Informatica

Proteggere il computer è ancora possibile?

di Nicola Bortolotti

Mentre - come ipotizzato e auspicato nel numero scorso - è giunto in extremis con il D.L. 24 giugno 2004, n. 158 il più che giustificato rinvio del termine del 30 giugno per la presentazione del primo DPS (Documento Programmatico sulla Sicurezza) da parte della moltitudine di utilizzatori professionali del computer che non era sin qui soggetta agli adempimenti sulla privacy - se non a quelli davvero minimi previsti dal DPR 318 del 1999 - è opportuno soffermarsi in questo numero su alcuni particolari propedeutici alla redazione del documento.

Una proroga senza troppo clamore

Come si ricorderà, la proroga è giunta anche per l'imbarazzante ritardo con il quale è stata licenziata dal garante della privacy la promessa "Guida operativa per redigere il Documento programmatico sulla sicurezza", facilmente reperibile sul sito all'indirizzo www.garanteprivacy.it e sulla quale si sono basate le tabelle esemplificative pubblicate sul numero scorso della rivista. Se la guida è a portata di click, così come la pubblicità talora fuorviante di un gran numero di software che promettono una compilazione pressoché automatica del DPS, quasi fosse solo una mera formalità burocratica, in rete è assai meno evidente la notizia della proroga. Al contrario - in molti siti informativi, compreso quello del garante - vi sono numerosi richiami che farebbero ancora credere alla tassatività del termine del 30 giugno.

È dunque bene rammentare quanto riportato - in maniera invero criptica - in coda al D.L. 158, pubblicato sulla Gazzetta Ufficiale n. 147 del 25 giugno 2004: "Art. 3 - 1. Al decreto legislativo 30 giugno 2003, n. 196, concernente il codice in materia di protezione dei dati personali, sono apportate le seguenti modifiche: *a) all'articolo 180, comma 1, le parole: '30 giugno 2004' sono sostituite dalle seguenti: '31 dicembre 2004'*; b) all'articolo 180, comma 3, le parole: 'entro un anno dall'entrata in vigore del codice' sono sostituite dalle seguenti: 'entro il 31 marzo 2005'; c) all'articolo 181, comma 1, lettera a), le parole: '30 settembre 2004' sono sostituite dalle seguenti: '31 dicembre 2005'."

Un software datato può essere meno vulnerabile

Il Documento Programmatico, comunque, non è che la punta dell'iceberg di adempimenti che possono essere assai pesanti (e onerosi, qualora non si segua la strada maestra dell'open source) soprattutto qualora si trattino dati sensibili - anche se in piccole realtà.

C'è tuttavia un diffusissimo e pericoloso malinteso, circolante anche tra gli addetti ai lavori, che si può sintetizzare nell'equazione "software 'vecchio' = software insicuro = inadempienza agli obblighi di legge".

In realtà i fatti - documentati e documentabili - degli ultimi anni smentiscono in modo anche clamoroso questa semplicistica affermazione, almeno per quanto concerne il diffusissimo mondo Microsoft.

Vero è che sistemi operativi come Windows 95/98/ME non offrono adeguate protezioni a livello "locale": chiunque possa accedere fisicamente al PC (che va quindi protetto almeno con la password del BIOS all'accensione) può infatti esplorare senza problemi tutto l'hard disk di quella macchina. Questo può tuttavia accadere anche con un Windows NT/2000/2003/XP mal configurato o - in ogni caso - se la macchina prevede la possibilità di fare il "boot" da CD (e a quel punto basta - ad esempio - uno Knoppix per bypassare le protezioni standard)...

Il punto tuttavia è che - a livello di rete - tutte le più gravi vulnerabilità degli ultimi anni (con conseguenti pandemie virali) sono state manifestate solo dai sistemi operativi Microsoft più avanzati (NT/2000/2003/XP) e non dai più economici e vetusti.

Questa notazione non riguarda solo i sistemi operativi: i più seri allarmi degli ultimi tempi hanno riguardato Internet Explorer e Outlook Express 6 SP1 e non la più anziana ma ancora supportata (di entrambi) versione 5.5 SP2. Paradigmatico è anche l'ultimo preoccupante warning che riguarda addirittura qualcosa di fino ad ora inoffensivo come la visualizzazione di immagini JPEG, reperibile nel bollettino ufficiale Mi-

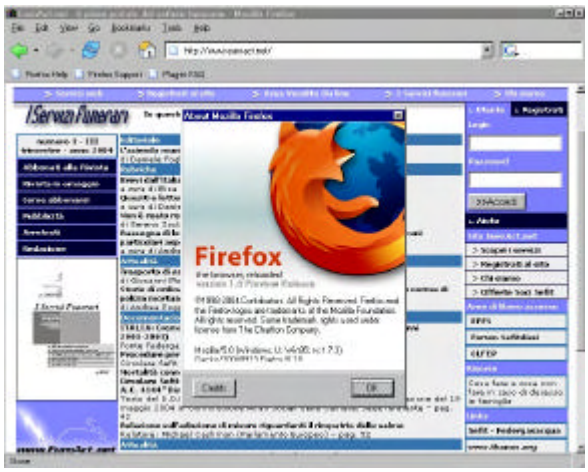

Figura 1

crosoft all'indirizzo www.microsoft.com/security/bulletins/200409_jpeg.mspx, e che affligge anche le ultime versioni di Office.

Gli "update" non bastano

Lo scaricamento automatico degli aggiornamenti di sicurezza, che potrebbe essere considerato tra le misure minime, in realtà porta più luci che ombre: non di rado gli update provocano più problemi ed effetti collaterali di quanti ne risolvano, per cui l'installazione deve essere sempre supervisionata da un amministratore per prevenire e limitare i problemi. Ma che dire poi di "Service Pack" di centinaia di MB che impiegano mezza giornata per installarsi (salvo problemi) e che al termine possono bloccare alcuni applicativi? E del "periodo finestra" tra la scoperta della vulnerabilità e l'approntamento della patch?

Cambiare software

In taluni casi la migliore "misura minima" è quella di cambiare programma. Potrebbe sembrare una provocazione, ma in realtà il consiglio giunge da fonte autorevolissima. Nel giugno scorso destò infatti sensazione in tutto il mondo il bollettino dell'US-CERT www.kb.cert.org/vuls/id/713878 nel quale la partnership statunitense tra pubblico e privato per la protezione della rete informatica nazionale (United States Computer Emergency Readiness Team) concludeva la lista delle soluzioni prospettate suggerendo nientemeno di "Utilizzare un altro web browser".

Tra le alternative disponibili a costo zero, forse la migliore in assoluto è rappresentata oggi dal portentoso Mozilla Firefox (figura 1), scaricabile dal sito ufficiale www.mozilla.org/products/firefox dove è possibile downloadare - al link www.mozilla.org/products/thunderbird - anche una alternativa ad Outlook Express.

Firefox, ormai prossimo alla versione 1.0 ufficiale, è un prodotto assolutamente maturo che - con soli 4.5 MB di programma di installazione - consente di navigare senza problemi anche nei siti ottimizzati per Explorer - ad esempio quelli delle principali banche - offrendo un ottimo livello di sicurezza nonché una serie di utilità integrate come la soppressione dei fastidiosi pop-up.

Immunizzarsi dagli spyware

Non di soli virus può soffrire un computer: assai pericolosi per la salvaguardia della privacy sono ad esempio i cosiddetti programmi spia o "spyware", che si installano silenziosamente alla sola visita - talvolta involontaria - di numerose pagine web.

Oltre al cambio di browser, che non sempre è totalmente efficace, esistono due strumenti possibili per limitare l'azione di questi pericolosi parassiti: la rimozione di quelli esistenti e l'immunizzazione per prevenirne di nuovi.

Sono nati pertanto programmi in grado di assolvere a questi compiti, molti dei quali a pagamento per utilizzo commerciale come il noto AdAware. Ben presto si è però affermato l'ottimo software gratuito del tedesco Patrick M. Kolla: SpyBot (homepage www.spybot.info o security.kolla.de), giunto alla versione 1.3, è ormai diventato un must. Una volta installato e rimosso lo spyware esistente, con un click è possibile immunizzare in pochi secondi il proprio sistema (figura 2).

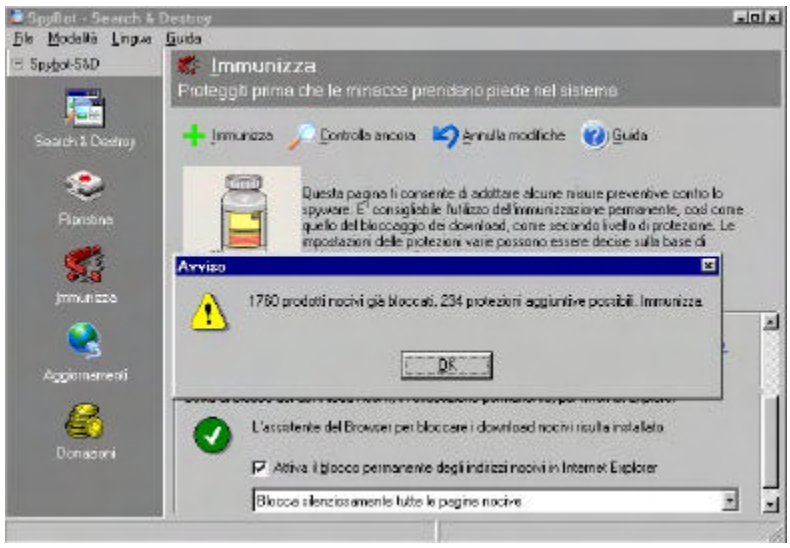

Figura 2

Figura 3

Attenzione al server

Tornando ai sistemi operativi, il problema di sicurezza locale ricordato prima, riguardante Windows 95/98/ME, non li rende tout-court inadeguati ai sensi del D.Lgs n.196/2003 sulla privacy: è infatti sufficiente far si che nella rete locale i dati siano memorizzati su un unico server che consenta l'accesso solo tramite l'idonea accoppiata user/password per superare l'impasse e mantenere senza timori i "vecchi" Windows.

Ogni considerazione sulla sicurezza, ovviamente, si sposterà ora sul sistema operativo del server.

Esistono ottime ragioni, oggi più di ieri, per privilegiare la scelta di un sistema operativo Open Source come Linux sul server: la maturità raggiunta dal software gratuito Samba, che consente a una macchina Linux di operare in una rete Microsoft Windows come primary domain controller con grande efficienza ed estrema flessibilità; la protezione intrinseca offerta dai robusti filesystem e dalle funzionalità native di firewall, routing e NAT; la disponibilità di server web, di posta, proxy, tutti gratuiti e a livello professionale; la insensibilità alla maggior parte dei virus circolanti in rete.

Configurare in maniera corretta un server Linux non è molto più arduo del configurare un server Microsoft con un livello di sicurezza paragonabile.

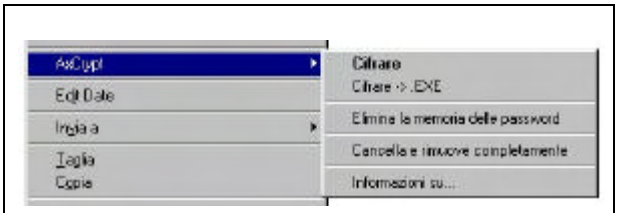

Figura 4

Crittografia a costo zero

Oltre alla protezione mediante credenziali di accesso, è possibile anche aggiungere un ulteriore livello di protezione crittografando i files contenenti dati di particolare interesse.

Tutti i programmi di compressione dati (dal notissimo WinZip al gratuito e potente 7-Zip, visibile in figura 3 e scaricabile all'indirizzo www.7-zip.org) offrono possibilità di protezione tramite password, ma se si desidera qualcosa che offra un livello di sicurezza elevato (pur senza arrivare alla crittografia a chiave pubblica) come l'algoritmo simmetrico AES, successore della tripla DES e divenuto standard statunitense, ci si può rivolgere all'ottima applicazione open source AxCrypt di Axon Data (homepage www.axondata.se): dopo l'installazione, con un banale click sul tasto destro del mouse si può accedere alla semplicissima estensione del menu (figura 4) che consente di cifrare (figura 5) o decifrare (se con estensione .axx) qualunque file in pochi istanti.

Figura 5