

PROTEGGI I DATI DELLA TUA RETE AZIENDALE

Firewall

I firewall, letteralmente *muro di fuoco*, sono dispositivi atti a proteggere la rete aziendale da attacchi provenienti da Internet da parte di malintenzionati che vogliono sfruttare illegalmente eventuali debolezze delle protezioni di una rete per trarne un vantaggio o arrecare danni.

Gli scopi e gli effetti delle intrusioni sono molteplici: si va dal blocco momentaneo dei sistemi allo sfruttamento di eventuali risorse, come lo spazio disponibile sui server o l'invio di enormi masse di posta elettronica a terze parti tramite un server non protetto. Esistono spessissimo anche casi di furto o cancellazione di dati, fino all'utilizzo dei computer come sistema "ponte" per colpire terze parti e poi cancellare le proprie tracce.

Non sono inoltre da dimenticare tutti quei danni che un sistema privo dei firewall può subire a causa di certe forme di virus (i cosiddetti worm) che attaccano direttamente delle debolezze conosciute di particolari sistemi operativi. Un firewall accuratamente predisposto, è la base per una corretta gestione della sicurezza e per la prevenzione di danni provenienti dall'esterno.

Inoltre un firewall può essere configurato in modo da negare l'accesso a determinati servizi Internet (quali sistemi di messaggistica, reti per scambio di file tipo napster, kazaa, ecc.), per abilitare solo determinati computer alla navigazione Internet ed infine per impedire a programmi indesiderati installati sui PC di diffondere informazioni riservate all'esterno.

Proxy server per la navigazione internet

I proxy server sono dei servizi installati su un computer presente in azienda al fine di offrire dei vantaggi per la navigazione internet.

I vantaggi offerti dal proxy server di Linux sono molteplici: si va dalla semplice accelerazione delle pagine web (le componenti delle pagine già visitate vengono proposte immediatamente, in modo da evitare un loro ulteriore scaricamento, offrendo così un notevole risparmio in termini di tempo), alla possibilità di verificare e controllare, con statistiche estremamente approfondite, la navigazione degli utenti in ambito aziendale.



Un proxy server offre inoltre la possibilità di richiedere una password di accesso per abilitare la navigazione esterna al fine di identificare l'utente in maniera univoca. E' anche possibile proibire l'accesso a determinate tipologie di file o siti pericolosi o controproducenti per l'immagine aziendale e per i personal computer stessi. Il proxy server di Linux supporta inoltre diversi metodi per la rimozione di virus e contenuti pericolosi che possono risiedere all'interno delle pagine internet. I contenuti non desiderati quali lo spamming ed i file multimediali di grandi dimensioni possono abbassare la produttività dei dipendenti e degradare le prestazioni di sistema. I contenuti sconvenienti - quali i messaggi volgari e offensivi - possono comportare responsabilità civili e causare gravi danni alla reputazione di un'azienda. La perdita di informazioni riservate e della proprietà intellettuale possono generare danni.

Rilevazione intrusioni - IDS

E' un sistema di rilevazione delle intrusioni, sia interne che esterne, capace di individuare violazioni delle politiche di sicurezza ed attuare dei sistemi di controllo e alerting. Riesce a rilevare attacchi ed avvertire gli amministratori dello stato in cui si trova il sistema attaccato. E' la *telecamera* della rete e dei sistemi che contengono informazioni critiche.

Individua automaticamente, nel minor tempo possibile e con minor margine di errore, un tentativo di intrusione sia alla propria rete che ai propri sistemi. E' capace di mettere in atto sistemi di difesa contro l'attacco avvenuto.

Mantiene la tracciabilità di un attacco in modo da averne evidenza, anche giuridica, della dinamica dell'intrusione. ■

