Come proteggere l'azienda attraverso il network: un approccio ragionato alla sicurezza

La sicurezza delle informazioni è diventata un obbligo per tutte le aziende. I dati relativi a carte di credito, account privati, acquisti, fornitori e inventario non devono essere divulgati al di fuori dell'ambito aziendale. Ma quali sono le caratteristiche di un'infrastruttura che soddisfi queste necessità?

Il successo di un sistema di sicurezza dipende da alcuni requisiti fondamentali:

- Protezione dagli attacchi che provengono dall'interno e dall'esterno della rete
- Salvaguardia della privacy per tutte le comunicazioni
- Controllo degli accessi attraverso identificazione puntuale di utenti e sistemi di connessione
- Riduzione dei rischi legali
- Creazione di una cultura aziendale e di procedure operative ottimali
- Mantenimento del livello produttivo anche nei periodi di implementazione di nuove soluzioni e protocolli
- Garanzia di ritorno degli investimenti e adozione, laddove possibile, di hardware e software già in uso

Le tecnologie Cisco sono leader nel settore della protezione dei sistemi informativi aziendali. In una Self-Defending Network Cisco le funzionalità di sicurezza integrate in tutti gli elementi dell'infrastruttura (applicazioni, desktop, laptop, telefoni IP, server, router, switch e access point wireless) operano congiuntamente e in modo intelligente proteggendo tutte le informazioni critiche.

Capire come funziona un sistema di sicurezza è importante

La protezione globale di un'azienda non dipende esclusivamente dall'adozione di un metodo unico e coerente, ma anche dall'implementazione di barriere protettive a più livelli. Nel caso di malfunzionamento di un dispositivo di sicurezza, la protezione viene garantita da altri metodi di salvaguardia.

L'adozione di livelli di protezione multipli, integrati nel network e in grado di supportare tutte le tecnologie in uso in azienda, protegge applicazioni e dispositivi in modo automatico ed istantaneo. Questo concetto è alla base della filosofia Self-Defending Network Cisco. La forza di questa soluzione risiede nella sua estrema flessibilità; la rete protegge l'infrastruttura in tutte le fasi del ciclo di vita di un'azienda: durante le fasi di espansione, nei casi di riduzione del personale, quando si effettuano aggiornamenti hardware o quando si trasferisce la sede.

L'offerta Cisco per la sicurezza comprende:

- **Implementazione dei firewall —** I firewall bloccano il traffico indesiderato e pericoloso operando come filtro tra la rete aziendale e le altre reti. In pratica, controllano il traffico in transito in base alle policy specificate dall'utente (una serie di regole che definiscono quale sia il traffico autorizzato). In questo modo, le applicazioni d'uso quotidiano come le e-mail, l'IM (Instant Messaging) e i browser Web, vengono protette da un uso non appropriato.
- **Creazione di comunicazioni sicure —** Le reti private virtuali o VPN (Virtual Private Network) hanno lo scopo di codificare e criptare le informazioni prima dell'invio, gestire la verifica dell'identità degli utenti e proteggere tutte le informazioni in transito. Le VPN sono fondamentali per permettere il telelavoro e consentire l'accesso sicuro alle risorse aziendali attraverso una connessione Internet domestica o attraverso hotspot Wi-Fi pubblici.

- **Prevenzione delle intrusioni e degli attacchi —** I sistemi di prevenzione delle intrusioni o IPS (Intrusion Prevention System) sottopongono a scansione la rete alla ricerca di comportamenti dannosi o sospetti. Sono anche in grado di adottare misure correttive e, in caso di attacco, di inviare notifiche ai responsabili della rete.
- **Controllo delle minacce Internet —** I sistemi avanzati di difesa proteggono i dati e gli utenti da virus, spyware e spam.
- **Gestione della sicurezza a livello di endpoint —** Un dispositivo NAC (Network Admission Control) protegge la rete verificando l'identità degli utenti ad ogni accesso.
- **Gestione dell'accesso —** I servizi di autenticazione, autorizzazione e concessione degli accessi permettono di verificare l'identità degli utenti, di concedere i livelli di utilizzo appropriato e di salvaguardare il sistema dagli abusi.

Per sfruttare al meglio i vantaggi di questi strumenti, Cisco ha sviluppato una Smart Business Roadmap per le medie e piccole imprese. La roadmap fornisce un percorso strutturato che analizza le soluzioni tecnologiche evidenziandone i vantaggi per l'azienda e fornendo tutte le informazioni necessarie per evitare di rimanere bloccati nei passaggi critici e riuscire a fare crescere il business e la rete in modo ottimale.

Maggiore sicurezza significa anche contenimento dei costi

Il contenimento dei costi è una delle preoccupazioni principali delle aziende di tutto il mondo. L'uso di una soluzione per la sicurezza del network facile da implementare, integrare e gestire, permette di controllare al meglio anche i costi. Sfruttare al meglio l'investimento in infrastrutture e applicazioni Cisco significa anche ridurre le spese e minimizzare le perdite causate da attacchi o perdite di dati. Con un livello di sicurezza adeguato:

- Internet diventa uno strumento conveniente e sicuro per le attività aziendali.
- L'eventualità di perdita di dati causata da attacchi di virus e worm viene mitigata.
- I responsabili dei sistemi informativi aziendali sono in grado di amministrare il network anche da ubicazioni remote, riducendo le trasferte e aumentando la produttività.
- L'azienda necessità di minori investimenti per i dispositivi di sicurezza.
- Si riducono i rischi di dispute legali.
- Vengono soddisfatte le policy aziendali e le normative, come, ad esempio, i requisiti per la gestione dei dati delle carte di credito o sulla privacy.
- La larghezza di banda della rete viene allocata in modo adeguato e commisurato all'effettivo utilizzo, migliorando le prestazioni globali e le capacità di risposta del sistema.

Maggiore efficienza operativa

Una Self-Defending Network Cisco permette di integrare tutte le funzioni di sicurezza nella normale gestione delle attività aziendali che transitano attraverso la rete. Un sistema di sicurezza di questo tipo può individuare e rispondere automaticamente alle minacce impedendo il propagarsi di file pericolosi o lo sviluppo di attività dannose. Tutta la rete di contatti, dalle sedi distaccate, ai fornitori, ai rivenditori e ai partner, può operare all'interno di un sistema globale con transazioni protette. Con un sistema di sicurezza integrata:

- I dipendenti, compresi quelli mobili e i telelavoratori, sono sempre produttivi, ovunque, e accedono in modo sicuro alle risorse e alle applicazioni aziendali.
- Le attività possono essere eseguite con la certezza che la sicurezza delle informazioni non venga compromessa.
- I dati sensibili relativi a clienti e fornitori non vengono divulgati.
- I tempi di inattività causati da attacchi e minacce vengono drasticamente ridotti.
- L'efficienza dei dipendenti cresce, grazie alla maggiore tempestività operativa garantita dalle migliori prestazioni del network e delle applicazioni aziendali.

- Le transazioni commerciali vengono eseguite elettronicamente e tempestivamente e tutte le informazioni finanziarie sono disponibili in tempo reale.
- Tutta la documentazione necessaria per la gestione di fornitori e policy viene prodotta con il minimo sforzo.
- Il livello di efficienza dell'impresa beneficia enormemente dei servizi di gestione on-line ed elettronici di clienti e fornitori.
- Il livello produttivo viene ottimizzato grazie alla miglior gestione dei processi operativi.
- La posta elettronica e la messaggistica istantanea sono protette dagli abusi.

Migliore reattività alle esigenze del cliente

Fondamentalmente, una maggiore reattività alle esigenze dei clienti, significa:

- Semplificare i rapporti tra clienti e il personale ad essi dedicato.
- Mettere a disposizione migliori strumenti di connessione e interazione con i clienti.
- Disporre di un sito Web affidabile, aggiornato e davvero utile nel rapporto con i clienti.
- Permettere alla forza vendita di accedere in modo rapido e protetto alle informazioni relative al cliente.

Per soddisfare tutti questi obiettivi, avere un network sicuro è una condizione irrinunciabile, perché consente a dipendenti e fornitori di utilizzare i servizi voce e dati aziendali in modo sicuro, ovunque si trovino. Il processo di gestione dei clienti diventa più snello ed efficiente e diventa realmente possibile rispondere a e-mail, telefonate e messaggi importanti da qualsiasi luogo e in qualsiasi momento.

Inoltre, disporre di un sito Web professionale e sicuro è estremamente rassicurante e fornisce la sensazione di estrema disponibilità e attenzione verso le esigenze dei clienti. Le tecnologie Cisco dedicate alla sicurezza proteggono il sito Web aziendale in modo ottimale e lo rendono sempre accessibile e consultabile per la gestione dei rapporti commerciali con i clienti. Grazie a un sito Web sicuro:

- I clienti ricevono le informazioni in modo rapido e semplice.
- I clienti hanno sempre la certezza che i dati sensibili siano protetti.
- I clienti percepiscono che l'azienda è dinamica, aggiornata ed estremamente competitiva.
- La disponibilità di accesso completo alle informazioni aziendali permette di soddisfare le necessità dei clienti dall'ufficio, in viaggio e anche dai telelavoratori che operano da casa.
- I clienti possono acquistare prodotti e servizi via Internet con facilità e sicurezza.
- Le pagine Web aziendali sono protette da hacker e abusi.

Un percorso per le PMI

La sicurezza è il servizio integrato maggiormente richiesto dalle aziende di tutto il mondo. La Smart Business Roadmap Cisco illustra come sia possibile fornire soluzioni per la sicurezza dei dati aziendali con funzionalità intelligenti, affidabili e personalizzabili. Le caratteristiche di sicurezza integrata salvaguardano ogni aspetto del network e proteggono le aziende in modo globale.

Per sapere come sfruttare i vantaggi delle soluzioni Cisco dedicate alla sicurezza, visitate: www.cisco.com/it/tupmi

Scopri come implementare la tua rete o una determinata tecnologia attraverso la Cisco Smart Business Roadmap: www.cisco.com/web/IT/solutions/smb/smb_roadmap/index.html

Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706 USA
http://www.cisco.com
Tel.: 001 408 526-4000
Fax: 001 408 526-4100

Sede italiana
Cisco Systems Italy
Via Torri Bianche, 7
20059 Vimercate (MI)
http://www.cisco.com/it
Numero verde: 800 787854
Fax: 039 6295 299

Filiale di Roma
Cisco Systems Italy
Via del Serafico, 200
00142 Roma
Numero verde: 800 787854
Fax: 06 51645001

Le filiali Cisco nel mondo sono oltre 200. Gli indirizzi, i numeri di telefono e di fax sono disponibili sul sito Cisco all'indirizzo: **www.cisco.com/go/offices.**