PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 3 - numero 429 di giovedì 25 ottobre 2001

Sicurezza: una sfida per le imprese (1/3)

Articolo a cura di Gigi Tagliapietra. "Le peggiori minacce per una rete arrivano da Internet o dal personale interno? Quali sono le precauzioni da prendere? E la legge che cosa dice?"

C'è qualcosa di nuovo nell'aria oggi, anzi d'antico..." Inizia così una famosa poesia che mi pare descriva molto bene l'aria che si respira oggi nel mercato italiano a proposito di sicurezza informatica. C'è una attenzione nuova a un tema maturo. Una delle ragioni è certamente il fatto che lo sviluppo della rete al di fuori delle ristrette mura aziendali, ha generato un'onda molto forte e mai conosciuta in passato, di attenzione e di comunicazione circa le grandi potenzialità e rischi della società dell'informazione. Si sono dette anche molte stupidaggini, è vero, ma c'è oggi una maggiore comprensione del valore intrinseco dell'informazione: come potremmo mai avere una attenzione alla sicurezza informatica senza la consapevolezza forte che le informazioni sono un bene vitale per l'azienda e per il suo successo nel mercato?

Tu chiamale se vuoi emozioni

La sicurezza, è risaputo, è un insieme pervaso da forti elementi emozionali, carico di richiami ai nostri meccanismi più profondi di paure dell'ignoto e ci porta a reazioni talvolta incomprensibili. Ma il primo passo è quello della consapevolezza; dobbiamo sapere che la sicurezza informatica, non diversamente da quella personale o ambientale, è un meccanismo complesso, è un insieme di azioni e comportamenti che non ci potranno mai portare a una certezza assoluta ma a una equilibrata gestione di un rischio.

Se in passato non era facile far uscire il tema dalle stanze degli informatici e dei responsabili dei sisterni informativi, c'è ora una diversa attenzione da parte dei manager di altri settori aziendali: un direttore vendite è consapevole del vantaggio di avere i dati in diretta dalla propria struttura periferica ma capisce che deve proteggere questi dati dalla concorrenza.

Un quadro immediato

Un direttore del personale apprezza il vantaggio di avere un quadro molto più immediato delle proprie risorse ma sa anche che esistono precise responsabilità di legge nella tutela dei dati personali. Un direttore marketing capisce perfettamente che il danno di una violazione di una pagina Web di lancio di un nuovo prodotto è di entità di gran lunga superiore al costo cui si deve far fronte per proteggerla.

Non che sia tutto rose e fiori, non che si siano colmati in pochi mesi diversi anni di ritardo culturale, ma siamo davvero sulla buona strada.

Le fonti del rischio

Da dove viene la maggiore fonte di rischio? Dalla miscela esplosiva di tre fattori: dalla diffusione capillare della rete e dal conseguente aumento del valore complessivo delle informazioni, dallo sviluppo della tecnologia (tanto nel bene quanto nel male) e dal differenziale di conoscenza tra vittime e aggressori.

Il primo fattore, la crescita esponenziale del numero degli utenti, è certo il fenomeno più evidente e, si sa, il rischio di fare un brutto incontro è statisticamente superiore in una grande città che non in un villaggio.

Molti di questi nuovi utenti non hanno la minima consapevolezza dei rischi legati alla connessione in rete; sono attratti dalle potenzialità e dalla quantità di informazioni disponibili e non comprendono un fatto semplice: se io posso vedere dati altrui, la stessa cosa potrebbero fare altri con me.

Supercomputer

La capacità di collegare migliaia di computer attraverso la rete, genera anche capacità di elaborazione simultanea che genera "supercomputer" virtuali di immensa potenza a costo praticamente nullo per chi voglia sviluppare sofisticate forme di violazione delle chiavi crittografiche.

La diffusione, poi, di piattaforme aperte di sviluppo e la capacità di scambio di software è ormai tale per cui, sia in positivo sia in negativo, esistono programmi di attacco e difesa di ottima qualità, il più delle volte gratuiti, sviluppati da team virtuali

composti
dall'aggregazione di centinaia di interazioni tra diverse persone ai quattro angoli del mondo.
Se volete farvi un'idea di quanto questo orizzonte sia vasto, partite dal sito Web di qualunque società che si occupi di sicurezza e troverete i collegamenti più straordinari, dai bollettini dei "buoni" che avvisano costantemente i "naviganti" di Internet delle insidie e degli attacchi conosciuti, fino ai siti degli hacker in cui è come essere al supermercato dello scasso.

II trend dei costi
La crescita del fenomeno complessivo rete/rischio porta con se due fattori apparentemente contraddittori: al crescere della rete cresce la sofisticazione necessaria (e quindi il costo) per proteggersi da eventi indesiderati, la crescita del mercato rende meno costose le soluzioni di base e a larga diffusione. In altri termini oggi è molto meno costoso prendere le contromisure elementari. Le security appliance rappresentano ad esempio tuttora la migliore soluzione per proteggere la connessione in rete di piccole e medie aziende, di scuole o di uffici periferici di grandi organizzazioni.
Inoltre esistono soluzioni davvero poco costose per monitorare e controllare i tentativi di intrusione e per avere una traduzione grafica dei dati che qualunque firewall mantiene accuratamente registrati nei propri archivi di log, in cui tutte le azioni vengono registrate come da un sismografo.
D'altra parte l'estensione della rete genera complessità e realizzare sistemi di autenticazione degli utenti per una organizzazione estesa e con molte persone che si spostano continuamente non è un compito da affidare a uno sprovveduto. Proteggere un sistema pubblico a cui possano accedere decine di migliaia di utenti non è semplice se si vuole (e si deve) far meglio delle poco sicure login e password statiche.

Nei prossimi giorni su PuntoSicuro sara' completata la pubblicazione dell'articolo.

Articolo a cura di Gigi Tagliapietra ? Amministratore Delegato di Siosistemi.

---

www.puntosicuro.it