"Prevenire è meglio che curare..."

... anche col PC! Consigli pratici.

Il tema della mia rubrica mensile questa volta è dedicato al mondo delle “infezioni informatiche” e, in particolare, alla distinzione fra i vari tipi di “virus informatici”.

Quante volte è capitato, a chi usa quotidianamente il PC, di imbattersi in fastidiosi programmi eseguibili che minano il corretto funzionamento del calcolatore o di sentir dire: “Ho beccato Marburg (noto virus informatico che disegna delle croci sullo schermo)! Puoi aiutarmi? Hai un buon antivirus?”. Bene, da questa breve premessa si evince che il problema è all’ordine del giorno non solo per i piccoli utenti di Internet, ma anche e soprattutto per la grande utenza del mondo aziendale che cura molto la sicurezza informatica e la protezione dei propri dati, onde evitare la paralisi dei propri server con conseguente danno economico non indifferente.

Una indagine di mercato ha calcolato che, negli ultimi 10 anni, i virus hanno provocato danni per circa 60 miliardi di euro. Ad essere soggetti al rischio di “infezione” sono tutti quei dispositivi (PC privati, telefonini, palmari) che, funzionanti attraverso un sistema operativo, fanno uso della rete Internet per le varie necessità (posta elettronica, aggiornamenti on line, visita di pagine web e quant’altro). Molti esperti del settore “sicurezza in rete” stimano che nel mondo ci siano oltre 300.000 programmi dannosi, cui vanno aggiunte le circa 250 varianti al giorno.

Pertanto, ad esempio, si assiste al tentativo di rubare soldi agli utenti creduloni o poco attenti attraverso virus nuovi sempre più sofisticati o tramite il re-indirizzamento verso pagine web costruite ad arte per captare password di accesso o numeri di carta di credito, e fin qui i danni si limitano, nella maggioranza dei casi, a poche centinaia di euro.

Le conseguenze diventano più pesanti invece nel caso dello “spionaggio” dei dati delle grandi aziende o dei dati di accesso al banking on line (conti bancari che vengono acceduti in rete); si calcola che, nel 2005, le truffe informatiche hanno portato circa 1 miliardo di euro nei conti dei criminali.

Classificazione dei virus informatici.

Ciò premesso, occorre innanzitutto precisare che i vari tipi di virus si differenziano principalmente per il “metodo di propagazione” e si possono così classificare:

VIRUS
Sono i programmi dannosi più vecchi e si diffondono solo all’interno del software di un PC, ossia, causano infezione in altri PC solo attraverso l’intervento incauto dell’utente, che invia un file infetto.

WORM
Sono i successori dei virus, dal momento che sono più diffusi e dannosi e si trasmettono ad altri PC attraverso modalità autonome quali la connessione in rete fra PC e la posta elettronica.

TROJAN
Sono dei programmi utility dannosi, scaricati ingenuamente da Internet sul PC dell’utente in quanto viene creduto essere un software gratuito molto performante, trattandosi invece di software applicativi che hanno il solo scopo di occupare la memoria centrale.

SPYWARE
Sono dei programmi veicolati sul PC attraverso i trojan. La loro peculiarità è quella di raccogliere e spedire dati sensibili dei quali altri possono servirsi per spedire pubblicità (in base ai siti web visitati) o, peggio, per fare acquisti folli col numero di carta di credito intercettato.

DIALER
Sono dei programmi che modificano i dati di accesso ad Internet per costringere ad usare numeri di telefono con tariffa costosissima che effettuano delle chiamate internazionali.

PHISHING
Sono dei programmi non proprio dannosi, ma pur sempre pericolosi, in quanto con essi ci si illude di ricevere un messaggio da un mittente come la propria banca, ad esempio, e questo messaggio induce l'utente a visitare un sito web uguale a quello originale, ma falso, in cui viene richiesto di inserire le proprie credenziali bancarie, con la conseguente fregatura che il conto bancario sarà oggetto in futuro dell'avidità e delle attenzioni altrui.

BACKDOOR
Sono dei programmi che permettono l'accesso diretto ed il controllo del proprio PC da parte del criminale informatico. Si tratta di un sistema molto cinico attraverso cui un utente ingenuo diventa mittente involontario di messaggi pubblicitari.

HOAX
Sono dei messaggi falsi che inducono l'utente ad installare da Internet un infallibile pseudo-antivirus che, in realtà, non è altro che un programma infetto che contiene uno dei virus elencati nel messaggio.

In che modo si prende il virus.
Il virus entra in azione nel momento in cui gli si permette di arrivare ai dati contenuti sul proprio PC. Ciò può avvenire tramite i comuni CD-Rom o supporti esterni, tramite la connessione ad Internet (in particolare, su siti non istituzionali poco raccomandati) o alla rete aziendale costituita da diversi PC, oppure tramite i file allegati della posta elettronica.

Possibili danni causati dai virus.
In genere, i virus sono dei semplici trucchi fastidiosi ed abbastanza pericolosi, che causano, ad esempio, messaggi di errore poco usuali che non modificano i dati sul PC. Tuttavia, i virus più pericolosi attaccano i dati distruggendoli o modificandoli attraverso la formattazione del disco fisso. Ci sono virus che addirittura vanno a sovraccaricare la scheda video del PC danneggiandola o che vanno a sovrascrivere i programmi che controllano l'avvio ed il funzionamento del sistema operativo.

Riconoscere un PC o un file infetto.
Occorre necessariamente servirsi di un programma antivirus. In ogni caso, anche un malfunzionamento temporaneo del PC (file che non si aprono, avvio del PC più lento del solito, improvviso ed intenso scambio di dati attraverso Internet) è indice della possibile presenza di una infezione informatica.

Una buona protezione del PC.
Il principio che deve ispirare l'utente diligente ed attento all'uso del PC è che in rete non si è mai sicuri né "invulnerabili", ma occorre stare allerta e soprattutto essere consapevoli di ciò che si sta facendo, adottando la buona abitudine di frequentare solo dei siti web istituzionali (quotidiani, istituzioni governative, siti aziendali) e non i soliti siti dove si garantisce che "tutto è gratis", perché

dietro questa affermazione si cela l'intenzione di permettere il download di qualche utilità a fronte di un pegno, ovvero la conoscenza dei dati sensibili.

Per concludere, le indicazioni che seguono sono delle semplici misure di sicurezza che tuttavia costituiscono una sorta di obbligo per l'utente informatico:

1) **aggiornare il sistema operativo e tutte le applicazioni che si usano quotidianamente**, scaricando i relativi aggiornamenti solo dai siti web ufficiali, in modo da ovviare ai problemi che si presentano improvvisamente;

2) **adottare quello che io definisco il "trio delle meraviglie"**:

- il **firewall** (controlla l'invio e la ricezione dei dati da Internet da parte dei programmi installati sul PC. Attraverso un elenco modificabile dall'utente, consente di riconoscere se un programma ha il permesso o meno di inviare/ricevere dati da Internet e dà l'allarme se si tratta di un programma non noto: in questo caso, è l'utente che decide se dare o meno l'autorizzazione al trasferimento dei dati);

- l'**antivirus** (controlla i file del PC scaricati più recentemente da Internet o che entrano sul disco fisso, ricercando eventuali virus. Se viene scoperto un virus, l'antivirus impedisce l'accesso al file in modo da non avviare l'esecuzione del virus e cerca di cancellarlo o metterlo in una particolare directory [quarantena], cosa che non sempre riesce efficacemente);

- l'**antispyware** (ha un comportamento pressoché uguale all'antivirus, tranne per il fatto che controlla solo gli spyware).

Componenti da installare per una buona protezione del PC.

firewall consigliato: **ZONE ALARM** (facilmente reperibile in rete o sui CD-Rom abbinati alla vendita di riviste di informatica);

antivirus consigliato: **NOD32** (acquistabile on line e votato sul web come uno dei migliori);

antispyware consigliato: **SPYBOT - SEARCH & DESTROY** (facilmente reperibile in rete o sui CD-Rom abbinati alla vendita di riviste di informatica).

Ing. Rizzo Giuseppe