▶ Sicurezza

Difendere il PC dagli intrusi

Come controllare se il vostro sistema operativo è vulnerabile? E quali strumenti utilizzare per scegliere se accettare, rifiutare o eliminare i cookie? Abbiamo selezionato i quattro migliori programmi gratuiti che troverete nel CD ROM

Ogni software che viene sviluppato non è mai privo di bug. Per quanti test possano essere sviluppati prima del rilascio, sempre più di frequentemente accade che, dopo l'installazione, emergano problemi inattesi o si evidenzino deficienze più o meno gravi.

I difetti nascono dalle configurazioni hardware su cui vengono utilizzati, dalla piattaforma software adottata (basti pensare alle differenze che ci sono tra i vari sistemi operativi e addirittura tra le diverse versioni di Windows), dalle applicazioni installate (quando si installa un nuovo programma questo deve essere in grado di funzionare correttamente senza causare problemi alle altre applicazioni e condividendo, spesso, risorse e librerie di sistema).

Si comprende, quindi, come il lancio di un nuovo sistema operativo sia un'operazione ancor più delicata: per quanto siano lunghi i periodi di beta testing e approfonditi i controlli ai quali viene sottoposto il prodotto che acquistiamo molto spesso nasconde al proprio interno alcune imperfezioni che vengono messe a nudo soltanto durante l'utilizzo quotidiano da parte di molte persone.

Nella pratica, dopo che un sistema operativo viene lanciato sul mercato, gruppi di utenti, associazioni e aziende specializzate, continuano a effettuare pesanti test in modo da mettere in luce eventuali pericolose falle. In alcuni casi si tratta invece di persone che lo fanno per soddisfazione personale, per dimostrare come un sistema operativo possa essere violato; nella norma si tratta di vere e proprie aziende che effettuano queste prove per difendere la sicurezza delle reti dei propri clienti.

Proprio per questi motivi, Microsoft ci ha abituato, sin dalle prime versioni dei suoi sistemi operativi, a patch e Service Pack. Le *patch* sono "rattoppi" del sistema operativo che consentono di risolvere imperfezioni e bug mentre i *Service Pack* sono veri e propri aggiornamenti gratuiti, prelevabili da Internet, che raccolgono solitamente tutte le patch rilasciate in precedenza e talvolta includono anche nuove funzionalità.

Al momento della stesura di questo articolo, sono usciti, ad esempio, nel corso dei mesi, ben sei Service Pack per Windows NT 4.0, due per Windows 2000 (è in arrivo il terzo) mentre è di imminente uscita il Service Pack 1 per Windows XP.

È bene, tuttavia, non attendere l'uscita di un Service Pack prima di applicare le patch per il proprio sistema operativo. Sempre più spesso accade, infatti, che virus e programmi "maligni" diffusi in particolar modo attraverso Internet, sfruttino le vulnerabilità per far danni.

Se si è provveduto ad installare la relativa patch, il virus o il programma "maligno" non potrà sfruttare la vulnerabilità del sistema ed entrarvi. In caso contrario il nostro disco fisso verrà inesorabilmente infettato.

Un esempio? Provate ad inserire nella barra degli indirizzi del browser: www.solutions.fi/iebug2/run.cgi

Si tratta di un test, totalmente innocuo, sviluppato da Solutions.fi (www.solutions.fi/in-

LE PATCH PER INTERNET EXPLORER

Gran parte delle vulnerabilità sfruttate da virus, programmi "maligni" e pirati informatici, riguardano il sistema operativo e, sempre più di frequente, i software che utilizziamo per comunicare in Rete (ad esempio il client di posta elettronica ed il browser Internet).

Per prima cosa verificate la versione di Internet Explorer da voi utilizzata: cliccate sul menù *?* quindi sulla voce *Informazioni su Internet Explorer*. All'interno di questa finestra troverete la versione di Internet Explorer installata ed, in corrispondenza della dizione *Versioni di aggiornamento*, la lista delle patch e dei Service Pack applicati.

Se fate uso di Internet Explorer 5.01 o versioni precedenti, vi consigliamo di passare a Internet Explorer 6.0, applicare le patch che vi suggeriamo noi e quelle indicate da parte di Windows Update e/o HFNetChk. È infatti ormai sconsigliato pensare di aggiornare la versione 5.01 e precedenti: le patch da applicare sarebbero moltissime e ormai si tratta di browser superati.

Se utilizzate, invece, Internet Explorer 5.5 e non vi va di passare, ancora, a Internet Explorer 6.0, sappiate comunque che è di vitale importanza effettuare un aggiornamento sia del browser Internet che del client di posta elettronica Outlook Express. Per prima cosa installate il Service Pack 2, un pacchetto "pesante" che contiene tutte le patch rilasciate da parte di Microsoft per risolvere problemi e bug presenti all'interno del browser. Il Service Pack 2 in lingua italiana per Internet Explorer 5.5 è scaricabile direttamente da qui:
http://download.microsoft.com/download/ie55sp2/Install/5.5_sp2/W98NT42KMe/IT/ie5setup.exe
Si tratta di un file eseguibile di circa 500 KB che, una volta lanciato sul proprio sistema, permette di prelevare dai server Microsoft solo gli aggiornamenti adatti alla configurazione software del proprio sistema. In questo modo si evita di dover scaricare dati superflui per il corretto aggiornamento del sistema.
Ad installazione conclusa eseguite Windows Update per installare le ultime patch.
Tra le ultime patch rilasciate, destinate quindi anche agli utenti di Internet Explorer 6.0, ve ne sono tre di cui due "cumulative" poiché includono la raccolta di tutte quelle rilasciate in precedenza. Ricordate comunque che, per applicarle, dovete disporre di Internet Explorer 5.5 con Service Pack 2 oppure di Internet Explorer 6.0.
Ecco la lista di tali patch:
www.microsoft.com/windows/ie/downloads/critical/Q313675/default.asp
www.microsoft.com/windows/ie/downloads/critical/q316059/default.asp
www.microsoft.com/windows/ie/downloads/critical/q318089/default.asp
Dopo l'installazione delle patch noterete che all'interno del menù *?/Informazioni su Internet Explorer*, troverete i riferimenti ad esse in corrispondenza della voce *Versioni di aggiornamento*.

dex.cgi/?lang=eng), un'azienda finlandese, esperta in problemi legati alla sicurezza dei sistemi operativi.

Se il vostro sistema è vulnerabile il programma verrà scaricato ed eseguito (vi compariranno alcune righe in finestra MS DOS): se si fosse trattato di un virus o di un programma maligno il vostro computer sarebbe stato irrimediabilmente infettato; qualora il vostro Windows non sia affetto da questo problema vi verrà semplicemente richiesto di scaricare un file: premendo il pulsante *Annulla* annullerete l'operazione (in ogni caso il programma non verrà automaticamente eseguito). I due programmi che vi presentiamo nelle prossime pagine vi permetteranno di tenere il vostro personal computer sempre aggiornato ed immune dai pericoli della Rete.

Altri sgraditi "ospiti"

Ogni volta che ci si collega con un sito Internet, il browser preleva automaticamente tutti gli elementi che compongono le pagine visualizzate e li salva in una cartella temporanea denominata cache. Il quantitativo di spazio occupato su disco viene giustificato dalla maggiore velocità di caricamento dei siti ai quali si accede frequentemente.

Molti di questi file, anche se vengono utilizzati una sola volta, tendono ad accumularsi sul proprio disco fisso occupando spazio prezioso.

In Internet Explorer selezionate dal menù *Strumenti* la voce *Opzioni Internet*, fate clic sul pulsante *Elimina file*, attivate la casella *Elimina tutto il contenuto non in linea* infine premete il pulsante OK: in questo modo eliminerete tutti i file temporanei (cache) creati in precedenza.

Cookie: quando accettarli, come rifiutarli ed eliminarli

Oltre alla cache, il browser Internet memorizza, sul disco fisso, anche i cosiddetti *cookie*. Si tratta di piccoli file testuali che vengono inviati dal server Web al browser che li memorizza nel computer locale, per poi restituirli al server ogni volta che l'utente torna a visitare il sito. I cookie possono svolgere quindi operazioni utili, senza alcun intento di danneggiare dati o violare la nostra privacy. I siti Internet che li sfruttano, ne fanno uso, solitamente, oltre che per controllare quante volte uno stesso utente accede al sito Web, anche per memorizzare informazioni che possano rendere migliore la navigazione di una persona all'interno di uno stesso sito. Non solo, alcuni cookie si spingono oltre e possono richiedere *username* e *password* per la verifica dell'autenticità dell'utente. Anche in questo caso i cookie non dovrebbero essere eliminati.

Il problema sorge quando il server che fornisce i cookie li utilizza per seguire gli spostamenti degli utenti da un sito all'altro oppure per scoprirne l'identità: in questo caso è violata la privacy.

Per evitare problemi sarebbe opportuno accettare cookie solo dai siti Internet "fidati" evitando di scaricare quelli provenienti da siti di dubbio contenuto oppure quelli sfruttati da aziende pubblicitarie che, in modo poco rispettoso, utilizzano i cookie per visualizzare banner pubblicitari ad hoc, sempre diversi, oppure noiose finestre pop-up. Purtroppo non sempre l'utente è consapevole di quanto sta accadendo al suo computer. Un modo semplice per decidere quale livello di protezione applicare alla propria navigazione è fornito dai normali browser.

Internet Explorer 6.0, ad esempio, fornisce sei livelli crescenti di filtro: si parte da un basso livello di protezione che applica solo restrizioni a cookie inviati da terze parti e all'invio di dati personali senza il consenso esplicito dell'utente fino al livello più alto che blocca tutti i cookie, passando ovviamente per tutti i livelli intermedi. In più, il pulsante *Elimina cookie* di Internet Explorer (contenuto anch'esso in *Strumenti, Opzioni, Internet, Generale*), permette di cancellare gran parte dei cookie, anche se alcune tracce non vengono eliminate: rimane, per esempio, il file *index.dat*, contenente informazioni sui siti visitati e che può assumere, con il passare del tempo, dimensioni molto elevate (ben più dei 32 KB standard).

Tale file non si può eliminare perché è bloccato da parte del sistema operativo. Essendo apribile con un normale editor di testo, *index.dat* può rappresentare una minaccia per la nostra privacy perché permette di ottenere informazioni su alcuni siti Web da noi visitati, rendendo così possibile carpire informazioni sulle nostre preferenze.

Per sbarazzarsi del file *index.dat* e di tutti i cookie vi consigliamo il programma gratuito Empty Temp Folders (vedi pag. 54). Per scegliere, di volta in volta, quali cookie ricevere e quali rifiutare, è meglio CookieCop (vedi pag 55). Entrambi i programmi sono contenuti nel CD ROM allegato a questo numero di *PC Open*. n

Michele Nasi

I SITI INTERNET PER EFFETTUARE TEST E MANTENERSI INFORMATI

In Rete sono disponibili una serie di test, gratuiti e totalmente innocui, che permettono di evidenziare bug e falle di sicurezza all'interno del browser Internet utilizzato.

Personal Security Advisor

(www.microsoft.com/TechNet/MPSA/start.asp)

Il primo tool, basato sul Web, che consigliamo si chiama Personal Security Advisor ed è stato realizzato e messo a disposizione direttamente da Microsoft.

Personal Security Advisor può essere eseguito, tuttavia, solo su personal computer su cui sia installato Windows NT, Windows 2000 oppure Windows XP. Questo sistema di controllo, attivabile cliccando sul pulsante Scan Now, permette di scaricare sul proprio sistema alcuni moduli di appoggio e di avviare una scansione del proprio sistema alla ricerca di Service Pack, hot fix e patch mancanti.

Al termine dell'ispezione, Personal Security Advisor mostrerà, per prima, la lista di tutti quegli aggiornamenti che è vivamente consigliato installare da subito (indicati come ad "alto rischio").

George Guninski (www.guninski.com)

Il sito di George Guninski, un famoso "cacciatore di bug" che ha scoperto e messo a nudo numerosi bug riguardanti i principali browser Internet, Windows 2000 ed altri pacchetti software, raccoglie una vasta schiera di *"exploit"* ossia una serie di piccoli programmi che consentono di mostrare quali azioni può intraprendere un hacker su un personal computer sul quale siano in esecuzione software vulnerabili (quindi non correttamente "patchati"). Tutti gli "exploit" presenti sul sito di Guninski sono, ovviamente, del tutto innocui ed aiutano a sensibilizzare l'utente sul problema sicurezza.

LockDown Online Security Tests

(http://stealthtests.lockdowncorp.com)

Per tutti coloro che conoscono la lingua inglese e che vogliono approfondire le tematiche legate al problema della sicurezza in Rete suggeriamo il sito LockDown Online Security Test che offre un'ampia gamma di test atti a verificare il proprio effettivo livello di sicurezza in Rete. Sono disponibili anche una serie di consigli per rendere il proprio personal computer veramente "invisibile" durante la connessione. LockDown propone servizi e programmi gratuiti per verificare quali informazioni vengono trasmesse durante la navigazione e suggerimenti per rendere il personal computer immune da attacchi esterni.

I siti Internet informativi

Microsoft TechNet (www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp)

Il primo sito, fonte d'informazione per tutti coloro che vogliono tenersi aggiornati in merito alla sicurezza, è certamente Microsoft Technet: nelle sue pagine si trovano analisi e metodologie per risolvere tutti gli ultimi bug resi noti, molto tempo prima che le relative patch siano disponibili.

BugTraq (http://online.securityfocus.com/archive/1)

BugTraq è un sito Internet che da anni tratta il tema della sicurezza informatica. Nell'archivio che vi segnaliamo, aggiornato a cadenza giornaliera, troverete informazioni dettagliate su qualsiasi genere di vulnerabilità, bug o falla di sicurezza relativi a qualsiasi sistema operativo e a qualunque software.