Questo articolo è apparso su Ticino Management del mese di gennaioi/febbraio 2006 nella rubrica ATED

Sicurezza informatica e piccole aziende

La Svizzera e le PMI non sono esenti da problemi di sicurezza informatica, come conferma il rapporto Melani, la Centrale svizzera d'annuncio e d'analisi per la sicurezza informatica

Silvano Marioni **www.marioni.org**

Oggi chi vuole documentarsi sul tema della sicurezza informatica può trovare su Internet numerosi articoli sulle minacce e sui rischi informatici. Il fatto che la maggior parte di questi documenti riguardino la realtà americana lascia però il dubbio che questi problemi interessino marginalmente la nostra piccola e sicura Svizzera. È quindi di attualità il primo rapporto semestrale sulla sicurezza dell'informazione pubblicato da MELANI, la Centrale svizzera d'annuncio e d'analisi per la sicurezza dell'informazione. Il documento illustra le principali tendenze ed evoluzioni sul tema della sicurezza e degli incidenti informatici e permette di comprendere che cosa realmente succede in Svizzera.
Tra i rischi presenti sulla scena nazionale nel primo semestre di quest'anno vengono evidenziati l'aumento della criminalità organizzata che utilizza sempre più le infrastrutture informatiche per commettere reati, le reti Bot che prendono il controllo dei PC coinvolgendo gli ignari possessori in attività illecite, la professionalizzazione della scena hacker e gli attacchi mirati di spionaggio contro imprese e enti statali. Tutto questo dovrebbe far nascere qualche riflessione soprattutto per quello che potrebbe accadere in un futuro non troppo lontano. Qualsiasi tipo di organizzazione, sia essa azienda o ente pubblico ha ormai tutte le informazioni indispensabili per le sue attività esclusivamente su sistemi informatici e una loro manomissione potrebbe compromettere in modo importante la qualità del servizio con conseguenti perdite finanziarie. Ma mentre le grandi organizzazioni hanno generalmente i mezzi finanziari e le competenze per affrontare e risolvere al loro interno i problemi di sicurezza, le piccole organizzazioni con sistemi informatici semplici e limitati a pochi PC non dispongono di competenze autonome e sufficienti.
Per sopperire a questa limitazione sono costrette a trovare soluzioni economiche delegando, quando è possibile, le attività di sicurezza ai fornitori di materiale informatico. Questo risolve i principali problemi di sicurezza legati alla tecnologia ma non affronta, né tanto meno risolve, i problemi organizzativi e comportamentali relativi alla sicurezza.
Spesso le piccole organizzazioni non pensano alla sicurezza informatica perché ritengono di non essere interessanti per un potenziale attaccante e trascurano le misure più semplici ed economiche come ad esempio l'uso corretto delle password.
In tutti i casi dove sono presenti dati personali o aziendali c'è sempre il rischio di attacchi esterni ma anche di possibili furti da parte di dipendenti infedeli. Ci sono poi fenomeni nuovi come quello delle reti Bot in cui un attaccante esterno accede al computer e non tanto per i dati memorizzati ma usando la sua potenza di calcolo per svolgere attività illecite.
Ma cosa dovrebbe fare una piccola impresa con le poche risorse a disposizione per verificare la propria sicurezza informatica?
È necessario identificare le applicazioni informatiche critiche ed esaminare l'impatto per l'azienda nel caso di un loro mancato funzionamento con una verifica dei requisiti di sicurezza di base. Innanzitutto la disponibilità dei dati, il requisito di sicurezza più importante per una piccola organizzazione che deve avere la certezza che i suoi sistemi funzionino sempre e correttamente, l'integrità dei dati, la garanzia di protezione contro perdite o danneggiamenti delle informazioni e nei casi in cui è necessario la riservatezza dei dati e la loro protezione da accessi non autorizzati.
Una valutazione della sicurezza informatica permette di fare un inventario delle risorse informative aziendali, siano esse informazioni, apparecchiature o servizi, per definire la loro importanza e criticità. Dopo di che si possono analizzare sia le possibili minacce esterne, sia i rischi comportamentali e organizzativi interni che riducono il livello di protezione dell'azienda.
Tutto questo dovrebbe permettere di capire se i processi di sicurezza informatica utilizzati sono adeguati a garantire le informazioni aziendali e dove fosse necessario prevedere di intervenire con nuove soluzioni di protezione.