



AREA CULTURALE

IP Security

Tre mosse per difendersi



Alla luce delle vulnerabilità riscontrate più di frequente nello scorso anno, NETASQ ha definito alcune misure di prevenzione contro minacce e falle informatiche per l'intera azienda, onde garantire una maggiore sicurezza nel nuovo anno.

Tre suggerimenti per incrementare il livello di protezione dell'infrastruttura aziendale minimizzando l'impatto dei 10 attacchi informatici principali, li racconta Jeremy D'Hoinne, Product Marketing Director di NETASQ.

N° 1: Attenzione alle cosiddette "soluzioni trasparenti"

La mera installazione di soluzioni per la sicurezza in una rete aziendale non è la misura risolutiva contro tutte le eventuali vulnerabilità perimetrali. Al contrario, la produttività aziendale deve godere, giustamente, della massima priorità. È fondamentale **conoscere l'architettura e le esigenze dell'azienda**. È altresì necessario **scegliere una soluzione idonea**, apprenderne le modalità di impiego ed investire tutto il tempo necessario per una corretta configurazione, in modo da garantire da un lato la massima protezione e dall'altro ridurre l'incidenza sull'operatività aziendale.

Infatti le **soluzioni trasparenti** realizzate a fronte dell'esigenza di semplificare il lavoro alle aziende, vanno a **discapito della più vasta ma meno visibile parte sommersa dell'iceberg: la sicurezza**. Molti vendor hanno sviluppato da un lato **soluzioni "plug & play"**, che però non bloccano alcunché poiché tutte le funzioni di protezione sono disattivate, e dall'altro alcuni programmi di installazione automatica sono dotati di espedienti per "ottimizzare" la durata del servizio (scansione, filtraggio ecc.), cosa di cui molte aziende non sono consapevoli e quindi ritengono di essere protette pur non essendolo.

N° 2: Chi tace acconsente..

Con "silenzio" NETASQ fa riferimento **tutte le libertà implicitamente garantite ai dipendenti** in assenza di chiare regole proibitive.

Cosa occorre fare? **Generare ed aggiornare una documentazione scritta** su ciò che è consentito o non consentito sulla rete aziendale. Un tale accordo con i dipendenti può fare la differenza poiché, definendo chiaramente i comportamenti accettabili, implica specifiche responsabilità degli utenti qualora insorgano problemi. Inoltre, tale documentazione **informa i dipendenti dei rischi di cui potrebbero non essere a conoscenza oltre ad incoraggiarli ad attenersi alle regole**.

N° 3: Fare attenzione ai finti "affari"

Ogni amministratore ha un budget a cui attenersi – una necessità incontestabile all'interno di ogni azienda. Senza mettere in dubbio questo principio, è sorprendente notare come **soluzioni già selezionate ed ormai ben definite siano state di fatto abbandonate a fronte di un risparmio irrilevante**. Il costo di un incidente informatico per un'azienda è raramente inferiore a 500 €, considerando esclusivamente il tempo necessario per il ripristino dei dati / sistemi.

L'**illusione del risparmio** è spesso il frutto del lavoro di abili vendor o reseller: ad esempio un pacchetto di "assistenza tecnica all inclusive" per un anno ad un prezzo imbattibile che cela però gli improbi costi per il rinnovo di tale abbonamento allo scadere dell'anno, oppure un pacchetto che include mezza giornata di installazione e training, che molto spesso sfocia in frequenti chiamate ad una hotline sempre occupata, pagabile al minuto.

Le raccomandazioni di natura tecnica vengono di rado seguite a fronte di un minimo risparmio a brevissimo termine.