

SICUREZZA I CONSIGLI DELLE IT FACTORY

«I virus? Attenzione agli attacchi interni»

Le compagnie italiane non danno il giusto peso alla protezione dei dati. E trascurano i pericoli che vengono da un cattivo uso dei computer. Lo sostengono i fornitori. Che consigliano...

Fabio Sgroi

Giornale delle assicurazioni, settembre 2004

Sicurezza informatica. Un tema più che mai attuale che riguarda qualsiasi azienda. A maggior ragione le compagnie assicurative, che basano il loro business e la loro attività proprio sulla trasmissione di dati. Come proteggere le informazioni? Ecco i consigli dell'offerta.

Gestire il rischio nella comunicazione interna. Una policy credibile di protezione (dei sistemi deve e rendere sicuri i canali di contatto con gli assicurati. È l'opinione di Roberto Lorini, amministratore delegato di Vp Tech (gruppo Value Partners). «Le società hanno la necessità di rendere sicuro il passaggio di informazioni dalle agenzie alle strutture centrali che raccolgono le informazioni» sottolinea Lorini. «E devono rendere sicure sia la multicanalità, soprattutto nel settore vita e gestione del risparmio, sia le modalità di interazione con i clienti, Le compagnie hanno inoltre l'esigenza di gestire in modo sicuro i documenti generati nelle agenzie, in particolar modo la contrattualistica e l'adozione degli standard normativi emanati dall'Isvap».

Simon Perry, vice president security strategy di Computer Associates, punta invece su un costante monitoraggio delle intrusioni e un continuo aggiornamento delle applicazioni. «I software sono diventati sempre più vulnerabili, e i nuovi worm creati dagli hacker si spargono in tutto il mondo molto velocemente. È stato calcolato che un virus impiega dalle cinque alle otto ore per fare il giro del mondo se viaggia via e-mail: su software, invece, ci mette meno di dieci minuti. Non aprire gli allegati, ormai, non basta più».

Tutela dei dati: un problema sottovalutato. «Quello della sicurezza è un tema sentito dagli americani, molto meno da noi», asserisce **Tino Prato**, country executive Italia di Brocade Communications. «Me ne rendo conto quando si organizzano i seminari con clienti e utenti: ogni volta che si parla di sicurezza si ha l'impressione che al problema non sia dato il giusto peso. Non sembra che ci si appassioni troppo alla questione. Senza dubbio, come già detto, negli Stati Uniti si hanno maggiori preoccupazioni. Lo testimonia il fatto che su questo tema si continua a investire e a implementare continuamente dei software». Prato, che *Assicurazioni* ha incontrato in occasione del Forum It, ritiene che il tema della sicurezza non possa più essere sottovalutato. «Anche le compagnie assicurative hanno capito che la protezione e la tutela dei dati è fondamentale. E che il dato stesso rappresenta il valore su cui si basa il business e l'attività della compagnia. Oggi c'è maggiore consapevolezza che i dati più importanti e significativi vanno assolutamente tutelati e messi con lo storage appropriato di livello più alto e con i sistemi di storage networking migliori». Ma i pericoli maggiori arrivano davvero dall'esterno? «Su questo avrei qualche dubbio. Pensare che qualcuno possa entrare in una rete dati di un istituzione finanziaria e riuscire a tirare fuori le informazioni riservate, francamente è difficile», afferma Prato. «È più verosimile, invece, che qualcuno dall'interno possa fare inavvertitamente qualche operazione che possa mettere a repentaglio la struttura. Faccio

un esempio: prendo un normalissimo switch e mi connetto al Fabric e ho la password per questo switch. Lo stesso switch diventa parte del Fabric e quindi posso andare a cambiare le configurazioni. Basta solo questo, senza modificare i dati...».

Reati informatici: spunta la mafia. Secondo Perry in esiste un altro aspetto. Ancora più preoccupante. «Nell'ultimo anno abbiamo assistito all'entrata in scena della mafia», dice Perry. «Da quando la criminalità organizzata ha iniziato a occuparsi personalmente di reati informatici, il pericolo di attacchi ha registrato un incremento notevole. La mafia si serve di veri e propri hacker per sferrare attacchi di *denial of service* contro la comunità economica e finanziaria. Minaccia la chiusura del sito attraverso un eccesso di traffico, che manda tutto in tilt. Come è possibile? Semplice: gli hacker si impadroniscono, attraverso cavalli di Troia, di computer altrui, senza farsi scoprire dai titolari. Questi computer vengono poi diretti inconsapevolmente verso il sito che si vuole attaccare, causando così l'overflow. Spesso, chi non ha ceduto al ricatto è stato costretto a chiudere il sito per molti giorni, con conseguente perdita di denaro».

Rendere sicuri i canali di comunicazione. VP Tech sta puntando decisamente sulla messa in sicurezza dei diversi canali di comunicazione. «Stiamo focalizzando le nostre attenzioni sulle reti di promotori, sugli shop finanziari e sulle agenzie», dice Lorini. «Inoltre, stiamo lavorando anche alla gestione sicura delle modalità di interazione con gli assicurati e alla gestione documentale». Come vi state muovendo sul fronte del trattamento e del passaggio sicuro dei dati? «La nostra azienda, che nel settore finance ha rapporti con Sara, Axa e il gruppo Intesa, ha sviluppato un portale web based, gestito dalla funzione information security, che classifica e smista le richieste di dati ricevute e fornisce strumenti per analizzare casi simili già risolti», precisa Lorini. Per la gestione complessiva della sicurezza, invece, abbiamo messo a punto sistemi di reporting direzionale, ideati per tenere sotto controllo ciò che accade ai sistemi informativi e alla sicurezza all'interno della compagnia». Anche perché è necessario proteggere non solo le macchine interne, ma anche quelle esterne», aggiunge Perrv. «Per intenderci, quelle in uso ai dipendenti e ai clienti. Sono infatti i computer a uso misto (interno ed esterno) a portare virus nel sistema. Per esempio, attraverso un portatile che il dipendente utilizza anche a casa. Un consiglio? Installare a tutti i computer esterni un personal firewall, che serva almeno a fermare gli ingressi illegali di hacker».