Attacco alla rete informatica: ecco le strategie italiane

Dopo l'attacco a 2.500 aziende e 75mila tra computer e server realizzato da una rete di criminali informatici dell'est Europa, rivelato dalla stampa americana due giorni fa, il direttore della polizia postale italiana Antonio Apruzzese evidenzia che l'unico modo concreto per arginare questo tipo di attacchi è ''aumentare la sicurezza dei sistemi informatici''. Anche perchè, sottolinea, ''gli attacchi degli hacker quasi mai sono improvvisati e, anzi, molto spesso sono preceduti da 'test' per saggiare le difese''.

Più della metà dei colpi che gli hacker realizzano in Rete - rubando identità ma soprattutto numeri di carte di credito e di conti correnti a migliaia di cittadini - sono dovuti al mancato rispetto delle più banali regole di sicurezza sul web. Come, appunto, chiudere la 'porta' quando si esce o proteggere la 'casa' con adeguati sistemi di sicurezza.

L'intrusione che è stata scoperta, dice ancora Apruzzese, ricorda un episodio verificatosi alla fine del 2008, quando i ''pirati'' si impadronirono di dati sensibili di una delle più importanti società che 'processano' i dati informatici.

Un furto che ebbe riflessi anche in Italia, dove furono riscontrate tra le 70 e le 80 mila operazioni effettuate con le informazioni rubate proprio alla società. È dunque molto probabile che anche in questo caso l'Italia venga coinvolta''.

Ma come si protegge l'Italia dagli hacker?

Apruzzese spiega che il sistema messo in piedi dalla polizia italiana si muove su due livelli.

Il primo riguarda quelle che vengono definite 'infrastrutture strategiche', cioè i sistemi informatici delle società che fanno funzionare il Paese: energia, trasporti, economia. Per proteggerle, osserva Apruzzese, ''vengono eretti dei sistemi di fortificazione esterna ai 'castelli informatici', un sistema di vigilanza e sorveglianza che ci consente di registrare in tempo reale ogni anomalia''. In sostanza l'apparato funziona così: ogni azienda ha una sua protezione, interna ed esterna. La polizia postale, con software tecnologicamente avanzati, crea una ulteriore rete di protezione esterna che ha la duplice funzione di proteggere dagli attacchi e di far scattare l'allarme al Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (Cnaipic). Questo fa si che le altre aziende, collegate con il Centro, possano essere avvertite all'istante. Sono diverse le realtà pubbliche o con funzione pubblica che stanno aderendo al sistema.

Il secondo livello su cui agisce la polizia postale riguarda le aziende più piccole e i singoli cittadini. ''In questo caso l'unico vero intervento che si può fare - sottolinea Apruzzese - è quello di dotare i sistemi informatici di antivirus e firewall sempre aggiornati e rispettare le norme di sicurezza'': non navigare e non scaricare da siti ritenuti pericolosi, non rispondere mai a email che chiedono informazioni sensibili, non usare i propri dati su siti che non sono certificati. Insomma, ''chiudere bene la porta di casa''.

20/02/2010