La rete delle truffe

Il recente rapporto 2006 sul cybercrime presentato dalla Polizia Postale ha evidenziato come Internet sia diventato il paradiso dei truffatori. Vediamo quanti e quali minacce viaggiano in rete.

Sono sempre più le insidie per chi naviga in rete, secondo il rapporto sulla sicurezza delle reti informatiche presentato a Milano dalla Polizia Postale. Il malware, che comprende virus, worm, dialer e spyware, le truffe, come il phishing e il pharming, l'hacking e lo spam, con gli hoax e le catene di S. Antonio. **I dati relativi al 2006 sono allarmanti: 1.219 denunce nel settore della telefonia fissa e mobile, 1.725 nell'e-commerce (triplicate rispetto alle 566 del 2005), 242 in quello dell'hacking.**
Internet è sempre più spesso utilizzato per commettere reati: dalla clonazione di carte di credito e bancomat ai dati personali carpiti con l'inganno. Come confermato dalla stessa Polizia Postale, per le sue caratteristiche il cyber crime è difficile da individuare e ancor più da combattere. In particolare per la distanza che nella maggior parte dei casi esiste tra il criminale e la vittima. La minaccia criminale nel mondo virtuale infatti, non è paragonabile a quella tradizionale. Ha una connotazione transnazionale, che esula dai confini degli stati, o meglio ancora immateriale, svincolata da ogni riferimento territoriale. I delitti possono concretizzarsi in più azioni svolte in tempi diversi o contemporaneamente, da più soggetti o da uno solo, in luoghi diversi o in uno spazio virtuale.
Attualmente si sta sempre più assistendo a un coordinamento tra criminali con differenti specializzazioni e tra le diverse tipologie di attacchi. Ondate di attacchi virus per esempio precedono intense campagne di phishing e spam. La prima attività di diffusione virale viene infatti utilizzata per introdurre trojan horse e worm in quanti più sistemi possibili, in modo che poi gli stessi possano essere collegati alle botnet (immense reti di sistemi violati) e utilizzati per l'invio massiccio di mail.

Dati pesanti

In ambito e-commerce nel corso del 2006 sono avvenuti 63 arresti per truffe relative al commercio elettronico, 1.725 denunce, 6.245 operazioni di verifica e monitoraggio e 257 perquisizioni. I dati relativi alla telefonia mobile e fissa hanno fatto registrare dati più contenuti, e in particolare: 7 persone arrestate, 1.219 denunce, 780 monitoraggi e 139 perquisizioni. Per quanto riguarda le attività etichettate con il termine generico di hacking (termine utilizzato per indicare genericamente tutte le altre attività illecite perpetrate in rete) sono state infine registrate 0 arresti, 242 denunce, 3.189 i monitoraggi e 51 perquisizioni.
Le attività criminose più frequenti perpetrate via web hanno compreso l'intercettazione di password, la decrittazione delle password, l'intercettazione del traffico Web e della posta elettronica, l'asportazione di documenti e progetti segreti, la sottrazione di account di navigazione e di login alla rete e dei numeri delle carte di credito.

I possibili rimedi

La Polizia Postale non si è comunque limitata a presentare i risultati del rapporto, ma ha **fornito anche una serie di utili suggerimenti per ridurre al minimo l'esposizione alle minacce più comuni**. Come prima cosa, anche se apparentemente può suonare banale, prestare sempre **grande attenzione per gli account, password e servizi prevedendo un cambio frequente delle password e una loro lunghezza specifica** (come del resto, prescritto anche dal D.Lgs. n. 196/2003 e dal relativo allegato B, norme minime di sicurezza e Documento Programmatico sulla Sicurezza). **Prestare attenzione anche al cosiddetto auditing**, ovvero all'ascolto dei problemi segnalati dai dipendenti, la verifica giornaliera dei log, l'analisi delle attività anomale, il controllo dell'applicazione della policy di sicurezza informatica.
Per la trasmissione dei documenti riservati o importanti è stato suggerito **il ricorso a tecniche di crittografia, la raccomandazione a non tenere il pc inutilizzato on line, la regolamentazione dell'accesso ai dati con norme precise e basate su livelli di gestione a seconda delle mansioni svolte in società**. Per ridurre notevolmente i rischi, il suggerimento è stato quello di definire precise policy aziendali in base alle quali non tutti possano accedere a tutto, con particolare riferimento ai dati aziendali. **Particolare evidenza è stata data inoltre alla cura dell'aggiornamento dei software e l'implementazione degli stessi con le relative patch, tramite la costante consultazione dei relativi bollettini sulla sicurezza**.
Anche la posta elettronica è stata oggetto di suggerimenti, con la raccomandazione a **non aprire o copiare un file allegato senza averlo verificato con l'antivirus, a non lasciare il pc collegato a un sistema di posta elettronica senza avere attivato uno screen saver protetto con password, a cambiare con frequenza le password della posta elettronica e dello screen saver, a cancellare i messaggi spostati nel cestino almeno una volta alla settimana, a salvare i dati sensibili in cartelle protette da sistemi crittografici e a non aprire mai per nessuna ragione allegati inviati da sconosciuti.**

Conclusioni

Che Internet fosse diventato un 'territorio a rischio' era ormai un dato di fatto, ma a confermarlo è intervenuto il recente rapporto presentato dalla Polpost (Polizia Postale). **Migliaia di denunce e una nutrita lista di minacce nuove e vecchie hanno confermato quanto siano indispensabili alcune basilari, ma fondamentali, misure di prevenzione per tutti quei sistemi che quotidianamente si affacciano su Internet, o che utilizzano servizi ad esso collegati.**
Nel corso della presentazione del rapporto la Polizia Postale ha indicato alcuni comportamenti base per contrastare le minacce più comuni. A tal proposito **suggeriamo di visitare saltuariamente il sito della Polizia Postale** (http://www.poliziadistato.it/pds/informatica/), nel quale vengono spesso pubblicate guide alla sicurezza e suggerimenti per contrastare le minacce emergenti. **Il ricorso al sito della Polpost è particolarmente indicato alla ricezione di messaggi mail di dubbia provenienza o al verificarsi di episodi sospetti. Spesso infatti le minacce e le tecniche di frode e/o attacco più recenti sono già segnalate sul sito della Polpost, e questo consente di evitare i tranelli di ultima generazione**.