La sicurezza in **azienda**

Cifratura, protocolli sicuri, firewall e VPN sono inutili se non ci si assicura che le policy di sicurezza vengano rispettate da tutti gli utenti

MASSIMO GIUSSANI

Al giorno d'oggi ogni azienda è dotata di almeno un sistema informatico che contiene dati sensibili: analisi finanziarie, piani di sviluppo, dati di produzione, strategie future o segreti industriali. Proteggere queste informazioni dall'accesso non autorizzato affinché non possano essere divulgate alla concorrenza o alterate in maniera da danneggiare l'azienda è uno dei compiti fondamentali degli amministratori di sistema: un compito sempre più arduo.

QUALE SICUREZZA

Nella lingua italiana, il termine 'sicurezza' traduce due diversi vocaboli inglesi: safety e security. Il concetto di safety viene solitamente riferito alla protezione da guasti, danni, errori, incidenti che possono mettere in pericolo l'incolumità di macchine o persone; quello di security, invece, è maggiormente improntato alla gestione degli accessi e alla protezione delle informazioni. Nel contesto delle sole reti telematiche, il termine security copre una vasta gamma di discipline volte a tutelare la riservatezza, l'integrità e l'accessibilità dei dati: si va dalla creazione e messa in pratica di una politica della sicurezza, al controllo degli accessi con sistemi di identificazione biometrica, per arrivare alla scelta e alla configurazione degli elementi dell'infrastruttura di rete e degli elaboratori a essa connessi. È una partita che viene giocata a tutti i livelli: hardware, software e formazione del personale. Il primo passo per la messa in sicurezza di una rete telematica consiste in un'attenta valutazione dei rischi, attività che permette l'identificazione delle aree vulnerabili e delle possibili soluzioni; successivamente viene redatta una policy di sicurezza che descrive le contromisure indispensabili a garantire un livello minimo di sicurezza per la rete e i comportamenti da tenere per non compromettere gli sforzi fatti. Verifica, manutenzione e aggiornamento sono ulteriori essenziali passi importanti per preservare l'efficienza delle difese telematiche. La fase più importante è tuttavia quella che normalmente si tende a dare per scontata: far rispettare in maniera rigorosa e a tutti i dipendenti la policy di sicurezza intrapresa.

Fonte: D-Link

AMICI E NEMICI

La maggior parte delle contromisure atte a garantire la sicurezza delle comunicazioni si basa in ultima analisi su tecniche crittografiche. L'autenticazione degli interlocutori ha solitamente luogo con lo scambio di informazioni parzialmente cifrate che permettano solo ai diretti interessati di ricostruire una chiave segreta comune; la riservatezza delle comunicazioni si ottiene cifrando i contenuti con una chiave precedentemente scambiata; l'integrità dei dati può essere verificata con firme digitali o message digest la cui verifica si rifà a principi di crittografia. La sicurezza può essere implementata nei diversi strati dello stack di comunicazione, dallo strato fisico fino a quello applicativo. La scelta è un compresso tra comodità e prestazioni. L'implementazione nello strato di rete, ad esempio con il ricorso al protocollo sicuro IP Sec, ha il vantaggio di risultare trasparente agli utenti e di non richiedere modifiche alle applicazioni: risulta in questo modo implementata a prescindere dalla volontà dell'utente. L'aggiunta di controlli e cifratura a livello applicativo estende la sicurezza da un estremo all'altro della rete di comunicazione, ma richiede maggior attenzione da parte di tutti gli utilizzatori.

Anche le informazioni scambiate sulla rete (cifrate o meno) possono essere filtrate a più livelli, utilizzando dei router per eliminare i pacchetti in base agli indirizzi IP e dei gateway applicativi per selezionarli sulla base ai contenuti.

L'elemento più debole di tutta la catena, come ben sanno gli amministratori di rete, è tuttavia quello che si colloca tra la sedia e la tastiera: l'utente. L'utente medio, infatti, si connette spesso in rete per motivi non inerenti all'attività lavorativa e tende a scordare i più elementari principi di sicurezza (scelta, conservazione e modifica periodica di password sicure; installazione di programmi di origine dubbia; disabilitazione di firewall e antivirus; navigazione su siti 'a rischio'). Il 37% dei lavoratori ammette di navigare in Internet costantemente durante la giornata lavorativa (fonte: Vault.com) e il 30 - 40% dell'utilizzo di Internet non è correlato all'attività lavorativa (fonte: IDC Research, ricerche scorrelate). Ai pericoli della navigazione si aggiungono quelli dei programmi di condivisione peer-to-peer e di messaggistica istantanea.

Fonte: Phoenix Contact

Fonte: LSI

GATEWAY, FIREWALL E ROUTER

Firewall hardware, firewall software e antivirus vengono messi a dura prova dal crescente utilizzo dei siti di social networking: le reti odierne devono essere dotate di una politica di sicurezza espressamente orientata ad affrontare le minacce del cosiddetto Web 2.0. Con i firewall della famiglia NetDefend, D-Link mette a disposizioni degli strumenti in grado di scoprire e prevenire attacchi e intrusioni, segmentare la rete e prevenire l'accesso a siti Web con contenuti non produttivi o impropri. Questi dispositivi consentono di bloccare le applicazioni peer-to-peer e di messaggistica istantanea ed effettuano la ricerca di virus nei messaggi di posta in entrata e in uscita, allegati inclusi. Le funzionalità di NetDefend includono l'autenticazione degli utenti, il supporto per le reti private virtuali (VPN), la configurazione delle regole di accesso, il filtraggio dei contenuti e la protezione nei confronti degli attacchi DoS (Denial of Service). L'integrazione con gli switch xStack permette di individuare e bloccare le attività illecite all'interno della rete e di mettere automaticamente in quarantena i computer contagiati da virus, evitando la propagazione di codice malevolo.

Per la protezione delle reti industriali, Phoenix Contact offre i router della serie MGuard. Il nuovo router FL Mguard Rs-b si installa su guida Din ed è caratterizzato da un'elevata portata di dati, fino a 2x85 Mbps. Le funzioni di sicurezza integrate mettono le reti industriali al riparo da accessi non autorizzati e utilizzi non corretti che potrebbero causare guasti agli impianti. Il modulo, configurabile tramite Snmp o interfaccia Web integrata, gestisce tutte le comuni funzionalità di routing: Standard-Routing, NAT (Network Address Translation) sotto forma

Fonte: WatchGuard

di Masquerading e Port-Forwarding, 1:1-NAT. L'analisi dei contenuti dei pacchetti è alla base delle soluzioni per la sicurezza Deep Packet Inspection (DPI) messe a punto da LSI con le architetture multicore Tarari T10. Grazie alla tecnologia DPI le soluzioni di LSI permettono di farsi carico non solo di azioni fondamentali per la sicurezza di rete come le scansioni antivirus/antispam e la prevenzione delle intrusioni, ma anche di altre applicazioni chiave della rete quali la fatturazione e il filtraggio sulla base dei contenuti, la gestione dell'ampiezza di banda e la qualità del servizio (QoS).
Le soluzioni su silicio LSI T2000 e T1000 offrono prestazioni fino a 10 Gbps su singolo chip, adatte all'elaborazione dei contenuti in applicazioni di rete ad alta velocità. Per semplificare l'integrazione delle soluzioni Tarari di elaborazione e protezione dei contenuti in reti con elementi preesistenti che implementano le succitate applicazioni di rete, LSI ha recentemente introdotto quattro nuove famiglie di schede (Serie 7900, 8600, 8800, 8900), basate sui fattori di forma standard PCIe, mini-PCIe, mini-PCI e Advanced Mezzanine Card.

RETI PRIVATE VIRTUALI

Un collegamento sicuro tra diverse sedi di una stessa azienda o tra il sistema informatico aziendale e dipendenti che si connettono da postazioni remote (ad esempio da un cliente o dalla propria abitazione) può essere realizzato a basso costo ricorrendo alle reti private virtuali (VPN, Virtual Private Network). WatchGuard ha messo a punto un prodotto per reti virtuali su SSL (Secure Socket Layer) che abbina l'elevata sicurezza delle connessioni a caratteristiche di semplicità d'uso e di flessibilità. Pensato per aziende con meno di 500 dipendenti, WatchGuard SSL 100 dispone di strumenti di disamina approfondita del dispositivo e di controllo dell'integrità dell'end point che permettono alle aziende di assicurare l'accesso alla rete esclusivamente ai dispositivi sicuri e conformi alla policy di sicurezza (ad esempio con firewall e antivirus aggiornati). SSL 100 offre funzionalità avanzate di logging e reporting con una ricca serie di informazioni sugli utenti remoti. Per le aziende che vogliono fornire applicazioni o strumenti per il lavoro a distanza, il prodotto di WatchGuard contempla anche applicazioni server e desktop non native come SSH (Secure SHell) e RDP (Remote Desktop). Particolarmente interessante, dal punto di vista della sicurezza è l'autenticazione a due fattori on-board: una doppia autenticazione veloce e sicura, che non richiede sistemi di terze parti, è possibile grazie alla generazione di un token tramite SMS e OTP (One-Time Password) da scambiare con un dispositivo portatile dell'utente (cellulare aziendale, smartphone o palmare).

readerservice.it
D-Link n. 07
Phoenix Contact n. 08
LSI n. 09
WatchGuard n. 10