COS'E' LA SICUREZZA INFORMATICA

Negli ultimi anni il problema della sicurezza informatica si è accresciuto in modo significativo e, con buona probabilità, continuerà a preoccuparci anche nel prossimo futuro.

Questo puo' essere visto come il rovescio della medaglia di un fenomeno, quello della crescente disponibilita' di connettivita', che, come principale obiettivo, produce sicuramente notevoli vantaggi. E gli aspetti positivi portati dalla grande connettivita' sono tali per cui vale sicuramente la pena di continuare nello sviluppo, imparando a gestire razionalmente i risvolti negativi.

Stiamo assistendo al continuo successo del fenomeno Internet. Ormai singoli professionisti ed aziende di ogni dimensione e rango posseggono un accesso alla rete Internet, utilizzato talvolta solamente per navigare e scambiare messaggi di posta elettronica ma sempre più spesso per fornire servizi di varia natura alla propria clientela.

Anche le modalità di accesso ad Internet stanno cambiando, grazie al passaggio dalla semplice connessione telefonica via modem (PSTN o ISDN) alle più moderne ADSL e HDSL, tecnologie che permettono collegamenti più veloci e meno costosi.

Il problema che ne deriva è che sempre più computers sono connessi alla rete in modo permanente e quindi finiscono per diventare potenziali bersagli dei pirati informatici.

Ne' piu' ne' meno di quanto accade per ogni attivita' umana che coinvolge una collettivita', c'e' sempre chi non accetta le regole concordate dai piu' per un correttao comportamento, ma gioca contro: per dolo, per dissenso represso, o, semplicemente, per dispetto.

Le aziende, sempre più legate alle opportunità offerte dalle reti

telematiche, molto spesso ignorano il pericolo che ne deriva in termini di sicurezza dei dati aziendali.

Ma quale dovrebbe essere l'interesse nel violare una rete aziendale?

Molto spesso ci troviamo di fronte a semplici curiosi o piccoli sabotatori che intendono procurare danni all'azienda compromettendo, quasi per gioco, attrezzature e dati, altre volte siamo di fronte a vere e proprie azioni di spionaggio industriale ed appropriazione indebita di informazioni riservate.
Non dimentichiamo inoltre che una buona parte dei furti telematici partono dall'interno dell'azienda stessa, sfruttando le debolezze della rete locale, e vengono solo successivamente completati per mezzo di un attacco esterno tramite Internet.
Così come è importante proteggere l'azienda dall'intrusione di ladri e malintenzionati utilizzando porte blindate e sistemi di allarme nella stessa misura è importante proteggere i dati strategici visto che le reti sono quasi sempre la nostra porta "virtuale" sull'esterno.

LA NORMA SULLA SICUREZZA INFORMATICA

E' opportuno precisare che sono in vigore normative di riferimento (codice penale, legge privacy, regolamenti tecnici) che individuano e richiedono a vario titolo precise responsabilità nell'implementazione nella propria azienda di misure di sicurezza a tutela dei sistemi informativi.

In particolare dal 2001 è pienamente in vigore la normativa che impone alle aziende l'adozione di misure minime di sicurezza nel trattamento dei dati, nell'ambito della più generale disciplina della privacy (legge 675/1996).

Per misure di sicurezza si intendono le procedure e i sistemi finalizzati a ridurre al minimo i rischi di distruzione o perdita dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

A titolo esemplificativo, si tratta di:

- parole-chiave per l'utilizzo di computer e software o per l'accesso a banche dati
- di protezione anti-virus e anti-intrusione
- di creazione e conservazione di copie di salvataggio
- di protezione fisica degli archivi cartacei, etc.

In caso di omessa adozione delle misure minime di sicurezza disposte dalla normativa specifica (DPR 318/99) sono previste sanzioni penali che possono essere comminate indipendentemente del verificarsi degli eventi sopra descritti, di perdita o danneggiamento di dati o di trattamento non consentito.

CHE FARE

Consideriamo tutte le le aziende, enti, studi professionali o privati che utilizzino Internet per il proprio lavoro, specialmente se collegati alla rete con connessioni permanenti quali ADSL, HDSL o CDN.

Quasi sempre non sono in grado di auto-proteggersi in maniera efficace, visto lo sviluppo di sempre nuovi sistemi e strategie d'intrusione.

Solo chi dedica costantemente tempo e risorse allo studio e all'implementazione di soluzioni per la sicurezza può garantire reti in grado di resistere a possibili intrusioni.

Questo obiettivo si realizza in parte attraverso la progettazione ed implementazione di reti 'sicure' ma soprattutto attraverso la fornitura di una serie di servizi correlati e costantemente aggiornati che si rivelano il vero punto di forza nel combattere gli attacchi esterni ed interni alla rete ed ai dati aziendali. Per esempio:

IMPLEMENTAZIONE RETI SICURE

- Creazione di security policies

- Crittografia delle comunicazioni
- Reti private virtuali (VPN)
- Sistemi di analisi delle intrusioni (IDS)
- Monitoraggio costante della sicurezza

VERIFICA E CERTIFICAZIONE DELLA SICUREZZA

- Applicazione di aggiornamenti critici
- Analisi delle security policies
- Tests di intrusione dall'esterno
- Tests di intrusione dall'interno
- Tests di cracking delle password

SISTEMI DI ALLARME

- Raccolta degli alert di sicurezza
- Notifica al cliente dei risultati tramite report
- Sviluppo di strategie di difesa personalizzate

Ing. Claudio Magistroni