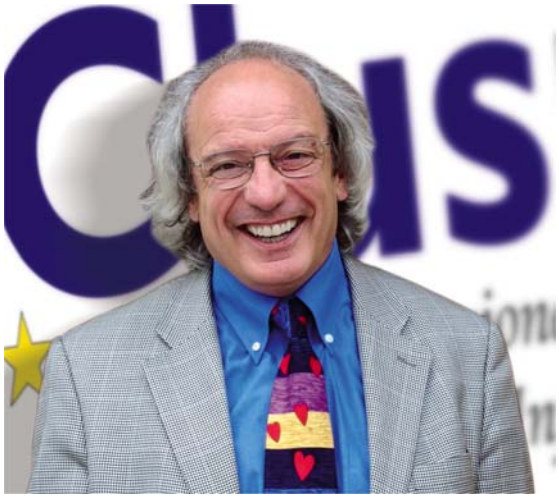
Sicurezza informatica: parla Gigi Tagliapietra, presidente Clusit.
I maggiori pericoli arrivano dai furti di identità elettronica.
La sicurezza del singolo diventa un bene per tutti
(Corriere Economia, luglio 2007)

Le maggiori insidie per la sicurezza informatica arrivano non solo da attacchi diretti, ma anche sfruttando i Pc di ignari utenti. Usati come “trampolini di lancio” per truffe e cybercrimini. Queste le conclusioni dell'Fbi, che tre settimane fa ha comunicato di aver scoperto oltre un milione di computer, che di fatto erano stati attaccati da virus e malware. Gli stessi diventavano così possibili punti di attacco da parte delle cosiddette "botnet". Le reti informatiche “maligne” in grado di controllare sistemi bancari, assicurativi e aziendali. Secondo Gartner Group, entro fine anno il 75% delle aziende avranno computer colpiti da software, capaci di aggirare i tradizionali sistemi di difesa, per mettere a segno attacchi di natura economica. Per saperne di più sul tema della security, Corriere Economia ha sentito il parere di Gigi Tagliapietra, presidente del Clusit di Milano. Una delle più autorevoli associazioni di sicurezza informatica.



In questo momento quali sono i pericoli più gravi per gli utenti del web?
«Sono in crescita tutti i fenomeni di spam, trojan, spyware e i cosiddetti attacchi "zero day". Ma sono soprattutto le botnet rappresentano la minaccia più grave. Molti si ritengono al sicuro perchè non effettuano transazioni di tipo economico. Pensano di non avere dati rilevanti e fanno fatica a comprendere che, con software specifici o catturando le nostre login e password, altri possono usare in modo “invisibile” il loro computer».

Per fare un paragone con la vita quotidiana?
«E' come se un malvivente guidasse la nostra auto per compiere una rapina, mettesse nel nostro garage merce rubata o materiale pornografico. Ma anche compisse un omicidio sparando dalla finestra della nostra camera da letto».

In questo momento, secondo i dati che arrivano al Clusit, qual è il crimine informatico più grave?
«Sicuramente il furto di identità. Quando parliamo di phishing, trojan e malware, dimentichiamo che questi rappresentano la punta di diamante del fenomeno. Il vero scopo è catturare le informazioni relative alla nostra identità digitale per utilizzarla a fini criminali. La Federal Trade Commission statunitense, in un’indagine dello scorso anno ha stimato in 8,3 milioni il numero dei consumatori colpiti da furti di identità digitale. Corrispondente al 3,7% della popolazione adulta».

Allora, come sta cambiando il concetto di security?
«Le intrusioni nei sistemi informativi sono quasi sempre motivate da crimini di natura economica. Dall'epoca in cui gli hacker volevano dimostrare la loro superiorità tecnica o la fragilità dei sistemi, si è passati rapidamente alle azioni del crimine organizzato, che trova in rete un terreno fertile per azioni globali. Dove si può investire con grandi profitti e limitata possibilità di identificazione. La rete, che per la criminalità di tutto il mondo è stata uno strumento per comunicare, oggi si rivela tra i mercati più ricchi. Il web è una infrastruttura vitale non solo per le imprese, ma per l'intero paese».

Ci può fare qualche esempio concreto?
«Pensiamo al recente attacco ai danni dei sistemi informativi dell'Estonia, paralizzata per diversi giorni e costretta a chiedere aiuto alla Nato. Oppure alla vulnerabilità degli Enti Locali, solo in Italia oltre 8 mila e più di 100 mila in Europa. Ebbene secondo il Clusit sono tra i settori più a rischio perché gestiscono servizi critici per i cittadini. Dall'Ici ai servizi scolastici, dall'anagrafe agli acquedotti e non sempre sono consapevoli della loro fragilità. Basta un banale incidente, un guasto o un'incuria interna per creare effetti dannosi. La sicurezza, non è solo la lotta poliziesca contro i “cattivi”, ma lo sforzo di garantire continuità operativa di sistemi vitali per aziende e Pubblica Amministrazione».
Ma la sicurezza ha un costo. Come lo giustifica per una Pmi, già gravata da tasse e balzelli?
«E' vero, ma bisogna fare alcuni distinguo. Il “signor Brambilla" che possiede una piccola azienda meccanica con 12 operai, fa fatica a capire perchè debba spendere soldi per proteggere le informazioni. Il problema non è tanto il rispetto di regole e leggi, è un problema di valore. Allora perchè ha messo l'antifurto al capannone? Perchè se entrano i ladri e gli rubano la merce non solo perde fatturato, ma rischia anche i clienti. Il signor Brambilla deve capire che l'informazione è l'energia invisibile che alimenta la sua azienda. Che permette di dialogare con i clienti, ricevere ordini, sviluppare più velocemente nuovi prodotti. E’ quindi un preciso valore e come tale va protetto».

Allora cosa bisogna fare?
«Le grandi aziende sono consapevoli dei rischi e danno la giusta attenzione alla security. Anche le Piccole e Medie Imprese non vanno escluse dagli obblighi normativi sulla sicurezza, come sembra intenzionato a fare il Parlamento. Allora bisogna tutelarle in modo concreto, aiutandole a capire che il loro futuro e la competitività dipenderà dalla solidità dei loro sistemi informativi. Ad esempio avviando un impegno collettivo che dia alle associazioni di categoria, al Clusit, alle Università e ai soggetti interessati, gli strumenti per supportare le Pmi nella protezione delle infrastrutture informatiche».
In un mondo che diventa sempre più globale come vede la sicurezza?
«La sicurezza non è un tema individuale ed egoistico, è una sfida che riguarda tutti, anche oltre i confini nazionali. Il concetto è semplice. Chi naviga in rete diventa in ogni istante una possibile vittima delle vulnerabilità altrui. Per sintetizzare con uno slogan direi che la nostra sicurezza dipende da quella degli altri».

# # #