E' di alcune ore fa la notizia, rimbalzata in tutto il mondo, di un megaprogetto del governo inglese per la messa a punto, si parla già per la fine dell'anno, di un sistema per l'intercettazione trasparente della posta elettronica da e verso l'utenza inglese. E pare che lo stesso parlamento europeo non sia proprio immune all'attrattiva di questa possibilità.

Lontano da sguardi estranei!

Dall'Inghilterra l'intercettazione trasparente della posta elettronica

di Raffaello De Masi

Ovviamente la cosa ha scatenato un putiferio in Gran Bretagna, dove le associazioni in difesa dei consumatori e garanti della libertà di comunicazione si sono fatte, anche energicamente, sentire, in difesa dei loro sacrosanti diritti. Come al solito, la cosa è stata fatta rientrare attraverso una dichiarazione del governo in cui si ammette l'esistenza del progetto (costato un centinaio di miliardi), ma che verrà finalizzato solo a indagini mirate; in altre parole l'uso del sistema sarà possibile solo dietro autorizzazione scritta del giudice. In bel modo per dire tutto e non dire nulla! E poi, come dicevano i romani, "Quis custodiet custodes?", chi controllerà i controllori?

E non basta; ascoltate questa! Pare sia stato definitivamente accertato che il popolare pacchetto RealJukebox abbia contenuto una routine che, arbitrariamente e senza alcuna periodicità, durante l'uso, trasmetteva alla casa produttrice dettagli sull'uso e sulle preferenze musicali dell'utente. Per essere precisi pare che il programma invii un pacchetto di informazioni contenente il tipo di pacchetto MP3 utilizzato, il numero di file MP3 presenti sul disco dell'utente e, se in quel momento si è connessi a Internet, anche il titolo del brano ascoltato in quel momento. Anche qui, ovviamente, lo scandalo non è tardato a scoppiare, e la compagnia ha assicurato che la nuova versione, già in distribuzione, aprirà una finestra in cui si chiede all'utente se è disposto a trasmettere questi dati che, ipocritamente, si dichiara siano stati finora prelevati a soli fini statistici!

Ormai non si è più sicuri di nulla. Non siamo ancora all'incubo di Orwell, ma non è mica detto che il Grande Fratello debba presentarsi sotto la maschera di spietato persecutore. In Giappone ormai quasi più nessuno usa la carta di credito, che, nessuno ci aveva pensato (vero?), è un ottimo sistema per monitorare l'attività e il movimento di una persona. Ogni giorno, a ogni pie' sospinto, per accedere a servizi offerti gratuitamente (ah, che spirito francescano!) su Internet, occorre fare una lunga trafila, in cui ci viene chiesto di rivelare praticamente ogni nostro dato, e poco ci manca che ci chiedano anche quando abbiamo fatto la prima comunione e la rosolia. Vi domanderete a cosa serva dare tutta questa messe di dati, compreso indirizzo reale, codice fiscale e indirizzo di posta elettronica. Ve lo spiego subito, in maniera brutale; queste generose persone collezionano un bel portafoglio di indirizzi, bell'e pronto per essere "affittato" a produttori che abbisognano di distribuire materiale pubblicitario, sia elettronico che cartaceo. E la legge sulla privacy? e le profferte di antispamming distribuite a piene mani nelle home page? Campa cavallo...

Cerchiamo di difenderci!

La comunità Internet è piena di persone che credono che la CIA, l'FBI, il KGB e le polizie e i servizi segreti di altro mezzo mondo siano pronti a spiarci per carpire i nostri segreti; pronti a superare le nostre password, a scoprire i nostri segreti, a leggere la nostra posta o a controllarci mentre facciamo chat. Non siamo proprio a questo, ma quanto ne siamo lontani?

Il fatto è che, da quando ci colleghiamo al Internet, non facciamo altro che lasciare, a destra e a manca, tracce e impronte del nostro percorso e delle nostre attività. Non è certo molto diffici-

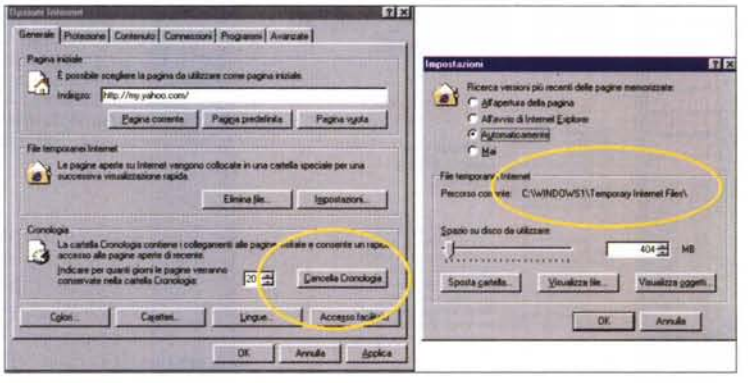
le monitorare la navigazione di un ignaro utente attraverso un semplice controllo continuo della sua connessione. Il solo sistema sicuro per tenere confidenziali i propri dati è di tagliare la linea telefonica, prendere a martellate il cellulare, tagliare la carta di credito, e ritirarsi in una grotta. In caso contrario si è soggetti al pericolo che qualcun altro possa controllare le nostre attività. Tutto sta a ridurre i danni il meno possibile. In altre parole, usare, per battere questi indiscreti occhi tecnologici, esattamente le stesse armi, la tecnologia. E un poco di sale in zucca!

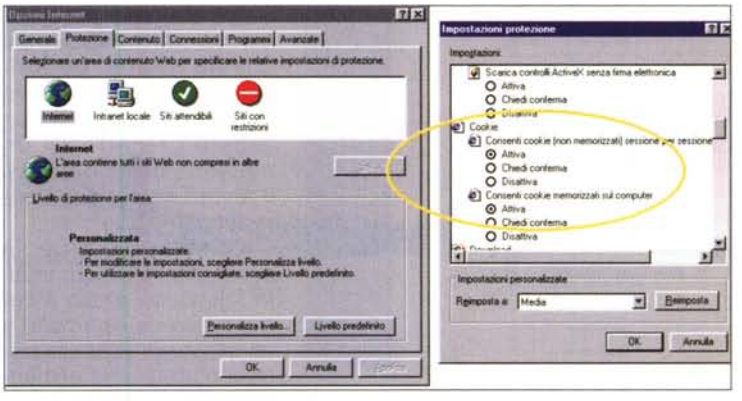
Perdonatemi la banalità, ma è inutile dotate la propria casa dei più sofisticati sistemi d'allarme, se poi si ha l'abitudine di lasciare le finestre spalancate. In altri termini, non dimentichiamo le basi più semplici della sicurezza, prima di adottare le più potenti e sofisticate tecnologie di protezione, con chiavi a centinaia di bit e connessioni più sicure di Fort Knox.

Ad esempio, non lasciare mai, in computer che possono essere utilizzati da altri (ad esempio quello dell'ufficio), informazioni riservate personali, come numeri di carta di credito o di conto corrente; e non culliamoci sulla falsa sicurezza di averli custoditi con una password! Si potrebbero avere amare sorprese! Lo stesso vale quando si usa un computer a disposizione anche di altri per operazioni come credito in linea o acquisti; non inserire mai dati "sensibili" in un sito non dotato di "secure server", e, se proprio si è costretti, assicurarsi di cancellare la cache e la cronologia dopo l'uso, e a conclusione della navigazione (in Explorer, Strumenti‡ Opzioni Internet‡ Generali‡ Cancella Cronologia).

Molti servizi, a cominciare dal collegamento iniziale, si basano sull'uso di password (ad esempio e-mail, drive virtuali personali, servizi bancari on-line, ecc.). Bisognerebbe avere password diverse per ognuno di essi (salvo riunire sotto una stessa stringa quelli di scarsa importanza) e cambiarle con una certa frequenza, se non tutte almeno quelle di importanza vitale. Quando si sceglie un nome, cerchiamo di essere creativi e non usiamo dati facilmente prevedibili, come nomi di mogli e figli, date di nascita, numeri telefonici o targa della macchina, anche se scritti al contrario, e con una lettera sì e una no. Una combinazione senza significato di lettere maiuscole, lettere minuscole e numeri è poco facilmente prevedibile da una persona diversa da chi l'ha creata (ovviamente saremo tanto furbi da evitare di tenere nel portafogli un foglietto di promemoria; non ridete, molti si portano appresso, accanto alla tessera del Bancomat, il foglietto con il numero di accesso. O magari fanno un bel file di testo, e lo conservano sul desktop!)

Per non lasciare traccia della nostra navigazione , ricorrere alle opzioni del nostro browser!





I cookie sono utilissimi, ma possono nascondere qualche insidia! impariamo come difenderci!

Anonymizer, http://www.anonymizer.co vi permetterà di viaggiare su Internet senza essere intercettati

Password, sempre password.

Molte persone usano continuamente il loro PC, magari un portatile, come compagno di lavoro e come diario-segreteria personale. Mai come

http://www.privacy.org è una organizzazione dedicata alla difesa della privacy, che indice ogni anno un concorso per l'assegnazione degli Orwell d'oro alle persone, siti o organizzazioni che si sono distinte nel violare la privacy delle persone. Bel riconoscimento!

in questo caso l'uso delle password è indispensabile (pensate solo allo smarrimento o al furto del portatile!).

La maggior parte dei word processor, spreadsheet e, ovviamente, database includono questa opzione (alcuni possono essere protetti anche con una doppia password, in modo da legare a due persone differenti l'apertura di un particolare documento), e anche molti client di posta elettronica sono dotati di chiave delle rispettive cartelle. Non credere di poter proteggere il PC ricorrendo alla password di Windows. Come abbiamo già diverse volte fatto notare su queste pagine, essa riguarda solo le preferenze d'uso e, a meno di non essere legati a un network, basta premere il tasto Esc per superare lo sbarramento.

Lo stesso vale per la password sul BIOS; inutile fidarsi, superarla è come rubare le caramelle a un bambino. Basta togliere la batteria che alimenta i servizi interni e il gioco sarà fatto; col vantaggio di non sentire neppure piangere il ragazzino.

Se il PC viene utilizzato anche dai nostri figli, potrebbe essere il caso di utilizzare un pacchetto come CyberSitter (http://www.cybersitter.com) o CyberPatrol (http://www.cyberpatrol.com) , o ancora NetNanny (http://www.netnanny.com) di cui abbiamo parlato in questa rubrica il mese passato. Se i bambini sono piccoli, forse la soluzione più interessante è rappresentata da KidDesk Internet Safe, che crea quello che viene definito un "walled garden", un giardino circondato da mura, vale a dire un'area dove il bambino si può muovere ma da cui non può sconfinare. Pregevole e affidabile; lo trovate da http://www.ionasoft.com/.

Se il vostro PC è utilizzato da altre persone nel vostro ufficio, e desiderate che la vostra attività, una volta conclusa, non sia più raggiungibile da alcuno, tenete bene da conto che non basta gettare nel cestino il materiale elaborato e poi "tirare la catena". I dati sarebbero facilmente recuperabili con la più stupida delle utility di "undelete" reperibile in commercio.

Se avete necessità di gestire la cosa proprio in questo modo, usate un'utility che sovrascrive ripetutamente l'area occupata dal file cancellato; la trovate in McAfee Office (http://www.mcafee.com) e in System Mechanic (si chiama Incinerator, http://www.iolo.com)

Molti dischi rigidi di qualità e molti PC di marca vengono forniti di utility destinati al recupero di dati, in caso di crash del sistema.

Questi pacchetti, come Nasp'N'Shot e GoBack, possono essere utilizzati anche per recuperare dati frettolosamente cancellati; quindi disinstalliamoli. Inoltre, teniamo in considerazione che usare il PC del posto di lavoro per usi personali potrebbe non essere compatibile con le direttive del nostro datore di lavoro, e che, nonostante tutta la privacy di questo mondo, ci sono diversi sistemi di monitoraggio dell'attività dei dipendenti.

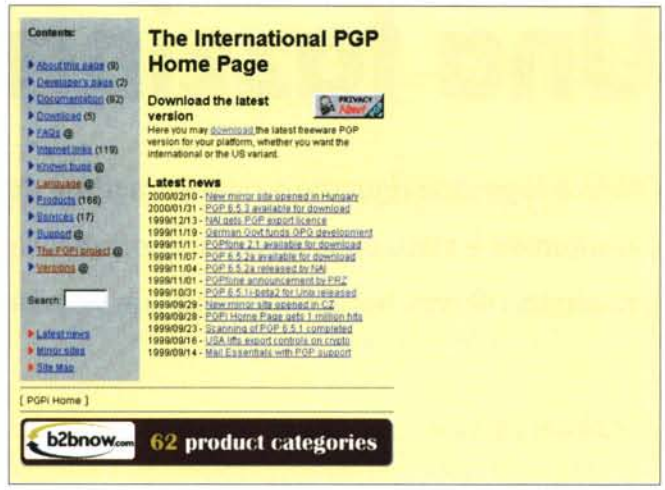
PGP, l'angelo custode della nostra posta

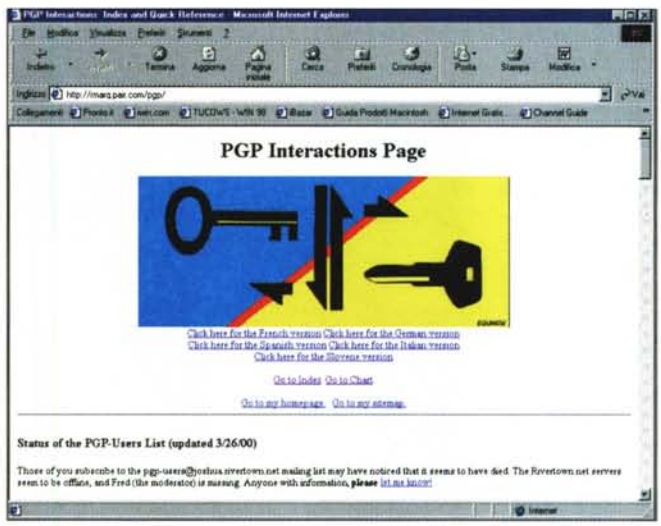
Cosa è PGP? Semplice, è un programma di cifratura della nostra posta che permette di spedire e ricevere messaggi che non possono essere letti durante il transito in rete. Il pacchetto si recupera da http://www.pgpi.org e, una volta installato, si aggiunge automaticamente a Outlook, creando in questo anche nuovi bottoni.

Per utilizzarlo occorre creare, la prima volta, la nostra chiave PGP. Schiacciamo il bottone appena creato, e ci troveremo di fronte a una finestra che ci chiederà una serie di dati , tra cui anche l'indirizzo di posta elettronica (stare molto attenti a digitare quest'ultimo dato; se si dispone di diversi indirizzi di posta, digitare esattamente quello che poi verrà gestito da PGP; la precisione è necessaria, altrimenti la chiave PGP sarà inutilizzabile). Ci verrà chiesto poi di digitare una password (in gergo passphrase) che terrà nascosta a occhi indiscreti la nostra chiave – ricordiamoci che più lunga è la password più è difficile da violare. Andiamo avanti e il programma ci chiederà alcune personalizzazioni riguardo all'ambiente; all'inizio lasciare tutto com'è, ci sarà tempo poi per provare le altre personalizzazioni. Ci verrà chiesto infine se si desidera fare l'upload della nostra chiave pubblica su un server PGP; la cosa è conveniente, in quanto non saremo costretti poi a inviare la stessa chiave a ogni utente cui invieremo posta.

A questo punto è finito tutto; usiamo Outlook nel solito modo e, se desideriamo inviare un messaggio cifrato, schiacciamo il nuovo bottone Encrypt; o , se si vuole dimostrare che il messaggio arriva proprio da parte nostra, schiacciare Sign. Pochi minuti, insomma, per poi usare la nostra posta in sicurezza.

aAnche Intel è molto attenta alla privacy dei suoi clienti, come membro della TRUST Privacy Program.I nostri bambini vogliono navigare con noi; accontentiamoli, partecipando alle loro avventure!





La pagina della http://www.pgpi.org. Il più popolare pacchetto di crittografatura di posta è disponibile in diverse versioni dedicate ai più differenti sistemi operativi , dal Windows al Mac all'Amiga e perfino allo Psion e al BeOS

Forse la cosa migliore è proprio non usare il PC dell'ufficio!

Biscottini da uno sconosciuto.

Indipendentemente dalla manipolazione dei dati personali conservati sul PC, occorre tenere presente che navigare nella rete è sempre fonte di esposizione , magari anche per dati non proprio riservati. Navigando è facile essere monitorati riguardo al nostro accesso e a una serie di altri dati e valori, come tipo di browser usato, IP address, e perfino risoluzione del nostro schermo. Non ci credete? Provate a collegarvi a http://www.anonymizer.com , per una dimostrazione in linea e, eventualmente, per prendere le opportune precauzioni.

I "cookie", i biscotti che riceviamo quando visitiamo molti siti, sono una grande comodità e, poiché sono facilmente editabili, ben difficilmente eventuali "pirati" ricorrono ad essi per attaccare il nostro sistema. Comunque, se il baco del sospetto vi rode fin nell'intimo, chiedete al vostro browser di non accettarne; andare sempre in Opzioni Internet e scegliendo Protezione‡ Personalizza Livello. Qui, oltre a disabilitare l'accettazione dei cookie, potremo ulteriormente personalizzare altre scelte, come quella relativa ai plug-in ActiveX, agli applet Java e così via. La contropartita è rappresentata dalla continua richiesta, però, di riempimento di finestre di accesso. C'è da dire, però, che i cookie possono essere usati anche per scopi, non diciamo illeciti, ma non proprio corretti. Ad esempio quelli depositati dai banner pubblicitari servono per determinare certe abitudini dell'utenza che, anche se non investono informazioni personali, possono essere usate a scopo di marketing.

E così abbiamo concluso. Non avremo certo sconfitto il grande fratello, ma almeno non siamo state vittime prone; a presto!