VareseNews

La “nuvola delle opportunità” della rete e le sue ombre

Pubblicato: Martedì 11 Giugno 2013

Al crescere dei servizi offerti su Internet, dalla possibilità di fare acquisti fino all’archiviazione dei dati nei cosiddetti cloud – le "nuvole" di dati allocate su server gestori che consentono un rapido accesso di essi da qualsiasi dispositivo: pc, mobile, tablet… – diventa sempre più importante mettere in atto quegli accorgimenti che consentono di proteggere da possibili “attacchi” la propria identità e le informazioni immesse in Rete. A questo occorre aggiungere anche la scarsa dimestichezza di alcuni utenti di questi servizi che, spesso, cadono nei tranelli delle e.mail civetta, il cosiddetto **phishing**, che con vari stratagemmi inducono a trasmettere le proprie password o numeri di carta di credito a chi, dall’altra parte, è pronto a ripulire il conto corrente.

Questo il cuore del convegno che si è tenuto ieri, 10 giugno 2013, al centro congressi **Ville Ponti** di Varese, organizzato dall’**Ordine degli Ingegneri varesino**, che ha visto al tavolo dei relatori alcuni dei maggiori esperti in materia.

Dopo il saluto del presidente dell’Ordine varesino, **Roberta Besozzi**, e del presidente del Consiglio nazionale ingegneri (Cni), **Armando Zambrano**, ad aprire il convegno è stato **Pietro Vassalli**, tesoriere dell’Ordine e componente della Commissione Ingegneria dell’informazione del Cni.
Lo scenario è estremamente complesso, come emerge dall’intervento di **Maurizio Dècina**, ora commissario Agcom (L’autorità per le garanzie nelle comunicazioni) ma a lungo mitico professore al politecnico Di Milano: «Attualmente siamo alla fase 3, al cosiddetto **Internet delle cose** (dopo web e social network): si parla di 1000 oggetti per persona, mille miliardi di entità che parlano tra di loro all’interno di una grande Internet, per fare tutto lo scibile umano: dal controllo dell’ambiente al monitoraggio di quello che succede (alluvione, evento ambientale) alla logistica, al trasporto dei veicoli,

ai servizi mobili, alla sanità, all'ingegneria industriale, all'energia (smart grid) per arrivare alle smart city. **In Giappone sessanta milioni di abitanti usano il telefonino per pagare,** in India i cartelloni delle fermate autobus sono dotati di sensori ai quali ci si può connettere con il cellulare… quindi tra 10 anni come si parlerà di sicurezza nella Rete? Un bel pilastro della sicurezza del futuro è il "Secure element" che sarà inserito all'interno della sim card o, in alternativa, tramite carta esterna, all'interno del dispositivo stesso o nel software».

«La cyber sicurezza non è soltanto un problema del diritto della persona, ma coinvolge anche aspetti quali la proprietà intellettuale e la contraffazione – ha spiegato invece **Nai Fovino –** I nuovi device che ci consentono di essere sempre connessi, purtroppo ci rendono anche vulnerabili: i telefonini sono ormai divenuti dei computer nei quali sono stivate tutte le informazioni che ci riguardano. Nel futuro interagiremo sempre di più oltre che con i vari dispositivi, anche nella nostra casa, anche e soprattutto con infrastrutture critiche. Occorre quindi che queste infrastrutture si dotino di una regolamentazione per la sicurezza. Infine, chi meglio riuscirà a proteggere la propria identità, aumenterà la sicurezza delle proprie attività in Rete».

Molti degli attacchi alla sicurezza però, provengono dall'interno delle aziende: «E' un problema del quale si parla poco ma esiste e causa danni enormi – spiega **Gerardo Costabile**, già ufficiale della Guardia di Finanza e già responsabile sicurezza delle Poste italiane e ora esperto in forensic, analisi sui reperti informatici trovati sulla Scena del crimine – Parlando di cyber spionaggio, sulla rete esistono servizi di vendita on line di "siti clone", di virus (trojan) oppure di infezioni "esclusive" per sottrarre dati, si tratta di veri e propri "supermercati del cyber crimine" con tanto di listino prezzi. Il phishing sta cambiando, il 27% degli utenti del web cade in questi tranelli, ma oggi il messaggio è molto personalizzato e sta diventando un misto tra e.mail e virus, il cosiddetto malware (codice che si installa nel device): mai cliccare su un link di phishing neppure per curiosità, perché oggi ci sono i cosiddetti "drive bad download", vale a dire infezioni che si installano con un semplice click sulla pagina incriminata. Nell'84% dei casi la compromissione iniziale avviene nell'arco di poche ore, mentre nel 22% dei casi il ripristino della normalità richiede anni. Le contromisure? La sensibilizzazione degli utenti sui rischi della diffusione dei dati in Rete».

Ma i nemici veri, chi sono? Prova ad azzardare una lista **Alfredo Gallistru**, vice presidente di Aiea: «I nemici della information security oggi sono gli hacker, alcuni servizi gratuiti on-line, l'inconsapevolezza dei rischi ed il rifiuto dell'applicazione delle best practice, delle elementari norme di sicurezza dell'utilizzo dei sistemi digitali».

Al termine del convegno, moderato da **Carlo Massarini** *(nella foto)*, e di fronte alle tante questioni aperte la risposta degli ingegneri, alla fine si è concretizzata una sorta di decalogo di buone regole per migliorare la propria sicurezza in rete.

Il decalogo completo

Redazione VareseNews

redazione@varesenews.it