



## AREA CULTURALE IP SECURITY

## Sorveglianza il business!

### La sicurezza IT in un mondo perfetto

Quale azienda può reimpostare settimanalmente le proprie misure di sicurezza?

La complessità della rete aziendale tradizionale vive un costante incremento: la continuità del servizio e lo scambio ininterrotto d'informazioni attraverso qualsivoglia strumento di comunicazione sono fondamentali per il successo aziendale. La nuova rete "estesa" deve essere in grado trasmettere "EoIP" (everything over IP) e di supportare diversi "incubi" quali i nuovi dispositivi mobili come l'iPhone. Purtroppo però – al contrario delle criticità informatiche – la protezione di dati ed informazioni sottostà all'allocatione del budget per l'IT, che non aumenta, costringendo il manager IT a selezionare una specifica strategia tra:

- cercare il compromesso tra funzionalità e prezzo, strategia spesso foriera di scelte basate sul "best deal"
- optare per soluzioni dedicate "best-of-breed", strategia che però richiede investimenti significativi ed un livello di know-how superiore rispetto a quanto eventualmente disponibile.

Diversi studi indicano inoltre che, a fronte di un investimento in sicurezza informatica, per il 40% dei manager IT la tutela della propria posizione ha la massima priorità, un atteggiamento con conseguenze quali i "lunedì neri", in cui gli utenti mobili / remoti si connettono alla rete, infettandola con i "regalini" dell'accesso ad internet del week-end. Lo staff IT avrà bisogno dell'intera settimana per identificare l'origine dell'infezione, scansare e ripristinare i sistemi alterati, reimpostare le policy di sicurezza, risolvendo la situazione solo di venerdì, appena prima che il ciclo ricominci nuovamente. Le aziende possono permettersi di ricostruire la propria infrastruttura di sicurezza ogni settimana? È ormai impensabile sentirsi protetti senza impiegare soluzioni per il filtraggio dei contenuti e la prevenzione contro le intrusioni (IPS), la corretta gestione delle policy di sicurezza a

livello di utenti, la protezione antivirus ed antispyware, la strong authentication per desktop, la cifratura del traffico (VPN SSL o IPsec), il filtraggio web, la gestione delle vulnerabilità applicative con i relativi patch... Un elenco davvero lungo! Se da un lato tutte queste soluzioni si rivelano sempre più necessarie, quanto costa impiegarle, integrarle ed aggiornarle?

Per rendere veramente sicura l'infrastruttura informatica non basta una mera combinazione di diverse tecnologie, è bensì necessario impiegarne di intelligenti, usandole nel modo corretto! In un mondo perfetto, il manager IT dispone di strumenti adeguati ad appianare l'apparente paradosso tra livello di protezione e le prestazioni della rete, e, allo stesso tempo, di soluzioni di sicurezza automatizzate, che forniscano una vera protezione day-0 in tempo reale. In un mondo perfetto il manager IT impiega una singola soluzione che copre tutti gli aspetti legati alla protezione, definire un'unica policy ed essere sicuro che questa sia applicata correttamente ed in modo automatico a tutti i nodi della rete, dalla connessione internet alla singola workstation, PDA, laptop ecc.

Inoltre i sistemi di protezione, oltre a bloccare proattivamente minacce note e non note, sia interne sia esterne, si adattano automaticamente alla realtà dell'infrastruttura esistente ed al reale rischio corso dall'azienda. I sistemi infetti e le componenti IT che si discostano dalle policy di sicurezza impostate devono essere aggiornati automaticamente, messi in quarantena e rilasciati solo dopo l'applicazione dei patch corrispondenti ed un'accurata scansione.

