CRIMINI E NUOVE TECNOLOGIE
Di Mirco Turco

La protezione dei sistemi informatici è ormai oggi un grosso impegno, non solo economico, per molte aziende e pubbliche amministrazioni. I sistemi informatici gestiscono ormai miliardi di dati e quindi miliardi di segreti industriali che, ovviamente, devono essere protetti e opportunamente gestiti.
Il mondo di internet ha aperto, oltre a vantaggi palesi, anche migliaia di nuove problematiche proprio legate al concetto di sicurezza aziendale. Ogni organizzazione oggi possiede (dovrebbe possedere) una vera policy di sicurezza al fine di combattere attacchi interni ed esterni (inside e outside attack).
Esistono sostanzialmente due fronti di quello che è conosciuto come computer crime: gli hacker e gli insider.
Gestire la sicurezza aziendale oggi non è compito facile proprio in virtù delle molteplici minacce e della complessità intrinseca della materia.
Da un punto di vista teorico e pratico un sistema può essere considerato sicuro quando riesce a soddisfare alcuni principi:
• confidenzialità: accesso ragionato e protetto delle informazioni;
• disponibilità: possibilità di accedere ai dati;
• integrità: considerare il dato integro.
I crimini aziendali interni (insiders) sono molto insidiosi anche perché difficilmente denunciati alle polizie, al fine di proteggere l'immagine aziendale.
Gli attacchi inside comportano:
a) un danno primario: divulgazione dati sensibili
b) un danno secondario: perdita di immagine
Alcune ricerche condotte anche a livello internazionale mostrano che i crimini inside sono sostanzialmente maggiori rispetto a quelli outside e che, paradossalmente (ma non troppo) esiste poca consapevolezza e percezione del crimine/reato informatico.
Gli autori dei crimini informatici interni sono, inoltre, difficilmente rintracciabili ed hanno conseguenze allarmanti per tutte le organizzazioni. E' importante sottolineare che il computer altera sostanzialmente la percezione del crimine (tecno-mediazione).
Alcuni modelli di criminal profiling e le indagini relativi evidenziano che la maggioranza di crimini inside è fatta da dipendenti celibi, di sesso maschile, con un'età di circa 30 anni. Le ragioni spesso sono: difficoltà finanziarie personali o familiari, vendette, insoddisfazioni lavorative (retribuzione, clima lavorativo, …), sensazione di non essere sufficientemente apprezzato dall'azienda, disturbi psichiatrici.
Ai fini della prevenzione e della lotta a tale criminalità, oltre ai riferimenti normativi (legge sul computer crime, privacy, …) occorre operare attraverso opportune strategie di analisi dei rischi e tramite una opportuna formazione tecnica, legale e psicologica. In ogni caso, il fattore principale di rischio è sempre quello umano!