Software libero, libertà di software

Interlex 02-12-2002

Trasparenza della PA: una commissione "chiusa" per i programmi "aperti"

E' normale che della commissione insediata dal ministro Stanca non si conoscano nemmeno i nomi dei componenti? Ed è giusto che la commissione lavori "per" il software libero e non con l'obiettivo di verificare "se" esso è preferibile per la pubblica amministrazione? Ecco alcuni interessanti punti di vista: discutiamone.

L'open source è una scelta politica (M. Cammarata)

Qualche ipotesi di lavoro per la commissione open source (A. Monti)

Se la risposta è già nella domanda (G. Scorza)

Lo scenario dell'open source in un documento dell'AIPA

E in tutto questo, che c'entrano gli hacker?
Il pensiero del ministro delle comunicazioni espresso in un discorso del 14/02/2002

I giovani: hacker o spett-autori?

Il termine “hacker” ha assunto attualmente significati diversi e talvolta contrastanti. Sicuramente individua gli esperti nelle tecnologie alla base della rete Internet, ma ha assunto connotazioni diverse non sempre in positivo.

Nell’immaginario collettivo gli **“hacker”** sono prevalentemente dei giovani che passano molte ora davanti al computer e che sono in grado di sfruttarne la potenzialità dei PC molto oltre la media. E’ proprio la conoscenza approfondita delle tecnologie, e talvolta una condizione di disagio, isolamento, esclusione da comunità naturali in cui è favorito il processo di socializzazione, che li porta a dominare la rete. Praticamente hanno quel *know how* che gli permette nel giro di poco tempo di imparare a fare qualsiasi cosa, riuscendo a trovare nella rete i siti giusti da cui apprendere preziose informazioni.

L’ **“hacker”** è quell’indirizzo email a cui chiederemmo un consiglio. E’ l’esperto che scrive nelle mailing list, che partecipa ai news groups. Ama la libertà della rete, quella senza confini, ma si da un ferreo codice di comportamento. E’ quella persona che ti da volentieri un consiglio, ti aiuta a braccia aperte, ma se si innervosisce ti ritrovi scollegato dalla rete senza nemmeno saperne il perché !!!

Internet per loro non è solo un luogo di studio o di lavoro: spesso è un luogo di incontri virtuali, un topos in cui possono crearsi una nuova identità per sfuggire dagli stereotipi con cui vengono liquidati dalla società. Combattono guerre virtuali nelle chat di IRC per “opparsi” (acquisire privilegi) e conquistare il dominio completo di un canale o per “bannare” (cacciare) chi non rispetta alcune regole di comportamento. Non si può continuare a stereotipare il loro modo di comportarsi: oramai sono un fenomeno radicato, complesso, sfuggente, da studiare e prendere in esame nei dettagli e nelle sfumature che lo caratterizzano.

A volte il loro nome viene collegato con quello dei cyber-criminali. E può essere anche vero che la preparazione e le conoscenza di cui dispongono gli gli permetta di perpetrare crimini telematici. Tuttavia non è giusto generalizzare e considerare tutti coloro che sono in grado di forzare un sistema informatico come potenziali criminali. Nella rete non è così facile fare questi distinguo, se un navigatore è in grado di infiltrarsi in una rete aziendale di solito lo fa solo per semplice curiosità, mentre è facile immaginare che vada a ricercare i più profondi piani aziendali e chissà quali segreti industriali.

Di solito navigano di sera, lavorano nel campo delle TLC o magari studiano informatica, ingegneria, fisica… , e vivono l'informatica come un hobby che progressivamente gli invade sempre di più la vita fino a plasmare la loro identità, quella reale. Magari lavorano malvolentieri come programmatori per una software house, mentre nel tempo libero sviluppano e ridistribuiscono codice open source.

E' un mondo di paradossi e contraddizioni quello degli "hacker", sono più facili da catturare in un termine che non da descrivere o definire.

Tuttavia accanto a questa visione poetica dei più grandi esperti della rete occorre anche prendere in esame i comportamenti, sicuramente meno romantici, di quella parte seppur limitata di criminali che commettono reati nella rete. In generale possono identificarsi tre tipologie di attacchi da attuare attraverso Internet: gli attacchi criminali, gli attacchi a scopo pubblicitario e gli attacchi basati su sistemi legali.

Gli attacchi a scopo pubblicitario sono i più diffusi e tuttavia i meno pericolosi. Hanno una motivazione molto semplice: provocare abbastanza disagio per attirare l'attenzione della stampa. Possono essere attuati attraverso il così detto "Denial of Services" (DoS), il sistema di attacco attraverso la negazione del servizio.

Gli attacchi criminali possono consistere in frodi, attacchi distruttivi a sistemi informatici, furti della proprietà intellettuale, furti d'identità, di marchi registrati, violazione di proprietà, violazione della privacy, sorveglianza o spionaggio, analisi di database riservati, analisi del traffico e spionaggio elettronico su vasta scala. Sebbene non sia ancora facile imbattersi in questo tipo di crimini, è importante continuare a formare reparti delle forze dell'ordine, come ad esempio la Polizia Postale e delle Comunicazioni, in grado di confrontarsi sullo stesso terreno dei cyber-criminali. Anche la magistratura, tuttavia, deve acquisire una maggiore coscienza dei crimini realizzati nelle reti elettroniche, perché non è sempre necessario l'intervento del legislatore, in particolare quando la validità di un provvedimento può essere estesa per analogia ai crimini elettronici sulla base di procedure già definite per la criminalità convenzionale.