne.

La Cyber Security: è il corpo di tecnologie, processi e pratiche volte a proteggere reti, computer, programmi e dati, da attacchi o accessi non autorizzati.

Dal punto di vista aziendale è fondamentale garantire l'integrità e la segretezza delle proprie informazioni perché non è raro che queste vengano violate dai malintenzionati della rete: i cosiddetti Cracker o Black Hat Hacker.

I Cracker o Black Hat Hacker creano particolari programmi malevoli (malware), con lo scopo di accedere a sistemi informatici privati, per rubarne le informazioni sensibili, talvolta a fronte della richiesta di un riscatto. Da qui nasce, da parte delle aziende, l'interesse alla Cyber Security per rendere la propria rete sicura, attraverso la realizzazione di sistemi adibiti a tale scopo.

STUDIO ROSSI
& PARTNERS
Commercialisti & Consulenti del Lavoro
Via F. Ferrucci 6 - 20145 Milano
tel. 02.55187013 - fax. 02.5469729
www.studiorossipartners.it email: info@rossistudio.it

Cyber Security: Strategia di sicurezza

In un ambiente aziendale, una strategia di sicurezza ben ponderata è essenziale.
Secondo Andrea Zapparoli Manzoni, considerato il maggior esperto italiano di Cyber Security, in Italia il 60% delle aziende è preoccupato dalle tematiche della sicurezza informatica, eppure solo il 30% investe nella gestione del rischio. È decisamente ora di cominciare a vedere la sicurezza di rete come un must della vita 4.0, presente nel quotidiano delle imprese e dei cittadini.

Il crimine informatico oggi può provocare danni economici molto ingenti e decretare, in ultima istanza, anche il fallimento di un'azienda; si tratta quindi di pericoli reali che non possono più essere sottovalutati.

C'è ancora troppo valore non sottoposto a sicurezza nel panorama locale. La protezione dei dati deve essere avviata su più livelli attraverso una strategia verticale di Cyber Resilience, che racchiude al suo interno persone, processi e tecnologie.

Come si fa quindi a mettere in sicurezza la propria rete aziendale da attacchi ?

STUDIO ROSSI
& PARTNERS
Commercialisti & Consulenti del Lavoro
Via F. Ferrucci 6 - 20145 Milano
tel. 02.55187013 - fax. 02.5469729
www.studiorossipartners.it email: info@rossistudio.it

Ecco 6 passi fondamentali

Per spiegare con chiarezza da dove cominciare, possiamo individuare 6 passi fondamentali da compiere per mettere in sicurezza la propria organizzazione:

1. Partire da un'approfondita Analisi dei Rischi può sicuramente aiutare a far chiarezza sullo scenario aziendale: è essenziale individuare le criticità più urgenti dell'infrastruttura, per poi adottare le prime misure volte alla protezione dei dati sensibili.

2. È indispensabile poi avvalersi di un firewall. Il firewall è un hardware o software che protegge la rete da accessi non autorizzati e prevenendo le intrusioni impedisce la sottrazione di informazioni. Esso è come la dogana di un grande continente i cui agenti controllano tutto ciò che entra nella città ed eventualmente bloccano l'ingresso a chi non rispetta determinati parametri.

3. Successivamente si deve individuare un antivirus professionale, che è un software atto a rilevare ed eliminare programmi dannosi garantendo una protezione più profonda della rete. Conseguentemente, allo stesso modo dell'antivirus si può scegliere con attenzione anche un'antispam, che controllerà la nostra posta elettronica impedendo l'ingresso di spam, virus e mail di phishing. Non bisogna dimenticare assolutamente il servizio di posta elettronica! Molti dipendenti ancora non condividono che la posta sia un servizio business molto critico in tema di sicurezza informatica aziendale, invece è proprio quello preso più di mira.

4. Inoltre bisogna dotarsi di un buon sistema di backup e disaster recovery per rispristinare file o addirittura server in caso di problematiche gravi così da evitare perdite di informazioni importanti. Effettuare un backup regolare rappresenta una dimensione fondamentale per la sicurezza IT, se si considera quanto tempo e quali sforzi potrebbero essere necessari per recuperare i dati perduti, appare subito chiaro come gestire una strategia di backup sia una mossa vincente.

5. La quinta strategia da non dimenticare è quella rivolta agli aggiornamenti dei software. Sembra ovvio, ma non lo è affatto perché spesso ce ne dimentichiamo. Aggiornare spesso i software e i sistemi operativi in uso, permette di applicare le patch di sicurezza più recenti che vanno a sopperire difetti di programmazione e bug.

6. Per ultima ma non meno importante, è la formazione interna all'azienda. Statisticamente i problemi di sicurezza IT più comuni e rovinosi sono proprio dovuti a errori umani. Le persone non pratiche di sicurezza o non consapevoli del valore di determinate informazioni possono compiere gravi errori senza saperlo E' perciò essenziale offrire sessioni di formazione al personale così che abbia la piena consapevolezza del contesto.

E' grazie a questo mix di tecnologie e buon senso, che si può controllare costantemente gran parte del contenuto che transita sotto e dentro la nostra rete.

STUDIO ROSSI
& PARTNERS
Commercialisti & Consulenti del Lavoro
Via F. Ferrucci 6 - 20145 Milano
tel. 02.55187013 - fax. 02.5469729
www.studiorossipartners.it email: info@rossistudio.it

Conclusioni

Naturalmente non si potrà mai ottenere un livello totale di sicurezza perché tutto ciò che è possibile proteggere può comunque essere violato, ma le soluzioni individuate costituiscono un ottimo punto di partenza per rendere la vita più difficile ad eventuali intrusi e in caso di intrusione evitano più probabilmente danni irreversibili.

Sviluppare nuove capacità e nuovi strumenti per migliorare la sicurezza di rete del proprio sistema aziendale, rappresenta quindi una sfida di grande importanza per la crescita della propria impresa; adottare un buon sistema di sicurezza informatica significherà potenzialmente la differenza tra poter fare business oppure no!