

per prendere delle contromisure è necessario prima avere cognizione del problema

## Ecco come ci possono spiare sul web

### Mailbox, navigazione, instant messaging tutto è potenzialmente esposto allo sguardo altrui

MILANO - Un tempo si pensava che le intercettazioni potessero essere appannaggio della sola magistratura o di esperti di spionaggio internazionale. Oggi non è più così. A diversi livelli siamo diventati potenzialmente tutti un po' spioni. E non occorre essere dei «cyber-terroristi» o degli «hacker».

PERCEZIONE DEI RISCHI - Le tecnologie digitali ci consegnano infatti una grande libertà d'azione e con essa ovviamente una grande responsabilità. Tuttavia, l'utente medio è scarsamente sensibile alla cura dell'ambiente informatico che sta fisicamente alla base della sua vita digitale. Nell'uso quotidiano di macchine, software e protocolli di rete diamo per scontati parecchi passaggi sui quali può fiorire ogni genere di controllo illecito e intrusione.

LAN - Su internet è possibile reperire centinaia di applicativi che servono per controllare ed avere piena visione dei dati in entrata e in uscita da una qualsiasi LAN (local area network). Una LAN è per esempio la rete interna (locale) dei computer di un ufficio, siano essi un numero di tre o di cento. Oppure i terminali in rete tra loro di uso domestico, ma anche quelli di una scuola o di un Internet point.

FREE-SNIFFER - Basta poi digitare «free sniffer» su un qualsiasi motore di ricerca per avere un'idea dei programmi disponibili in forma gratuita o quasi per eseguire delle intercettazioni. L'attività di sniffing consiste infatti nell'intercettazione passiva dei dati che transitano in una rete telematica. Gli sniffer, occorre precisarlo, sono programmi usati e implementati legittimamente per fare analisi del traffico di rete. Questi software sono nati per risolvere problemi, per fare debug, analisi statistiche e migliorare lo sviluppo delle reti. Non sono quindi di per se da criminalizzare. Tuttavia è vero che se ne possa fare un uso scorretto e che possano contribuire ad alimentare il fai-da-te delle intercettazioni.

VIOLARE LA PRIVACY - Esistono poi alcuni sniffer che hanno degli obiettivi specifici e a seconda del caso è possibile capire se sono stati creati appositamente per violare la privacy oppure per fare analisi di rete. Per esempio uno sniffer dedicato a intercettare le comunicazioni via MSN (instant messaging) difficilmente avrà un uso lecito, poiché gli unici dati in transito su questo tipo di protocollo sono assolutamente privati. Ma, guarda caso, sniffer di questo tipo sono tra i più scaricati dagli utenti della rete. Lo stesso vale per quelli dedicati ad estrarre informazioni dagli allegati di un client di posta. Applicativi di questo genere sono acquistabili per meno di venti euro.

PICCOLI FRATELLI - Mailbox, navigazione, instant messaging tutto è potenzialmente esposto allo sguardo altrui. Dal momento in cui lo sniffer entra in azione, e prende visione di tutto il traffico di una rete, il passo nella direzione di modificare i dati in transito è breve o lungo a seconda delle competenze e dell'interesse di chi lo sta usando. Un fidanzato geloso? Un capufficio diffidente? L'inquilino del terzo piano? La verità è che accorgersi della presenza di uno sniffer è davvero molto difficile, soprattutto se non si ha alcuna percezione, nemmeno culturale, del fenomeno. Oltre ai potenziali Grandi Fratelli, siano essi Google o Facebook, è bene sapere che ci sono anche tanti potenziali piccoli fratellini che giocano più o meno lecitamente anche sulle reti maggiormente vicine a noi.

SICUREZZA INFORMATICA - Per proteggersi è prima di tutto essenziale prendere coscienza dell'importanza che le tecnologie hanno nella nostra vita. Non solo perché le macchine diventano sempre più la sede delle nostre memorie e del nostro lavoro, ma anche perché il loro funzionamento non è sempre completamente delegabile ad un «esperto». Da un lato quindi è giusto fare richiesta formale ai fornitori di servizi e di software protezioni adeguate, dall'altro è necessario fare uno sforzo di formazione e cominciare ad interessarci alle tecnologie relative alla sicurezza informatica. In primis ai software che ci garantiscano una migliore riservatezza nella navigazione e in seconda battuta a quegli strumenti che ci aiutano a rendere inviolabili le nostre e-mail.

Lavinia Hanay Raja  
stampa |