Parliamo di ….

Sicurezza: intervista a Raoul Chiesa

A cura di Massimo Pavese, Ingegnere, PhD, giornalista

Conosciuto come Nobody negli anni '80, pioniere degli hacker oggi si definisce Ethical Hacker ed è uno dei più noti e stimati consulenti di sicurezza informatica a livello internazionale

Che la sicurezza sia ormai diventato un settore centrale dell'industria informatica è evidente. Al punto che lo stesso premier Monti ha recentemente dichiarato: "Un attacco cibernetico può produrre effetti devastanti ed immobilizzare l'intero Paese". Un grido d'allarme lanciato all'inaugurazione della scuola per gli "007" italiani. Sul tema abbiamo sentito l'opinione decisamente molto qualificata di Raoul Chiesa, Presidente di Security Brokers ScpA, cybercrime advisor presso l'UNICRI e membro del Permanent Stakeholders Group dell'ENISA, l'agenzia europea per la sicurezza informatica. Origini piemontesi, volto da eterno ragazzo, è riuscito a fare di quella che era una passione un'affermata professione. Dieci domande. Dieci brillanti flash sulla materia.

1. Sentiamo parlare in continuazione di sicurezza informatica è solo un grande business o una vera necessità?
È assolutamente una vera, concreta e molto sottovalutata necessità. Certamente, è anche un business: nonostante il settore sia molto variegato spaziando dall'hardware al software alla consulenza, di più tipi, è un settore che purtroppo non conosce crisi. Dico purtroppo, perchè il fatto che non ci sia crisi significa che i problemi continuano ad esserci. Spesso si sottovaluta l'importanza dell'InfoSec l'Information Security. Viviamo oramai in un mondo totalmente informatizzato, dipendiamo completamente dall'ICT. Quando dobbiamo prenotare un aereo o un hotel, fare shopping se paghiamo con carte di credito e bancomat, effettuiamo o riceviamo chiamate, fisse o mobili che siano, l'energia che consumiamo. Tutto oggigiorno è gestito da infrastrutture informatiche. Che possono essere violate, abusate, attaccate. Ecco perchè, molto banalmente, ci serve l'ICT Security.

2. Mi spiega i suoi rapporti con le Nazioni Unite e cosa fa come consulente.
Ho iniziato nel 2004 a collaborare con l'UNICRI, l'agenzia delle Nazioni Unite che si occupa di criminalità e giustizia, insegnando ad alcuni loro master di specializzazione. Nel mentre, stavo curando un progetto di ricerca, l'Hacker's Profiling Project (HPP), che ho poi deciso di "donare" all'UNICRI e che portiamo avanti insieme a loro ed all'ISECOM (Institute for Security and Open Methodologies). Ad oggi è il più grosso progetto di ricerca al mondo nel settore del profiling applicato all'hacking, il che significa in parole povere che stiamo cercando di fotografare il mondo dell'hacking, i suoi attori e comportamenti, gli aspetti sociali, etici, legali di questo fenomeno in continua evoluzione. Per dirne una, quando iniziammo nel 2004-2005 non c'era Anonymous, non si parlava di "Cyber Warfare" ed il mondo del cybercrime era nettamente differente meno noto, meno diffuso, con realtà molto più piccole rispetto ad oggi.

3. Lei ha cominciato dall'altra parte della barricata. Ha voglia di raccontarmi qualcosa della sua vecchia vita?
Io iniziai avvicinandomi al mondo dell'hacking nel 1986, nell'era precedente ad Internet. Era l'epoca delle reti X.25, DECnet, le BBS ed il phreaking telefonico. Scoprii un mondo completamente nuovo, potevo confrontarmi con persone dall'altra parte del mondo, effettuare chiamate gratuite ovunque e soprattutto, imparare ad utilizzare i sistemi informatici e le reti di telecomunicazione. Incontrai hacker che oggi sono guru o personaggi famosissimi, quali Kevin Poulsen, Kevin Mitnick, Otto Sync, Venix. Fu un periodo bellissimo e molto particolare, anche perchè in svariati Paesi, tra cui l'Italia, non esistevano ancora leggi contro l'hacking, come avvenne invece nella prima metà degli anni '90. C'era il fascino del selvaggio west. Ero un hacker, avevo accesso a sistemi informatici e dati da fare drizzare i capelli un pò come nello storico film "Wargames". Ma non ho mai danneggiato i sistemi in cui entravo, non ho mai rubato denaro nè rivenduto le informazioni a cui avevo accesso. Ero semplicemente un ragazzo curioso che voleva imparare e viaggiare virtualmente per il mondo.

4. Oggi un ragazzino sveglio con un pc può veramente ancora mettere a repentaglio la sicurezza di un grosso ente?
Si, decisamente si. Anche un ragazzino, se sveglio e capace e con tanto tempo da investire può mettere a serio repentaglio la sicurezza di grossi enti, aziende o governi. Gli esempi non mancano e sono oggetto di cronache quasi quotidiane.

5. Nel 2007 c'è stato il caso eclatante della situazione estone con la chiusura dell'intero paese alla rete. Preistoria irripetibile o pensa che un caso del genere possa ripetersi?
Certamente. Anzi, sta già accadendo, ma in forma più subdola. L'Estonia è stato un caso eclatante, ma molto recentemente il CERT della Georgia ha denunciato pubblicamento una vera e propria operazione di furto di informazioni a suo danno, concertata dalla Russia e probabilmente con il sostegno o supporto del governo di Putin. La stessa cosa dicasi per il recentissimo attacco ad Aramco a Riyadh ed un'infinità di altri. Il problema è che il confine tra "Cyber War", parola forte e, forse inappropriata almeno per il caso dell'Estonia e lo spionaggio, politico, militare o industriale che sia, è sempre più sottile.

6. Quando si sente un arresto di un carder di solito sono criminali dell'est, almeno in Italia, spesso Bulgari o Rumeni. Dov'è la capitale del crimine informatico?
Dipende dal crimine. Se si parla di carte di credito abusate a livello "fisico" quindi, skimmer bancari, phishing abbastanza "di base", la Romania. Se parliamo di frodi via internet "classiche", i nigeriani sono dei maestri da sempre. Se parliamo di cybercrime ad alto livello, Russia ed Ucraina. Illuminante in materia il recentissimo report di Trend Micro.

7. Mi è recentemente capitato di intervistare un giovane hacker che ha dichiarato di essere parte di Cha0. Crede sia possibile che il più famoso, almeno dal punto di vista mediatico, hacker mondiale non sia in prigione in Turchia?
Uno non fa "parte di Cha0". Cha0 era una persona, con tanto di nome e cognome, arrestato dalle autorità turche come lei giustamente dice, oramai alcuni anni fa: il tutto, tra l'altro, è egregiamente spiegato in libri quali Kingpin di Kevin Poulsen di prossima uscita agli inizi del 2013 per Hoepli di cui ho curato l'edizione italiana, the Dark Market di Misha Glenny e Fatal System Error di Thomas Menn. Attenzione però, Cha0 non aveva nulla a che fare con l'hacking o con la sicurezza informatica. Molto più semplicemente, era diventato il più grande rivenditore di skimmer del mondo, riuscendo a scalzare dal podio persino il crimine organizzato rumeno, leader prima di lui in quel settore. Gli skimmer, per inciso, sono quei dispositivi hardware che si applicano nei bancomat, nella "fessurina" dove inseriamo la carta, copiano fisicamente il bancomat stesso, che viene poi clonato da bande criminali ed utilizzato per prelievi fraudolenti.

8. Il primo ministro inglese ha recentemente parlato di 27 miliardi di danni dovuti al cyber crimine, pensa sia un dato attendibile?
Sono cifre difficili da stimare, perché di stime si tratta. Symantec ha tirato fuori la cifra di 337 miliardi di dollari. Credo sia davvero molto difficile fare una stima economica dei danni conseguenti il cybercrime. Group IB ha fatto secondo me il lavoro ad oggi più attendibile, quotando l'introito diretto, e non quello indiretto come ha fatto invece Symantec. Nel nostro settore ci sono molti dubbi; ricordo anche alcuni post di colleghi esteri scettici a tal proposito quanto me su queste cifre, spesso sparate non dico a caso ma quasi. In merito invece ai ricavi diretti, le stime che vanno dai 6 ai 12 miliardi di dollari, per il 2011, sono giuste ed, anzi, purtroppo al ribasso.

9. Hanno ragione Saviano o Micha Glenny a dire che la criminalità organizzata è passata su internet?
Si hanno totalmente ragione. Ma è anche vero che in Italia le mafie nostrane non hanno ancora "colto l'occasione", salvo rarissimi, piccoli ed isolati casi. Sarà forse perchè da noi fanno più soldi con gli appalti truccati ed il gioco d'azzardo online?

10. La rete è libera? Lo so la domanda è stupida può tranquillamente non rispondere.
No, non lo è. Ed anzi, il trend che vedo è quello di volerla controllare sempre di più. C'entra e non c'entra, ma il caso MegaUpload secondo me è emblematico per capire cosa sta accadendo. E non sono segnali positivi.