La diffusione dalle fake news e la sicurezza informatica

Date : 12 giugno 2017

Ogni qualvolta si diffonde un nuovo ransomware scoppiano il caos e gli allarmi, si scrivono fiumi d'inchiostro digitale per dire e ridire le stesse cose, per descrivere il comportamento del malware, per dare istruzioni su come rimuoverlo o come non farsi infettare, sui possibili responsabili (NSA, Russi, Cinesi, Cia e bad guys generici), ne parlano i TG, ci sono le interviste agli esperti, ai fuffari, ai "digital qualcosa", insomma si muove un vero e proprio circo mediatico, ma la domanda è: a che serve tutto questo?

Faccio una riflessione da osservatore dell'ecosistema delle vite virtuali online ed è basata sul fatto che chi vogliamo informare è sempre colui che, come un esperto sciatore, riuscirà a scansare, con uno slalom olimpionico, tutti i messaggi, articoli ed interviste, inerenti l'argomento che dovrebbero interessargli.

Lo si nota dalla grande diffusione di articoli, video ed interviste che cercano di spiegare perchè i vaccini non causano autismo, che non esistono le scie chimiche, che la Terra non è piatta, se ci si fa caso, i commenti sono per lo più di persone già informate correttamente su questi temi, mentre l'ignorante che dovrebbe leggere e capire cosa sta sbagliando, puntualmente non viene raggiunto da queste informazioni, continuando così a diffondere fake news, bufale, complotti ecc. Ecc..

Il meccanismo del phishing e della diffusione dei malware, gioca proprio su questi fattori, ossia sempre lavorare sul grande numero di utenti contattati, perchè ci sarà sempre un'aliquota di gente che "non ha tempo", non ha competenze, non legge, non si informa, vive come dei bovini al pascolo e che farà quel maledetto click sull'allegato all'e-mail, scatenando l'armageddon informatico.

Sicuramente aumentare e martellando l'informazione sulla profilassi informatica, non fa male, tante persone anche non del settore, sono più guardinghe oggi di quanto lo erano anche solo 5 o 2 anni fa, però non sapranno mai tutto, come non lo saprà mai nemmeno l'esperto, è tutta una questione di livelli di conoscenza del mezzo.

Tutti noi sappiamo che le cinture di sicurezza e l'air-bag possono servire a salvare la vita in caso di incidente, ma un sottoinsieme di "tutti noi", sa che magari deve controllare anche i pneumatici, in giro si vedono spesso automobili con le ruote molto usurate, un altro

sottoinsieme di “tutti noi” magari sa che il pericolo può annidarsi in altre parti meccaniche dell’automobile, ecc. Ecc.

Quindi una profilassi assoluta richiede una conoscenza profonda, e non è nemmeno detto, del sistema o mezzo che si sta utilizzando, un esempio potrebbe essere che qualcuno abbia imparato a non fidarsi degli allegati e-mail, ma poi magari permette l’inserimento di una pendrive USB infetta, nel proprio computer, perché ignora che i malware si possono diffondere anche con questo sistema...

Poi ci sono le contromisure, molti sentono parlare di backup, di non condividere le directory (cartelle) senza protezione, di aggiornare i loro sistemi, ecc.. Ma poi magari il backup lo fanno su un unico disco sempre collegato al computer, in modo da renderlo infettabile agli occhi di un malware, questo non lo sanno, altri non fanno i backup, ecc..

Insomma, il caro vecchio “problem exists between keyboard and chair”, rimarrà sempre un detto valido e solo con una profonda, profondissima opera di “scolarizzazione” si potrà rendere il mondo informatico un posto migliore, ma questa è un’utopia, pensiamo che nel 2017 c’è ancora gente che fa sesso promiscuo senza usare il profilattico e lì c’è in ballo qualcosa di ancor più prezioso che una manciata di bit!

A cura di: **Nanni Bassetti**, *Consulente Informatico Forense*