Questo articolo è apparso sul Corriere del Ticino di sabato, 10 febbraio 2001 nella sezione Informatica e Sicurezza

Internet: quali rischi per gli utenti

Gli stati dovrebbero definire misure giuridiche per gli utilizzatori

Silvano Marioni **www.marioni.org**

Internet è un esempio importante di liberismo tecnologico. Basta dotarsi di comuni apparecchiature informatiche e si è subito pronti a ricevere e inviare qualsiasi tipo di informazione nei quattro angoli del mondo. Se pensiamo alle modalità e alle regolamentazioni che hanno caratterizzano la diffusione di altri mezzi di comunicazione quali il telefono o la radio, viene da chiedersi come abbia fatto Internet ad imporsi a livello mondiale in così breve tempo.
La risposta sta nella sua idea di base. Alla fine degli anni '60, quando il Dipartimento della Difesa americano iniziò a progettare quella che sarebbe diventata la rete Internet, decise di non utilizzare una struttura di tipo centralizzato, perché sarebbe stata più vulnerabile in caso di attacco militare. Al contrario pensò a un sistema decentrato, dove ogni partecipante avrebbe avuto la sua autonomia, limitandosi solo a specificare i protocolli di comunicazione.
Questo spiega perché oggi nessuno è in grado di controllare Internet e perché chiunque può collegarsi senza nessuna autorizzazione particolare. Negli anni successivi utilizzando questi protocolli si costruirono numerose reti, utilizzate soprattutto a livello accademico, e quando queste reti furono collegate tra loro, all'inizio degli anni novanta, nacquero Internet e il World Wide Web. Ma quella che si è presentata come una nuova grande opportunità ha mostrato anche il rovescio della medaglia.
Gli attuali mezzi di comunicazione ci hanno abituato ad una serie di certezze in particolar modo per quanto riguarda la nostra privacy. Internet è una rete di reti in cui non è possibile definire il percorso di una comunicazione tra due punti. Non c'è nessuna garanzia che un messaggio inviato ad esempio tra Lugano e Zurigo resti all'interno del suolo elvetico. A dipendenza dei collegamenti dei fornitori di servizi Internet, il messaggio potrebbe ad esempio transitare attraverso gli Stati Uniti dove sono collocati i principali nodi di interscambio delle reti.
Se andiamo oltre gli aspetti della privacy ed esaminiamo l'utilizzo che oggi si fa di Internet a livello aziendale scopriamo che le ripercussioni possono essere ancora più gravi.
Internet è molto pratico e veloce per l'invio di messaggi elettronici ed è sempre più utilizzato dalle aziende per lo scambio di corrispondenza. L'invio sicuro di corrispondenza commerciale ufficiale quali offerte, ordini, fatture, contratti richiede una serie di accorgimenti tecnici non sempre banali. Troppo spesso questi accorgimenti non vengono adottati e allora documenti, che in formato cartaceo verrebbero spediti in modo sigillato e protetto, vengono inviati sulla rete in modo chiaro e leggibile come fossero delle cartoline postali. E contrariamente ad un invio postale, dove siamo in grado di vedere se qualcuno ha manomesso la busta, un messaggio elettronico non ci indica se qualcuno è riuscito a carpirne il contenuto o addirittura a modificarlo.
La tecnologia informatica propone oggi una serie di accorgimenti tecnici per mettere al riparo da occhi indiscreti e rendere sicura la comunicazione su Internet e questo vale soprattutto per le attività di commercio elettronico che sempre più aziende e organizzazioni stanno portando su Internet.
Questo non toglie che, data la natura aperta e anonima di Internet, qualsiasi malfattore possa presentarsi sulla rete e tentare di mettere a segno truffe, furti informatici o altri reati. Da qui l'importanza per i singoli Stati di iniziare a definire anche le misure giuridiche che direttamente o in collaborazione con altri Stati permettano di garantire le protezione dei propri cittadini dai nuovi reati della rete.

Dai malfattori vecchio stampo alla nuova criminalità informatica

Intervista con Lorenzo Valeri dell'International Center for Security Analisys di Londra

Quali sono i possibili crimini che si possono presentare su Internet e quali rischi rappresentano per la società? Ne abbiamo parlato con Lorenzo Valeri, Research Associate presso l'International Centre for Security Analysis di Londra, dove si occupa di temi quali l'impatto della tecnologia sulle attività militari, la guerra elettronica e le sue ripercussioni su Internet

Che cos è l'ICSA, quale attività svolge e con quali scopi?

L'International Centre for Security Analysis, è un centro studi indipendente collegato al Department of War Studies del King's College di Londra. Sin dalla sua nascita nell'ottobre del 1996, il Centro ha concentrato la sua attività di ricerca sull'impatto di Internet sulla sicurezza nazionale ed internazionale. In particolare, i ricercatori si concentrano sui problemi legati all'utilizzo offensivo e difensivo di Interne,t con lo scopo di fare delle analisi il più precise possibile. Queste attività di analisi, svolte esclusivamente con il monitoraggio di fonti pubbliche permettono di preparare delle politiche per combattere la criminalità informatica in modo efficace e efficiente.

Quali sono per ordine di importanza gli attacchi informatici che si nascondono dietro ad Internet e quali sono le tipologie di "malfattori"?

È difficile fare una classificazione di attacchi informatici perché le tecnologie, sia di difesa che di attacco, sono sempre in evoluzione. Riguardo alle tipologie di possibili malfattori, bisogna fare una distinzione. Da una parte abbiamo i malfattori "vecchio stampo" che hanno deciso di utilizzare Internet per fare attività illecite di tutti i generi, molte delle quali vorrei dire causate anche da una certa ingenuità dell'utente Internet. Abbiamo poi i cosiddetti nuovi malfattori come gli hackers di diverso livello e capacità tecnica. Infine, chiaramente non va dimenticato il crimine organizzato che ha aggiunto Internet e e-commerce al suo portafoglio di attività illegali, quali sfruttamento della pornografia, riciclaggio dei denaro, ecc.. Infine, alcuni autori hanno parlato di organizzazioni statali. In questo senso è difficile fare un'analisi per mancanza di dati. Si è parlato recentemente di simili attività a seguito delle discussioni riguardanti Echelon. Queste attività creano solo una cattiva fama alla Rete e insieme ai numerosi attacchi informatici di cui si sente parlare, possono minare la fiducia dell'utente verso Internet. Il successo di Internet e delle attività commerciali collegate è legato al fatto che un numero sempre crescente di persone accede alla rete, non solo per la ricerca di informazioni, ma anche per acquistare e vendere beni e servizi. Questo può continuare ad avvenire solo se esiste la fiducia nei confronti delle capacità commerciali e tecniche delle società attive su Internet. Attacchi informatici, insieme a violazioni della privacy da parte di alcune società commerciali e organizzazioni governative, possono minare questa fiducia. Un esempio in questo senso arriva dall'Inghilterra dove un sondaggio del National Consumer Council ha indicato che 7 utenti inglesi di Internet su 10 hanno paura ad utilizzare la carta di credito via Internet. Simili statistiche sono confermate anche negli Stati Uniti da parte del Pew Internet and American Life Project.

Come e con quali mezzi i vari Stati riescono a contenere i rischi e a reagire ai possibili attacchi su Internet?

Gli Stati occidentali, capitanati dagli USA, stanno affrontando con una certa rapidità il problema della sicurezza informatica. Gli USA hanno creato strutture come il Critical Information Assurance Office, al fine di coordinare le attività di difesa a livello federale. Simili attività si stanno formando anche nel Regno Unito, in Francia e Germania. La cosa interessante è che dopo un iniziale approccio "nazionale", si è ormai convinti che l'unica via di uscita è la cooperazione internazionale. Interessanti in questo senso sono le recenti attività del G8, dell'Unione Europea e dell'OCSE. Le linee guida di queste iniziative sono più o meno identiche: cooperazione con il mondo privato per la lotta al crimine informatico, definizioni di linee guida oppure convenzioni internazionali come quella attualmente in discussione al Consiglio d'Europa, e investimenti nel campo della ricerca e delle risorse umane.

Possono i singoli Stati utilizzare queste infrastrutture non solo in modo difensivo ma anche per danneggiare o appropriarsi delle informazioni non tanto del singolo consumatore, ma di organizzazioni pubbliche o private di un altro Stato?

Si è parlato di questo rischio specialmente nel contesto di Echelon e del suo utilizzo per lo spionaggio economico da parte degli Stati Uniti.

Alle accuse europee, ha risposto James Wolsley, ex direttore della CIA, attraverso le pagine del Wall Street Journal dicendo che gli USA spiano perchè gli Europei corrompono quando si tratta di vincere grandi contratti internazionali. Una difesa che fa sorridere! Che le tecnologie informatiche possano permettere delle nuove possibilità di spionaggio, non c'è dubbio. Ma vorrei ricordare che molte delle attività di raccolta delle informazioni spesso richiedono un monitoraggio delle cosidette “fonti aperte”. Spesso si scopre più leggendo che spiando. Certo, leggere è lungo, spesso noioso e richiede attenzione, ma le tecnologie informatiche possono aiutare in questo. In conclusione, i rischi ci sono e continueranno ad esistere, ma non sono nuovi. Bisogna sempre ricordarsi che Internet non ha cambiato tutto, ha solo reso molte delle attività passate più veloci ed efficaci.