



### Onion: sicurezza in outsourcing

Le tematiche di sicurezza sono diventate la chiave del "corporate Internetworking", che è a sua volta la chiave dei processi comunicativi aziendali. E, come avviene per ogni processo chiave, il buonsenso impone che vengano affidati a personale fortemente skillato. Ma il processo di formazione di un valido Security Manager richiede tempo e risorse difficilmente reperibili in azienda. In una corretta visione, la Network Security è paragonabile ad un'operazione chirurgica: non è consentito improvvisare. In altre parole, non basta acquistare ed installare un firewall "di grido" per rendere sicura una rete, ma è necessario che venga configurato, monitorato, aggiornato e costantemente gestito per garantire un ragionevole margine di sicurezza. Ogni cambiamento può riflettersi in modifiche e aggiornamenti nelle policy di sicurezza, quando non addirittura nell'infrastruttura.

Se escludiamo le poche realtà in grado di sostenerne il costo, è facilmente comprensibile come un'alternativa economicamente vantaggiosa sia una "Security Task Force" esterna, a cui affidare la gestione e l'evoluzione della sicurezza. **Onion** ([www.onion.it](http://www.onion.it)), in partnership con NetFORCE, si rivolge al mercato con soluzioni di IT Security, per una gestione efficiente della sicurezza.

56% e 50%, focalizzati sui settori Utilities, IT/Telco e Finanziario» afferma **Manlio Tarantini**, Technical Consulting Manager MDG di SchlumbergerSema NIS.

Per quanto riguarda i sistemi di autenticazione, lo studio Schlumberger rileva che, sebbene il 74% delle imprese europee utilizzi tecniche di autenticazione, allo stato attuale gli investimenti in smart card, token, soluzioni biometriche e certificati digitali sono molto limitati.

«La tecnologia smart card si avvia a divenire un elemento intrinseco dell'ICT (IT e network). Attualmente si individuano alcuni mercati emergenti e, primo tra questi, quello legato a Wi-Fi (802.11b). Gli investimenti R&D saranno cospicui, mentre la standardizzazione costituirà ancora la sfida da vincere» conclude Tarantini.



**Manlio Tarantini**, Technical Consulting Manager MDG di SchlumbergerSema NIS

## 8. DISPOSITIVI DI AUTORIZZAZIONE

Il concetto di autorizzazione fa progredire la pratica dell'autenticazione (vedi punto 7), assegnando ruoli definiti agli utilizzatori di risorse quali server, applicativi, dati e file, e stabilendone condizioni di utilizzo. Si tratta di prodotti spesso impiegati negli ambienti Web server, per il controllo dell'utilizzo di applicazioni presso dipendenti, partner, fornitori e clienti. Alcuni produttori integrano alle soluzioni di autorizzazione funzionalità di single sign-on (SSO), che consentono agli utenti accessi ai diversi applicativi attraverso l'utilizzo di una singola password.

Alla domanda di strong authentication per le applicazioni Web in costante crescita, si affianca la richiesta sempre più pressante da parte dei clienti di integrazione con un altrettanto vasto campo di applicazioni (molte delle quali non sono nemmeno Web application), rappresentato dalle versioni aggiornate delle "vecchie" legacy application. La corsa dei produttori di Web single-sign-on (SSO) ad integrare legacy ties e funzionalità tipiche del Web agli applicativi è un elemento indicativo delle tendenze che si stanno sviluppando, così come il tentativo da parte di molti vendor Web SSO di riposizionarsi nel mercato della gestione della security, contestualmente ad un ampliamento della propria offerta che comprende sempre più frequentemente console per la gestione dei diritti di accesso.

## 9. IDS

Gli IDS sono dispositivi che esaminano il traffico sulla rete alla ricerca di potenziali attacchi a risorse protette dell'azienda. Disponibili sia in versione software che hardware (vedi punto 14), le tipologie di IDS sono principalmente di due tipi. Alla prima appartengono gli IDS di rete (Network IDS o NIDS), che sviluppano le funzionalità sopra descritte rispondendo agli attacchi con l'invio di alert alla console dell'amministratore della sicurezza. Della seconda fanno invece parte gli host IDS (HIDS), dispositivi che analizzano dati provenienti dai singoli computer della rete, principalmente log degli eventi registrati da sistemi operativi e applicativi, alla ricerca di attività anomale o non autorizzate.

L'evoluzione che sta investendo gli IDS porterà molto probabilmente ad una loro sostanziale modifica, in direzione della realizzazione di sistemi capaci di analizzare, filtrare e classificare gli eventi che minacciano la sicurezza della rete. Attualmente la maggior parte degli IDS utilizza tecniche di analisi degli attacchi cosiddette "Knowledge based" che, in un futuro abbastanza prossimo, si renderà necessario integrare con tecniche di tipo "Behaviour based", per aumentarne efficacia e affidabilità. «E' prevista una sempre maggior integrazione con le soluzioni di firewalling e, anche per gli IDS, lo sviluppo di strumenti di gestione integrata (Firewall IDS) per governare l'attuale complessità delle reti enterprise» ci dice Vecchione di HP.

Un altro importante sviluppo, che si profila in questo settore, è quello di rendere disponibile il presidio e la difesa anche degli end-point connessi alla rete, estendendo le analisi indifferentemente a server e client collegati alla rete aziendale. «La tecnologia Cisco Threat Response rende già oggi disponibile l'analisi automatizzata e in tempo reale di ogni host a rischio, determinando le probabilità che esso sia vittima di un attacco. Infatti, solo con l'analisi dell'host sotto attacco si possono classificare efficacemente le intrusioni effettive e stabilirne i livelli di criticità» afferma Mircoli di Cisco.

## 10. SOFTWARE CHE STIMANO IL GRADO DI VULNERABILITÀ (Vulnerability Assessment)

Si tratta di software che scansionano reti, server e applicativi di un'azienda alla ricerca di bug, vulnerabilità, falle e altre debolezze che potrebbero essere sfruttate per guadagnare un accesso non auto-