SICUREZZA INFORMATICA - *1a parte*

Introduzione

Questi appunti non hanno la pretesa irrealistica di rendere invulnerabili le difese di un computer, però dà alcune indicazioni per difendersi dalla maggior parte di programmi ostili, anche perché la stragrande maggioranza degli attacchi non è mirata a privati occasionali senza interessi specifici.

Ogni volta che c'è un attacco di un virus, milioni di utenti vengono infettati, altri invece non subiscono danni in quanto hanno installato nei loro computer efficaci programmi di difesa.
Sia ben chiaro, però, che c'è ben poco che possa fermare un intruso molto deciso che voglia specificatamente entrare in un computer. In questi casi, per difendersi ci vuole un esperto di sicurezza informatica che esamini il caso specifico.
Grazie a virus come Blaster e Sasser, per infettare un computer con S.O. Windows, è sufficiente collegarlo a Internet, non occorre visitare siti o scaricare messaggi di posta.
La convinzione è che avere un buon antivirus sia sufficiente, niente di più errato, in quanto chi ha intenzione di entrare in un computer di terzi non ha bisogno di infettarlo con virus per agire, ma può approfittare di un difetto del programma operativo o di Internet Explorer.
La buona sicurezza informatica, come qualsiasi altra forma di sicurezza, non si basa mai su una singola soluzione, ma su una serie di barriere, configurate in modo che se ne cede una ne restano da superare altre. Limitarsi all'antivirus è fare cattiva sicurezza informatica.

Prima di iniziare a prendere in esame gli interventi necessari per diminuire il pericolo di un attacco informatico, vengono date alcune indicazioni di carattere generale RICORDANDO CHE E' FONDAMENTALE INNANZITUTTO PREVENIRE l'ingresso di programmi infetti.

Alcune regole da seguire

1 – Installare un buon **Firewall**.

2 – Installare un buon **Antivirus** e tenerlo costantemente aggiornato e usarlo su tutti i file che arrivano a mezzo posta o scaricati da Internet.

3 – Fare frequentemente il **Backup** dei documenti personali.

4 – Mantenere aggiornato il **S. O**. (Sistema Operativo)

5 – Non installare **Programmi** sconosciuti o di dubbia provenienza.

6 – Non aprire gli **Allegati** di qualsiasi tipo inviati da sconosciuti; anche gli allegati ricevuti da conoscenti non vanno mai aperti immediatamente, ma vanno prima sottoposti ad un controllo con l'antivirus.

7 – Non fidarsi di **link** di Banche o negozi che sono stati forniti da sconosciuti a mezzo e-mail. Possono essere falsi e indirizzare a un sito truffa.

8 – Configurate la posta per la lettura dei messaggi in **testo normale.**

9 – Non inviare a persone poco affidabili documenti prodotti in **Word**. Tali documenti nascondono dati personali.

10 – Non fidarsi di messaggi che invitano a **cancellare** Files indicati come pericolosi.

11 –Installare sempre gli aggiornamenti gratuiti di **Windows** che Microsoft propone periodicamente per correggere errori del S.O. che possono pregiudicare la sicurezza.

Interventi da effettuare su Windows

Aprire **Esplora risorse**, quindi ***Strumenti ☞ Opzioni cartella*** e nella finestra di dialogo aperta, scegliere l'etichetta **Visualizzazioni**.

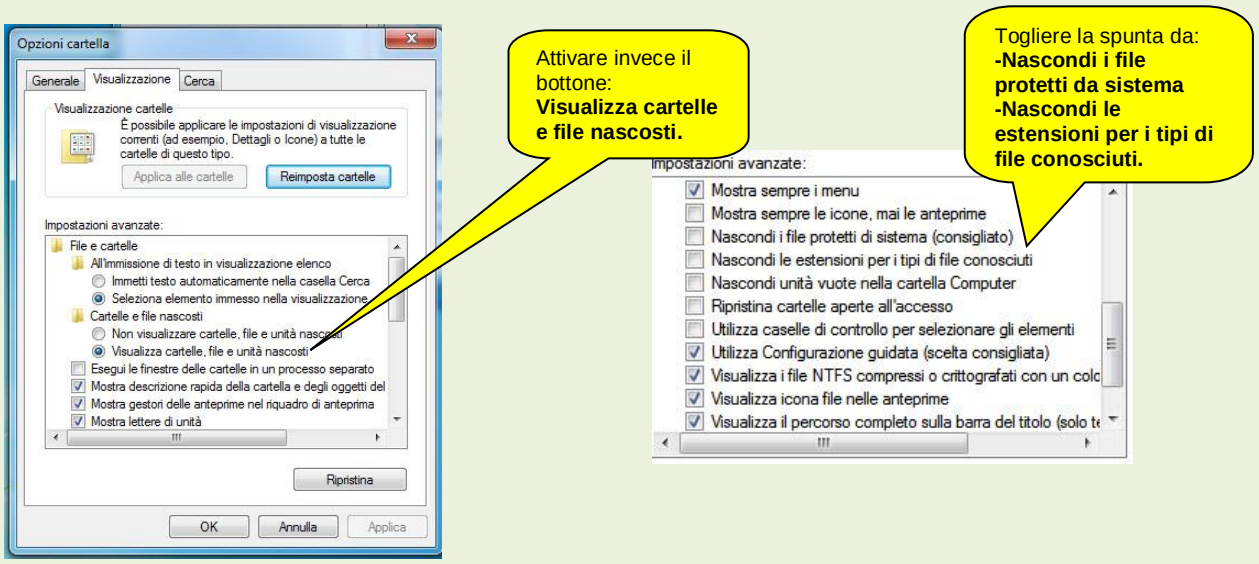

FIG. 1 FIG. 2

Cliccare poi sul pulsante **Applica a tutte le cartelle**, rispondere **Si** infine dare **OK**.

Sempre in **Esplora risorse**, scegliere ***Visualizza ☞ Barra di stato***: questo fa comparire, lungo il bordo inferiore della finestra di Esplora risorse, una barra che contiene informazioni utili, come lo spazio disponibile su disco e lo spazio occupato da ciascuna cartella o raggruppamento di files.

Inoltre, per aumentare la compattezza e completezza delle informazioni presentate da Esplora risorse, scegliere la ***Visualizza ☞ Dettagli***. Questa impostazione ha il vantaggio di mostrare subito la data di modifica di ciascun file, mentre nella visualizzazione standard la data di modifica viene visualizzata soltanto posizionando il mouse sopra il file che interessa. Dopo questi interventi, scegliere: ***Strumenti ☞ Opzioni cartella***, etichetta **Visualizzazioni** poi cliccare sul pulsante **Applica a tutte le cartelle.**

C'è un'ottima ragione di far emergere quanto nascosto senza ragione da Microsoft, infatti gli aggressori, in alcuni casi, sfruttano l'invisibilità di file ed estensioni nascoste utilizzano il metodo detto dei "***file travestiti***".

Nessuna estensione può considerarsi sicura, ma certamente le estensioni di file eseguibili, indicati di seguito, sono certamente quelle a più alto rischio.

Elenco delle principali estensioni pericolose:
.bat, .chm, .cmd, .com, .cpl, .dll, .exe, .hlp, .hta, .inf, .lnk, .ocx, .pif, .reg, .scr, url, .vbs

Esempio di attacco ostile con file travestito.
Ricevendo un allegato con un'estensione uguale ad una di quelle indicate nell'elenco precedente, si deve avere la massima precauzione prima di fare un doppio click per aprirlo!!
Mantenendo le configurazioni predeterminate, non si possono vedere le estensioni dei files conosciuti; per cui, ricevendo ad esempio un allegato denominato **Panorama.jpg.exe**, si vedrebbe come **Panorama.jpg** (*l'estensione .exe viene nascosta*) con un'estensione (.jpg) non a rischio; pertanto dando doppio clic anziché vedere "un panorama", si eseguirà il files con l'estensione **.exe** infettando il computer.

Disattivazione Assistenza remota

Altro punto debole predefinito è l'attivazione della possibilità dell'***Assistenza remota,*** porta da cui possono entrare attacchi ostili o bachi. Per disattivare tale proprietà di Windows 7, fare click su ***Start ☞Pannello di controllo ☞ Sistema e Sicurezza ☞Sistema ☞ Consenti accesso remoto*** Per aprire la finestra di dialogo di figura 4.

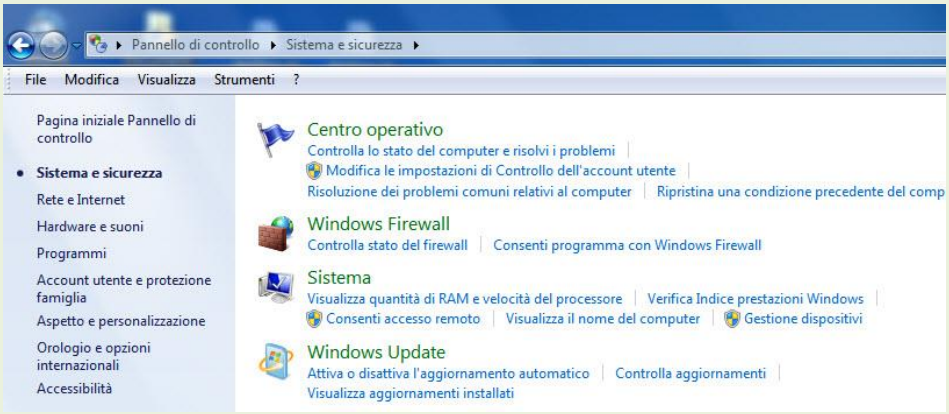

FIG. 3

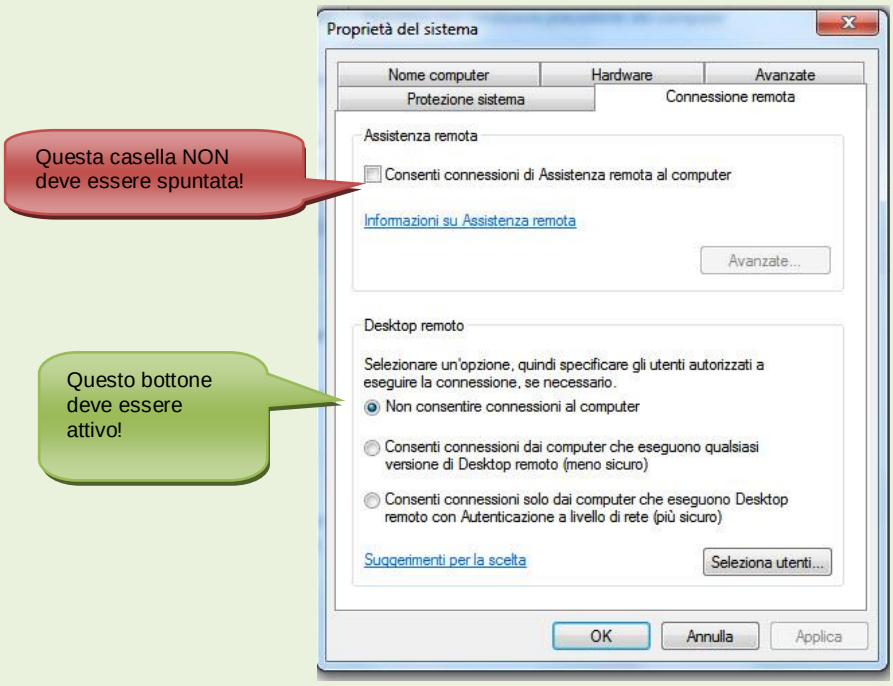

FIG. 4

SICUREZZA INFORMATICA - *2a parte*

Altre configurazioni per la protezione.

Aprire Internet Explorer scegliere nella barra dei menù ***Strumenti*** ☞ ***Opzioni internet*** poi etichetta **Sicurezza.**
Selezionare l'icona **Internet,** Figura 5, quindi fare scorrere il cursore del livello di sicurezza verso l'alto per aumentarla o verso il basso per diminuirla.
E' anche possibile personalizzare il livello di sicurezza, operazione che comunque deve essere eseguita da utenti molto preparati.
Più è alto il livello di sicurezza, maggiori sono le difficoltà di navigazione, pertanto si può variare la sicurezza di volta in volta, in funzione dei siti che si visitano.

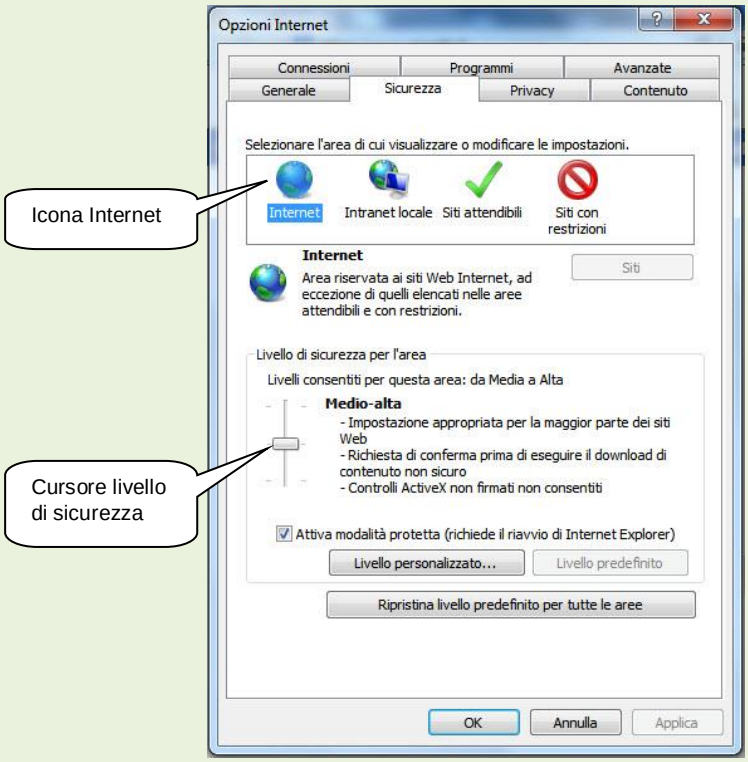

FIG. 5

Riconoscere i sintomi di un attacco

Ecco alcuni sintomi tipici di un attacco da virus informatico o da un tentativo di intrusione, anche se a causa della nota instabilità di Windows, la presenza delle suddette indicazioni non garantisce che si tratti di un'infezione, ma è comunque opportuno in questi casi effettuare approfondite verifiche.

- **Riavvio spontaneo**
- **Antivirus che si disattiva senza intervento dell'operatore**
- **Programmi che erano perfettamente funzionanti che improvvisamente si bloccano**
- **Computer diventato inaspettatamente lentissimo**
- **Internet molto lenta**
- **Spazio su disco che diminuisce senza aver prodotto documenti o avere installato programmi**

Strumenti di protezione

Gli strumenti di protezione che saranno presi in esame, sono **indispensabili** per navigare e utilizzare il programma di posta con un minimo di sicurezza.
Sono: ***Firewall, Antivirus, Spyware***.

Firewall

Un Firewall può essere Software o Hardware; in questa sede si prende in esame il Firewall software.
La funzione di questo programma è quella di controllare e bloccare tutte le visite indesiderate o presunte tali, e di evitare che informazioni non autorizzate partano dal computer verso l'esterno.
Normalmente sono programmi ad istruzione manuale, cioè quando presenta un blocco, richiede la nostra autorizzazione e in funzione della risposta data si auto istruisce.
Per chi non ha mai installato un Firewall, il primo impatto è sicuramente traumatico e la tentazione è quella di disinstallarlo o di modificarne la configurazione perché il numero di tentativi di ingresso e di uscita sono talmente numerosi che diventano un fastidio e un'apparente perdita di tempo.
Al contrario invece questa esperienza dovrebbe far valutare in modo positivo l'attività di questo programma.
Windows 7, contrariamente a XP, ha un buon Firewall.
Un ottimo programma ***gratuito*** per uso personale, è **ZoneAlarm** scaricabile su: http://www.zonealarm.com Versione localizzata anche in italiano.
Oppure **Comodo Firewall** scaricabile su http://personalfirewall.comodo.com/

Antivirus

I virus sono al minaccia più frequente e dannosa per la normale impostazione di Windows.
Un virus può causare danni di ogni sorta: può cancellare i files dei nostri documenti, alterarne il contenuto, paralizzare il computer, spiarne l'attività ecc..
Un virus si propaga in tanti modi. I più frequenti sono:

- *La navigazione in Siti di dubbia fama.*
- *Per mezzo di un allegato ad un' e-mail.* (non fidarsi troppo di mittenti di un messaggio contenente allegati).
- *Dischetti o cd di incerta provenienza* (anche se apparentemente vuoti)

Come funziona un antivirus – Un antivirus è un programma che ha al suo interno un database di tutte le stringhe relativa a virus conosciuti, e per mezzo di una scansione sul file sottoposto a controllo, verifica la presenza di tali stringhe. ***Da quanto suddetto, risulta evidente che un programma Antivirus deve essere costantemente aggiornato e attivo durante tutta l'attività del computer.***
Un antivirus ha un costo, ma accanto ai programmi commerciali a pagamento (**Norton, Mc Afee** ecc..), esistono buoni antivirus gratuiti per uso personale.

Avast Home Edition - *gratuito*. Scaricabile sul sito: http://www.avast.com localizzato anche in italiano. E' un buon antivirus per uso privato. Richiede solo una registrazione sul sito del produttore, la registrazione è libera e permette di ricevere via e-mail il codice di attivazione. Questo permette di avere gratuitamente per un anno l'aggiornamento delle definizioni dei virus. Scaduto l'anno si deve riregistrarsi. E' possibile collegarsi e scaricare gli aggiornamenti del programma.

AVG Antivirus Free Edition - *gratuito*. Scaricabile dal sito: http://www.avg.com/IT
Gratuito solo per uso privato, ben realizzato può contare su aggiornamenti per due anni.
Localizzato in lingua italiana.

Avira antivirus free – gratuito è sicuramente tra i migliori, manca però il controllo della posta.
Localizzato in lingua italiana. http://www.avira.com/it/avira-free.antivirus

Configurazione dell'antivirus – normalmente a seguito dell'installazione il programma Antivirus ha già una configurazione predefinita ottimale. Se si ritiene di modificarla, è opportuno aumentare le restrizioni, **MAI DIMINUIRLE !!**

Spyware e Adware

Gli Spyware sono programmi che una volta insediatisi in un computer, lo spiano ed inviano all'incursore le informazioni raccolte relative all'attività di quell'elaboratore.
Anche se non ha la furia devastante dei normali virus, non sono meno insidiosi e pericolosi.
Si provi ad immaginare l'attività criminale di uno Spyware in un computer di una Banca!
Gli Adware sono applicazioni specificatamente programmate per infestare di pubblicità non richiesta i computer.
Per difendersi da attacchi dagli Spyware e da Adware, oltre a programmi professionali di costo, esistono efficaci programmi gratuiti.

Ad-Aware SE personal Edition - *gratuito*. Scaricabile dal Sito: http://it.lavasoft.com
E' uno dei migliori Antispyware gratuiti. Offre solo funzioni di rilevazione standard, ma si dimostra efficace nei blocchi delle modifiche a HOMEPAGE/PAGINE di ricerca ed è apprezzabile anche per la rimozione dei servizi di Windows aggiunti dagli Spyware. Quindi è una valida alternativa per rimuovere Spyware, Adware, monitor di sistema, cookie di rilevamento. Localizzato in italiano.

SpybotSearch&Destroy - *gratuito*. Scaricabile sul Sito: http://www.safer-networking.org/it/dl/
Buon programma di difesa si apprezza soprattutto per la capacità di impedire la sovrascrittura del file **hosts**, individua le modifiche tentate alla *Home page* e ha la capacità di rimuovere programmi *Bho* e toolbar. Localizzato in italiano.

SpywareBlaster - *gratuito* Scaricabile dal Sito:
http://www.filehippo.com/it/download_spywareblaster/
Buon programma efficace in particolare su Spyware di origine Blaster. Localizzato italiano.

08 – Ultime raccomandazioni

- **I programmi di difesa installati, vanno mantenuti costantemente aggiornati.**
- **Non partecipare e non inoltrare "catene di S. Antonio".**
- **Non fidarsi di offerte apparentemente vantaggiose. L'avidità a volte si paga cara!**
- **Meglio utilizzare carte di credito prepagate per fare acquisti on-line.**
- **Non dare vostri dati sensibili a siti che lo richiedono a meno che non abbiano una reputazione cristallina.**
- **Usare molta prudenza con gli allegati a messaggi.**
- **Mai, mai, mai dare in una e-mail numeri di carte di credito, di conto corrente e di password. Se viene fatta una richiesta del genere è certamente di un truffatore.**
- **Eventuali file contenenti dati sensibili (numeri c/c, codici, password ecc…) vanno crittografati.**