Guida contro virus Computer

Serie di primi accorgimenti informali per migliorare la protezione del pc.

Link Guida: simonesudati.com/GuidaVirus

***Introduzione*—I virus sono dei programmi. Sono software informatico composto da righe di codice di istruzioni. Solitamente sono dei file di formato .exe eseguibili. Altri formati presenti sul pc quali ad esempio formati multimediali NON possono essere virus. Essendo programmi sono quindi eseguiti dal processore del computer, spesso in background. Dei primi segnali di presenza di virus sono: rallentamenti del pc e della connessione internet immotivati, l'antivirus inspiegatamente disattivato (non si disattiva un antivirus per errore, sono richiesti più passaggi), malfunzionamenti di periferiche quali webcam/casse/dispositivi bluetooth, apertura di pagine web senza averne fatto richiesta. Se si sospetta la presenza di un virus come prima cosa occorre disattivare immediatamente internet sia wifi che ethernet. Spegnere il pc e portarlo da uno specialista. Fondamentali sono i backup perchè potrebbe essere necessaria una formattazione che consiste in una cancellazione totale dei file sul computer.**

I. Email

La maggior parte dei virus provengono da email o da messaggi. Molte di esse vengono riconosciute dai filtri anti-spam presenti nei gestori email ma alcune riescono a passare il filtro. Un primo modo è tramite click su link presenti nell'email che si "spacciano" per premi, sconti ecc. e che rimandano a pagine malevole. Un secondo modo è tramite i media (immagini,file,audio) presenti nell'email provenienti da utenti sconosciuti o anche da email insolite provenienti da persone conosciute. Esse sono all'apparenza dei media ma in maniera nascosta installano virus. Un terzo modo che è il più pericoloso è ricevendo un'email da banche o istituzioni, che dopo aver cliccato sul link, richiedono le credenziali di accesso per le più svariate motivazioni. MAI farlo! Si tratta di una riproduzione dell'interfaccia della banca/istituzione fatta per rubare le credenziali. Gli hacker emettono queste email in quantità ingente non sapendo nemmeno se fai parte della banca/istituzione stessa. Procedere subito a bloccare il mittente (il suo indirizzo email).

Consigli:

- Creare un'email apposita per la gestione dell'account bancario, essa non deve essere mai usata se non per necessità particolari.
- NON cliccare su link provenienti da email di dubbia provenienza.
- MAI inserire le proprie credenziali su link di rimando da email anche se sono di banche o enti conosciuti e con interfacce grafiche famigliari.
- I virus si possono nascondersi nei media scaricati per email. Da preferirsi gestori email come Thunderbird che, ricevuta un'email, non ne scarica i media ma richiede all'utente se desidera scaricarli o meno.
- Per le aziende è fondamentale la VPN.
- Autenticazione a due fattori per gli account importanti.
- Cambiare la Password una volta al mese se è un account importante.

II. Navigazione su browser

Durante la navigazione su internet si può prendere un virus scaricando un file, cliccando anche non volontariamente su pubblicità o popup (finestre o riquadri che compaiono automaticamente). Vedi sezione B) e C) per aumentare la sicurezza durante la navigazione su browser.

Consigli:

- Usare sempre navigazione sicura in protocollo Https. Mai siti in Http che il solo protocollo è già un primo allarme. Preferire inoltre la navigazione in incognito.
- Quando si è dubbiosi su un link, andandoci su con il cursore del mouse si visualizza in basso a sinistra della pagina l'url a cui si verrà indirizzati in caso di click.
- Preferire browser come Firefox che è uno dei più sicuri perchè raccoglie meno dati rispetto ai prodotti Google e Microsoft.
- Scaricare file da enti certificati, evitare i torrent.
- Se vuoi registrarti su un sito ma non sai se è sicuro, registrati con un'email temporanea non tua creata su temp-mail.org/it

A. Come individuare un virus su Windows

Primo metodo:

1) Aprire il command prompt (terminale) in modalità amministratore.
2) Lanciare il comando "netstat -b"
3) In output verranno visualizzate le connessioni aperte esterne del nostro computer. Da analizzare sono quelle segnate in ESTABLISHED.
4) Aprire il task manager (Gestione attività) e con tasto destro attivare "nomi processo".
5) Ora andare a terminare tutti i programmi in esecuzione (dal task manager) che sono connessioni aperte (sul terminale) ma non sono riconducibili a programmi conosciuti sul task manager. Andare poi a disinstallarli.
6) NB: il virus potrebbe ri-generarsi all'accensione quindi disattivare i programmi che si attivano all'accensione non conosciuti andando su "App all'avvio" e deselezionare perciò le applicazioni non conosciute o che non servono attive all'avvio. Questa procedura inoltre velocizza l'accensione del pc.

Per guida completa vedi questi due video su youtube: Come Rilevare un Virus nel Computer Windows , e Come Rimuovere un Virus da un Computer Windows.

Secondo metodo:

Molto simile al primo ma il controllo avviene attraverso il codice PID.

1) Aprire il command prompt (terminale) in modalità amministratore.
2) Lanciare il comando ”netstat -ano”
3) In output verranno visualizzate le connessioni aperte esterne del nostro computer. Da analizzare sono quelle segnate in ESTABLISHED. Ognuna è identificata da un codice PID.
4) Aprire il task manager (Gestione attività) e andare sulla sezione ”Servizi”.
5) I diversi servizi sul task manager sono contrassegnati da codice PID. Ora controllare quali sono attivi ovvero contrassegnati come ESTABLISHED sul terminale.
6) Ora andare a terminare tutti i programmi in esecuzione (dal task manager) che sono connessioni aperte (sul terminale) ma non sono riconducibili a programmi conosciuti sul task manager. Andare poi a disinstallarli.

B. STO SCARICANDO UN FILE INFETTO?

L’antivirus di per sè analizza tutti i file scaricati sul computer (vedi che rileva come infetti i file scaricati da torrent per esempio). Ma per essere proprio sicuri si può andare sul sito: virustotal.com/gui e fare upload del file appena scaricato. Verrà analizzato gratuitamente da diversi antivirus che diranno se è un potenziale virus o meno. Avendo una panoramica sulla questione è virus o no virus da parte di molti antivirus permetterà di valutare accuratamente se tenere o eliminare il file.

C. LE ESTENSIONI BROWSER

Le estensioni (o add-ons) sono componenti software gratuiti che, una volta integrate con il tuo browser, ti permettono di ampliarne le funzionalità, aggiungendo nuove caratteristiche al browser o modificando quelle esistenti. Si consiglia di tenerne attive contemporaneamente non più di 5 perchè essendo operazioni che il browser deve fare, averne troppe attive, rallenterà le ricerche sul web. Focalizziamoci sul browser più utilizzato **Google Chrome** . Installarle è facile. Basta andare su questo sito chrome.google.com/webstore/category/extensions, cercare l’estensione e cliccare su ”installa”. L’estensione sarà automaticamente installata sul browser. Si consiglia di installare:

- AdBlock: Blocca annunci, pubblicità e popup sui siti in cui stai navigando. Puoi selezionare sito per sito se tenerlo attivo o meno.
- https everywhere: Usa direttamente https in navigazione in modo da criptare la comunicazione.
- Blur : Protegge le password, i pagamenti e aumenta la privacy. Molto di più di un gestore password, tiene traccia e al sicuro di tutte le tue informazioni online.
- Mercury Reader: Disattiva pubblicità, link, popup dal sito che stai leggendo. Rimane solo il testo dell’articolo.
- Extensity: Permettere di gestire velocemente quali estensioni tenere attive e quali disattivare. Per la questione dei rallentamenti se troppe fossero attive.
- Unshorten.link: Elimina i collegamenti ipertestuali abbreviati. Quando un url è abbreviato si possono nascondere degli url di rimando dannosi. E si può cliccare su qualcosa che non si dovrebbe.

Per quanto riguarda Firefox o in generale altri Browser, cambiano i nomi delle estensioni da installare ma basta ricercarle in modo che coprano le stesse funzioni.

D. ANTIVIRUS

L’antivirus in maniera semplificata analizza i programmi che sono sequenze binarie di 0 e 1. Esso ha memoria dei virus conosciuti che sono presenti in un database online e dal quale si connette per rimanere aggiornato. In questo modo confrontando i pattern di sequenze in binario decide se un file è un virus o meno. L’antivirus da scegliere deve inficiare il minimo possibile sulle risorse del computer e rimanere aggiornato in maniera tempestiva sul database dei virus. I nuovi antivirus attuano un controllo di euristica statica e un controllo di euristica dinamica. Di solito costi maggiori di antivirus corrispondono a algoritmi più efficienti e efficaci in termini di queste due euristiche. Il sistema operativo Windows ha già un antivirus di default che è Windows Defender ed è già perfetto se non si hanno particolari esigenze lavorative/di utilizzo e non si usa il pc per operazioni economiche. Un antivirus consigliato è Malwarebytes Anti-Malware che di base è gratuito, ma ne è disponibile anche una versione a pagamento che include un sistema per il monitoraggio del sistema in tempo reale. I migliori antivirus nel 2020 sono:

1) Bitdefender
2) Kaspersky
3) Norton
4) Webroot
5) Trend Micro

La spiegazione completa su questo video youtube I migliori antivirus 2020.