FRANCESCA PRANDI

Sicurezza delle reti: prospettive rosee, tanti problemi

Internet è difficile da controllare e gli utenti non possono essere lasciati soli

La vulnerabilità delle reti e dei sistemi è in continua crescita. Il minaccioso esercito dei virus informatici s'ingrossa in maniera esponenziale, gli hacker danno dimostrazione della loro abilità colpendo anche enti di servizio pubblico, con effetti che gravano sull'intera collettività: si pensi all'eclatante paralisi delle Poste Italiane dello scorso gennaio. Aumentano gli episodi di boicottaggio del servizio: le nuove forme di protesta attuate intasando le linee con l'invio simultaneo di un'infinità di messaggi elettronici. Insomma la fantasia dei malintenzionati pare essere molto stimolata dalla rete e la sicurezza di chi vi opera è quindi molto a rischio.

Va da sé che le prospettive per il mercato della sicurezza sono davvero rosee.
Secondo valutazioni di IDC se ne avvantaggeranno soprattutto i fornitori di servizi per i quali la spesa a livello mondiale esploderà dai 9.727 milioni di dollari nel 2002 ai 23.215 nel 2006. Ma crescerà anche il software che, nello stesso periodo, raddoppierà il fatturato arrivando a 12.411 milioni di dollari investiti in security software. L'impatto sull'hardware sarà minore, ma comunque il trend sarà crescente e consentirà di arrivare nel 2006 a 8.900 milioni di dollari di fatturato dei dispositivi per la sicurezza contro i 3.600 nel 2002.

UNA RICERCA IDC SUL COMPORTAMENTO DELLE AZIENDE ITALIANE

Garantire sicurezza alle reti aziendali è diventata una faccenda assai complessa. Non basta più occuparsi dell'inviolabilità degli accessi esterni, ad esempio usando scanning delle email, antivirus e firewall; chi opera in un'ottica di azienda estesa oggi deve superare il confine degli accessi per raggiungere i territori dei lavoratori mobili, degli uffici e delle sedi distaccate, dei clienti, dei fornitori, della rete di vendita e assistenza e in generale di tutti i partner del business. E alla sicurezza informatica si può anche abbinare quella fisica. Ad esempio è possibile seguire il movimento delle merci a cui sia stato applicato un chip oppure riconoscere l'identità degli individui controllati da un circuito di telecamere.
In definitiva: il bisogno c'è e le soluzioni sono numerose; ma proprio per questo le scelte di investimento si sono fatte piuttosto complesse.
Questo in estrema sintesi è il risultato di una ricerca condotta da IDC nel nostro Paese su 609 responsabili IT di aziende grandi e medio piccole al fine di analizzare la percezione aziendale del rischio, le policy e le soluzioni adottate finora e i futuri piani d'azione. La ricerca si è svolta nel corso dei mesi di febbraio e marzo 2003 e i risultati sono stati presentati a Milano, il 26 marzo, durante l'annuale IT Security Conference di IDC.
I principali rischi percepiti riguardano i virus informatici, che sono motivo di massima preoccupazione per il 73% del campione La minaccia di hacker esterni è avvertita dal 49% degli intervistati e a seguire vengono indicati l'accesso non autorizzato a database e applicazioni aziendali (43%) e gli errori e manomissioni involontari da parte dei dipendenti (38%). Pochi intervistati sembrano invece preoccuparsi dei sabotaggi interni che, secondo i consulenti della sicurezza, sono più della metà di quelli effettivamente realizzati.
Se questi sono i rischi percepiti, la domanda di sicurezza si focalizza quindi su antivirus e firewall, adottati da circa il 90% del campione, mentre soluzioni più evolute come sistemi di identificazione, di filtering dell'URL o software 3A sono utilizzati da un numero limitato di aziende medio-grandi. IDC ha rilevato anche una crescita di interesse per la firma e i certificati digitali che probabilmente vengono valutati anche in quanto strumenti evoluti di accesso a informazioni aziendali, o come storage dei dati. Ezio Viola, di IDC, illustrando questi risultati ha commentato che "gli italiani appaiono ancora legati a una visione della sicurezza focalizzata sui pericoli più evidenti, più che su un'analisi completa e aggiornata dei rischi cui va incontro l'azienda. Nella maggior parte dei casi questa visione si traduce nell'acquisto di singoli prodotti, più che in un approccio sistematico e pianificato, e la sicurezza è percepita nel suo aspetto più immediato ovvero come difesa e non anche come strumento di efficienza". E in effetti solo il 34% delle aziende sostiene di avere già una politica per la sicurezza con regole di comportamento che tengono conto degli intrecci tra IT, sicurezza, organizzazione e business. Il 29% è comunque interessato a svilupparla mentre nel restante 36% dei casi questo approccio non è previsto. In parziale incoerenza con questi dati, metà del campione riconosce alla sicurezza anche una valenza competitiva per il business aziendale, tant'è vero che il 90% tiene un back up all'interno della propria sede e iniziano anche a diffondersi forme di disaster recovery e business continuity che garantiscono non solo la sal-

Fonte Play Media

vezza dei dati, ma anche la continuità dell'operatività del business.
Le decisioni di investimento in questo campo sono rese difficili dal fatto che prevalgono le implicazioni tattiche rispetto a quelle strategiche. E infatti più della metà del campione non calcola il ROI (l'indice che valuta il rendimento degli investimenti), anche perché non è semplice. Come si può determinare il rischio reale a cui si va incontro? –ha osservato Martin Canning di IDC. Il percorso logico da seguire parte dall'individuazione e dalla distinzione fra le possibili minacce, per continuare con una valutazione dell'impatto prevedibile sulle attività aziendali e quindi del rischio connesso a ogni minaccia; e questo è decisamente l'aspetto più problematico. Il furto di dati, ad esempio, è una minaccia. L'impatto che può avere sul business può essere da minimo a disastroso, a seconda del tipo di attività svolta. Valutare una probabilità di rischio per questa minaccia è ancora un'altra cosa. E infine si tratta di capire a quale perdita economica si va incontro nel caso che la minaccia si concretizzi e tutto questo serve per giungere a una qualche valutazione del ROI degli investimenti in sicurezza informatica.
Per concludere, la ricerca fornisce anche alcune indicazioni sulle decisioni di acquisto in un mercato che, secondo gli analisti, si presenta estremamente confuso: ci sono molti prodotti e servizi ed è difficile scegliere la soluzione giusta.
Anzitutto in Italia si spende ancora poco, infatti nel 48% delle aziende intervistate la spesa in sicurezza è pari a meno del 5% della spesa IT. Nella scelta del fornitore si privilegia ancora il rapporto qualità/prezzo, ma un terzo del campione attribuisce un'importanza crescente anche alla capacità di consulenza specifica che viene offerta. Una posizione di leadership viene riconosciuta solo fra i fornitori di antivirus (Norton/Symantec), mentre per i firewall, i servizi di consulenza e quelli di Managed Security le aziende non sanno cosa dire. E del resto il mercato appare molto frammentato. Tra i player ci sono specialisti di sicurezza, vendor, player della connettività e delle infrastrutture e della consulenza aziendale.

Il consiglio di Canning alle aziende è quello di organizzare una politica aziendale per la sicurezza che, indicando i bisogni effettivi e gli strumenti necessari per soddisfarli, tenga anche in dovuto conto gli investimenti già realizzati e esalti in particolare gli aspetti della sensibilizzazione di tutto l'ambiente aziendale e della semplicità d'uso. Infatti, senza il completo coinvolgimento di tutti gli addetti, nessuna politica aziendale per la sicurezza potrebbe avere successo. Così come scelte troppo complesse, addirittura eccessive rispetto ai bisogni, potrebbero poi essere applicate male. Gli analisti per finire hanno lanciato un avvertimento ai potenziali utenti: i fornitori si stanno concentrando sui livelli più alti della domanda e in previsione avranno un orientamento ancora più marcato verso i grandi business. Ciò potrebbe tradursi in un'insufficiente esperienza con le problematiche delle imprese medio piccole, che forse farebbero bene quindi ad anticipare i loro investimenti.

SICUREZZA INFORMATICA: CRESCE CON L'IMPEGNO ANCHE DELLE ISTITUZIONI PUBBLICHE

Si è detto fin dalla sua nascita che Internet è difficilmente controllabile. Con la crescita esponenziale dei virus e degli attacchi informatici degli ultimi anni è parso altrettanto chiaro che gli utenti non possono essere lasciati soli. È indispensabile l'intervento di enti centrali che si occupino della sicurezza delle reti e che siano il più possibile coordinati a livello sovranazionale.
Di questi aspetti ha parlato alla IT Security Conference di IDC, l'Avvocato Carlo Sarzana di S. Ippolito, Membro del Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni e Presidente Aggiunto Onorario della Corte di Cassazione. La sua ricca relazione ha offerto

amica sulle proble-
istenti, tantissime, e
ha dato un'idea del
vello internazionale,
bile viste le difficol-
ntrano tutte le isti-
ovranazionali, e a
ionale, nonostante
portante condotta
e dal Ministero
azione. Ecco solo
mpi. La Commis-
opea ha elaborato
sta per una rete del-
e di Information
ne lavorino in stret-
mento con l'indu-
e di coordinamento
e di costituzione, ma
aesi di fatto queste
on esistono neppu-
sono, spesso non
o organizzate.
alle normative na-
plicabili al crimine
o è frequente che
o molto da paese a
ovente non sono neppure adeguate. C'è poi tutta una problematica relativa al bilanciamento fra diritti alla privacy e sicurezza informatica. Secondo Sarzana nei momenti di crisi deve prevalere quest'ultima, ma l'argomento è molto delicato. In Italia il Ministero dell'Innovazione, di concerto con il Ministero delle Telecomunicazioni, ha costituito il Comitato Nazionale per la Sicurezza Informatica, a cui ha affidato il compito di elaborare una strategia unitaria per la sicurezza nelle telecomunicazioni e nell'informatica, regolamentare la certificazione della sicurezza ICT nella pubblica amministrazione, predisporre linee guida per la formazione dei dipendenti pubblici. Nella PA infatti questi temi godono in generale di scarsissima considerazione, fatte salve alcune eccezioni di amministrazioni già dotate di buoni sistemi. ■

Citiraya Italia, per far comprendere come sia possibile smaltire correttamente i rifiuti derivanti da materiale elettronico, ha organizzato lo scorso marzo una visita ai propri stabilimenti di riciclaggio di materiale elettronico a Singapore. Alla visita ha partecipato una delegazione composta dai membri più autorevoli degli organismi italiani e maltesi che si occupano del fine vita elettronico.

Marconi ha aumentato nel 2002 la propria quota di mercato in Europa nel settore delle reti ottiche di ben quattro punti percentuali: il maggiore incremento registrato nel periodo. Marconi risulta quindi essere leader di questo mercato insieme ad Alcatel. Lo ha dichiarato RHK, impegnata in analisi di mercato per il settore tlc.

RS Components ha consolidato la partnership con Saint Gobain Performance Plastics mettendo a disposizione sia on-line sia sul catalogo cartaceo i due prodotti di punta di Saint Gobain: Tubo Norprene di grado industriale, Tubo in Tygon per alimenti, latte e latticini.

La ventennale esperienza di Orvem nella vendita e nel supporto tecnico dei componenti per protezione da sovracorrente, unita alla tecnologia e competenza di un produttore europeo del calibro di Wickmann Werke, sono sfociate il 1° marzo di quest'anno in un accordo di distribuzione per il mercato italiano. La maturazione di differenti scelte strategiche, commerciali e di servizio ai clienti ha portato il 28 febbraio scorso a una cessazione del rapporto di Orvem con Littelfuse.

TT electronics ha deciso di focalizzarsi nella realizzazione di prodotti per applicazioni specifiche e nell'assemblaggio, posizionandosi in modo tale da poter offrire ai clienti un valore superiore rispetto a un tipico fornitore di componenti commodity. Robert Flatcher, divisional chief executive della società, ha affermato che la focalizzazione sulle tecnologie application-specific è parte fondamentale della strategia di crescita della società.