

## CSI/FBI: indagine 2006 sulla sicurezza delle informazioni

A cura di **Simona Petaccia**  
Pubblicato il 13/11/2006

**Vi sono ancora imprese prive di sistemi di difesa a causa del poco budget investito contro le frodi on-line, ma oggi è possibile proteggersi senza spendere soldi ed evitare danni ai consumatori grazie a una campagna di sensibilizzazione alla sicurezza informatica condotta da GlobalTrust**



Secondo la indagine del *Computer Security Institute*, quest'anno le perdite economiche subite dalle aziende campione (615 aziende) ammontano a **268.000 US \$** poiché, sebbene le "difese" si siano ampliate e la sensibilità al problema delle frodi *on-line* si sia sviluppata, vi sono ancora aziende prive di sistemi di difesa adeguati (*Antivirus, Firewall, Intrusion Detection System* ecc.). Il dato relativo agli investimenti in Sicurezza è, infatti, ancora basso (solo il 40% delle aziende dedica oltre il 2% del *budget* dell'ICT alla Sicurezza) e ben il 5% degli intervistati ha dichiarato di non applicare alcun sistema finalizzato alla verifica di efficacia delle misure di protezione. Gartner ha, invece, quantificato il costo del *PHISHING* (frode informatica realizzata con l'invio di *e-mail* contraffatte, finalizzata all'acquisizione di dati riservati per scopi illegali) ai danni dei consumatori negli ultimi dodici mesi: **2,8 miliardi di dollari**, cinque volte ciò che costava nel 2005.

Grazie a una campagna di sensibilizzazione alla sicurezza informatica condotta da GlobalTrust, però, gli utenti del Web possono finalmente contare su un'ampia gamma di soluzioni per combattere le intrusioni e gli attacchi informatici via Internet, senza dover spendere denaro. È, infatti, possibile soddisfare l'esigenza di essere sicuri e protetti durante operazioni finanziarie e interazioni digitali grazie a tecnologie che, distribuite gratuitamente e per sempre, assicurano la protezione delle comunicazioni su Internet (verifica on-line dei contenuti, autenticazione reciproca, crittografia e assicurazione di identità) dalle frodi informatiche e dai sempre più frequenti attacchi di *PHISHING* o di *PHARMING* (truffa on-line che, tramite un intervento creato ad arte sul profilo delle vittime, le indirizza a un sito fasullo che richiede la registrazione attraverso un modulo per carpirne dati sensibili e finanziari).

Ad avvantaggiarsi di questa opportunità può essere sia l'utenza commerciale sia quella privata, entrambe costrette a difendersi dagli *hacker*. La prima è, infatti, obbligata dall'economia moderna a estendere l'accesso alle proprie risorse sensibili a un numero sempre crescente di attori (impiegati, soci, fornitori e clienti) e deve quindi saper gestire sia l'elenco di identità sia le relative responsabilità legate alla loro amministrazione, poiché una cattiva gestione o un furto potrebbe causare ingenti perdite di denaro e danni all'immagine aziendale dovuti alla sfiducia degli utenti nei servizi offerti. La seconda lotta sempre più con una vita dai ritmi frenetici, che può essere agevolata da transazioni online le quali, però, possono minare la riservatezza dei dati personali (carte di credito, recapiti ecc.) con la conseguente possibilità di essere vittima delle truffe informatiche quando si utilizzano i servizi di *E-commerce, Internet Banking* ed *E-business* in generale.

A tutto queste esigenze dettate dalla società della tecnologia risponde, in modo assolutamente gratuito, la **Risk Mitigation Suite (RMS)**: insieme di prodotti e utilità per sensibilizzare gli utenti all'uso sicuro di Internet e dei propri sistemi, personalizzabili su richiesta.

Per maggiori informazioni, visitare il sito web [www.riskmitigation.it](http://www.riskmitigation.it)