

Il difficile rapporto tra hacking e marketing (Dopo TIN, Bull: quanti seguiranno ?)

Nei giorni scorsi è apparso un mio editoriale sull'ultima campagna pubblicitaria della TIN, Telecom Italia Network (http://www.apogeeonline.com/informaz/art_314.html): l'impressione è che la caccia alle streghe sia ufficialmente iniziata.

Ho deciso di approfondire l'associazione **'hacker -> pubblicità'** - che tanto sta andando di moda in questo ultimo periodo - insieme a Antonella Beccaria alias Shalom, cercando e volendo un confronto sulle rispettive idee e visioni ideologiche, uno scambio di dati tra i rispettivi cervelli in un brainstorming di cultura, marketing, economia, immagine, logiche, mondi underground, etiche hacker, leggi scritte e non scritte, di tutti quegli elementi insomma che, oggi, compongono ed alimentano la Rete.



Per una migliore visione del contenuto testuale delle due campagne pubblicitarie cliccare sulle immagini.

Inizia Telecom Italia Network, la quale sventola una sagoma in ombra e suggerisce *"Richard Kust, hacker: e pensate di fermarlo con una password?"*. A distanza di qualche giorno la multinazionale a maggioranza francese Bull le dà man forte lanciando a livello mondiale una campagna pubblicitaria contro le intrusioni informatiche: "Carlo" nella versione americana diventa Tom, adolescente bianco Harlem-style su paesaggio misto tra il cyberpunk e un The Day After, e *"non svuota le tasche dei suoi genitori. S'introduce in rete e si impossessa dei dati"* (il chiedermi che ci farà poi a 15 anni con 'sti dati Carlo mi giunge spontaneo: li passerà all'amico Tom via E-mail senza che l'occhio vigile di Echelon se ne accorga? O le multinazionali non si curano di questi "problemi di poco conto"? Mah.....). Più sotto, il colosso europeo fondato nel 1933 affila le armi: *"per sfida o per nuocere, gli hacker, sempre più numerosi, minacciano la vostra rete"*. Peccato che si tratti, in alcuni casi, di armi grossolanamente scheggiate: al contrario della versione online, la campagna stampa di Bull soffre di un errore di ortografia che trasforma gli "hacker" in "haker" (*La Repubblica*, 5 aprile 2000, pagina 5): l'on-line vince di nuovo sul cartaceo? O chi cura le campagne pubblicitarie on-line è semplicemente più "esperto" di terminologia informatica? E "hacker" è un termine informatico o è destinato a dirigersi a breve verso ben altri contesti?

Correttori di bozze distratti a parte, veniamo alla sostanza di questo trend pubblicitario. Trend che si può identificare con una precisa connotazione: *terrorismo psicologico*. Di emergenze sulla sicurezza, intesa in senso ampio e non specificamente informatico, l'opinione pubblica viene periodicamente investita dai mass media: sbarchi di clandestini sulle coste adriatiche sono le più frequenti; città violente; criminalità capillare. Adesso è la volta degli hacker, definiti non solo più dai giornali come "pirati informatici" (l'esempio sconsolante è tratto dal *Collins Mondadori*, dizionario inglese-italiano). Con una sostanziale differenza: rispetto al passato non sono più solo ed esclusivamente giornali ed opinion makers ad accanirsi su eventi specifici amplificandone la portata per invocare stati d'assedio fittizi. Questa volta si va ben oltre perché le aziende, alleate in un patto d'acciaio con le agenzie pubblicitarie (o schiave delle stesse?), palleggiano al marketing il compito di dare nuovo respiro alla minaccia hacker. Detto in altre parole, si vende un servizio perché si genera paura e contro la paura di devastazioni telematiche Telecom e Bull hanno il rimedio. Basta acquistarlo. Un ragionamento semplice e lineare. E tutt'altro che corretto. Nella strategia militare tecniche simili si raggruppano sotto il nome di Information Warfare.

Alla faccia di educazione e formazione alla tecnologia, punto focale all'interno di una società in cui l'informatica ha lasciato già da tempo università e centri di ricerca per entrare nella sfera domestica (e si è solo all'inizio), si torna

a giocare in modo decisamente più violento sulla non conoscenza dell'individuo. Una non conoscenza che molto più che in passato genera, nel migliore dei casi, diffidenza, considerando le potenzialità di strumenti tecnologici costantemente in evoluzione.

Eppure, se si dovesse ragionare in termini strettamente di bilancio, l'allestimento di corsi di formazione costituirebbe la voce positiva per i profitti aziendali. Anche se sorge un dubbio: che i fatturati perdano importanza di fronte ad una merce di ben più valore? Se ragionassimo seguendo panorami futuribili alla Bruce Sterling, inizieremmo a far lavorare la fantasia ipotizzando scenari di oligarchie dell'informazione, censura dei contenuti, codici sorgente irrimediabilmente oscurati. A pensarci bene Sterling non si sbagliava affatto, almeno a mio avviso...

Facendo però un passo indietro e lasciando la fantascienza, appare chiara la non volontà di educare all'informatica e alla rete da parte di Telecom, Bull e aziende di pari dimensioni. È necessario dunque che esista una controparte che prenda l'iniziativa. Chi è l'hacker? Una splendida definizione l'ha data Steward Brand, fondatore del *Whole Earth Catalog*. *"Penso che gli hacker - programmatori innovativi e irriverenti che si sono consacrati al loro lavoro - siano stati la più interessante e sincera incarnazione dell'intellettuale (...). Riorganizzando l'era dell'informazione intorno all'individuo, attraverso il personal computer, gli hacker possono ben dire di aver salvato l'economia americana"*. E non restano una figura romantica ascritta alla storia dell'informatica e avulsa dalla realtà, soprattutto quella commerciale. Perché Eric Raymond, autore del volume *The cathedral and the bazaar*, partendo dall'impegno degli hacker e della comunità open source, descrive in una recente intervista rilasciata a Linux Journal la nascita di una nuova 'ecologia aziendale'. *"Dal momento che tutti stanno giocando con le regole open source invece di quelle della competizione, c'è una potenzialità per la cooperazione anche in modo da fare più soldi (...). Tutte queste persone condividono lo stesso dna centrale, ed è questo a far funzionare l'ecologia"*. Come dire: qui nessuno ruba, ma costruisce, anche dal punto di vista economico. E soprattutto costruisce qualcosa di nuovo. Ad iniziare dalla filosofia aziendale.

Cosa prevedere allora in questo scenario cyber grottesco? Tin e Bull sono solo le prime di una lunga cordata di imitazioni, una moda che vedo alquanto prossima a scatenarsi: Symantec è pronta ad uscire ed una McAfee non dovrebbe rimanere ferma a lungo.

Una volta le cose che prime erano "brutte" diventavano belle, le mode cambiavano e da banditi o terroristi si diventava eroi: l'hacker è evidentemente un personaggio estremamente sfigato. Se svolge il suo ruolo (che è, di fatto, quello di violare un sistema) viene arrestato e deve sopportare pene e multe molto pesanti; continuando a rimanere "il cattivo" nell'immagine comune, ma avendo anche la pubblicità che lo usa come uomo immagine. Infine, come se tutto ciò non bastasse, non ce la fa neppure a trarne giovamento, perché i suoi possibili clienti, frastornati dal battage pubblicitario, non si fidano di lui...

E allora via!, corriamo tutti ad inseguire l'hacker cattivo, corriamo tutti a tuffarci nel nuovo business che è l'I.T. Security: gli hacker, quelli veri, continueranno a bucarvi, con o senza il tool dell'ultima ora proposto dal fornitore di turno. E gli hacker, quelli veri e cresciuti, continueranno a fare sicurezza seria senza campagne pubblicitarie perché, per fortuna, le aziende che hanno *veramente* necessità di sicurezza stanno iniziando a capire la differenza tra l'*élite* e la massa. Che si parli di sicurezza, consulenze, pagine web o traduzioni...