Polizia di Stato

La guida per il nostro computer sicuro

Un mito da sfatare é quello che solo le aziende di una certa importanza rischino di essere attaccate. Si tende infatti a pensare che tanto maggiore sarà la notorietà della nostra azienda all'esterno e tanto maggiori saranno le **probabilità di essere attaccati**.

Questo perché susciterebbe maggiore curiosità e perché la violazione dei suoi sistemi informatici rappresenterebbe un ghiotto trofeo. **Ciò é vero solo in parte** poiché vengono messi in opera, con intensità sempre maggiore, alcuni attacchi che potremmo definire "alla cieca".

Con il termine "alla cieca" si indica che la vittima non é conosciuta a priori dall'hacker. Tali attacchi vengono portati **utilizzando specifici stumenti software** che permettono di "sondare" interi domini alla ricerca di macchine che utilizzino determinati sistemi operativi e programmi applicativi che contengano qualche bug noto.

Rilevate tali macchine avrà inizio **l'attacco vero e proprio** che potrà avere esito positivo nel caso in cui in tali programmi non siano state installate le relative "patch"(aggiornamenti).

Poiché vengono scoperti(e pubblicizzati) centinaia di bug al giorno, nessun amministratore di sistema potrà ritenere la propria macchina al sicuro senza **aggiornare i programmi installati** sulla stessa frequentemente.

L'unica cosa che potrà rendere le nostre macchine ragionevolmente sicure sarà quindi una corretta e continua applicazione di una "politica della sicurezza". Si riportano, di seguito, alcuni **consigli tecnici di base che ogni navigatore potrà utilmente applicare** e che ogni amministratore di sistema potrà comunicare ai dipendenti della propria azienda, onde farli riflettere sulle tematiche della sicurezza informatica.

Alcuni di questi consigli sono rivolti a quei dipendenti che si trovino ad utilizzare un computer portatile, contenente alcuni dati aziendali, con il quale si connettono, da casa propria, alla rete Internet. Utilizzare i firewall Utilizzare un software di tipo antivirus e aggiornarlo regolarmente Non aprire gli allegati di posta elettronica se non dopo averli esaminati con l'antivirus Non eseguire programmi se non dopo averli esaminati con l'antivirus Effettuare copie di backup Non fornire nella chat i propri dati personali Scegliere una password sicura e non comunicarla a nessuno Utilizzare software di cifratura per le comunicazioni riservate **UTILIZZARE I FIREWALL** I firewall sono degli strumenti, sia di tipo hardware che software, che permettono di vigilare sullo scambio di dati che intercorre tra il nostro pc o la nostra rete locale ed il mondo esterno. Essi sono programmabili con una serie di regole così da inibire, ad esempio, il traffico di dati proveniente dall'esterno e diretto verso alcune porte del nostro pc solitamente utilizzate per porre in essere intrusioni telematiche. Permettono inoltre la visualizzazione sul monitor dei tentativi di intrusione verificatisi, comprensive dell'indirizzo telematico utilizzato dall'autore di questi. In Rete possono essere facilmente reperiti numerosi software di tipo firewall gratuitamente. **UTILIZZARE UN SOFTWARE DI TIPO ANTIVIRUS ED AGGIORNARLO REGOLARMENTE**

Il virus informatico non é altro che un programma che ha la capacità di auto-replicarsi e, una volta scrittosi sui dischi, di effettuare una serie di operazioni sul pc ospitante più o meno dannose che vanno dalla visualizzazione sul video di un messaggio fino alla cifratura del contenuto del disco fisso rendendolo così illeggibile. Considerato che ogni giorno vengono creati nuovi virus e che, con lo sviluppo della rete Internet, questi si diffondono con eccezionale rapidità, risulta fondamentale, non solo installare sul proprio pc un buon antivirus ma anche aggiornarlo frequentemente. Infatti, un software di tipo antivirus, se non aggiornato con regolarità, ci potrebbe far correre rischi maggiori rispetto al non averlo affatto poiché ci potrebbe far sentire sicuri fino a trascurare le più elementari norme di sicurezza informatica. **NON APRIRE GLI ALLEGATI AI MESSAGGI DI POSTA**

ELETTRONICA SE NON DOPO AVERLI ESAMINATI CON UN ANTIVIRUS

Il principale veicolo di diffusione dei virus é la posta elettronica. Per essere più precisi dovremmo dire i messaggi allegati ai messaggi di posta elettronica. Infatti, un virus può trasmettersi unicamente tramite file eseguibili (programmi con estensione exe,com,drv e dll) o contenenti una parte di codice che viene eseguita.(Es. documenti in formato word che contengono macro). Non é quindi possibile infettare il nostro computer leggendo semplicemente il testo di una e-mail ma é necessario eseguire il file infetto che potremmo trovare allegato alle e-mail che riceviamo. Va inoltre precisato che l'aprire un file allegato ad un messaggio di posta elettronica solo se si conosce il mittente non é di per se sufficiente a metterci al riparo dal contagio poiché alcuni tipi di virus prelevano dal pc infettato gli indirizzi di posta elettronica registrati nel client di posta elettronica ed inviano a questi una mail a nostro nome contenente in allegato il virus. I destinatari di tali messaggi potrebbero aprirli (allegato compreso) senza utilizzare alcuna precauzione, forti della sicurezza che gli deriva dal conoscere il mittente. Ecco spiegato come il virus " Melissa" abbia potuto contagiare milioni di computer! D'altro canto non possiamo neanche cestinare tutti gli allegati che riceviamo presumendo che siano infetti! Vale quindi sicuramente la pena di perdere qualche secondo per salvare l'allegato in un floppy disk e poi analizzarlo con un antivirus. Va infine segnalato che vi sono alcuni programmi che, una volta eseguiti sul vostro pc, ne permettono il controllo da una postazione remota. Anche questi possono essere contenuti nei file allegati ai messaggi di posta elettronica e possono essere segnalati da un buon antivirus. **NON ESEGUIRE PROGRAMMI PRIMA DI AVERLI ANALIZZATI CON UN ANTIVIRUS**

Abbiamo visto che cos'é un virus e come si trasmette. Ciò vale, ovviamente, non solo per gli allegati dei messaggi di posta elettronica ma anche per tutti quei file eseguibili contenuti nei floppy disk o nei cd rom. É quindi opportuno, in ogni caso, analizzare tali file con un antivirus prima di eseguirli.
EFFETTUARE COPIE DI BACKUP

Gli antivirus riducono drasticamente i rischi di contagio ma bisogna anche tener presente che se un antivirus riconosce un virus é perché precedentemente c'é stata qualche vittima. Ciò significa che si potrebbe anche verificare il caso che il nostro antivirus, poiché non aggiornato o poiché deve analizzare un virus nuovissimo, non riconosca quel file come uno contenente un virus. In questo caso potremmo, a seguito del contagio, anche perdere i dati contenuti sul nostro disco fisso. In tale sventurato caso sarà di vitale importanza avere effettuato, nei giorni precedenti il disastroso evento, una copia di back up dei nostri dati. **NON FORNIRE NELLE CHAT I PROPRI DATI PERSONALI**

Non cedere alla tentazione durante le conversazioni virtuali (chat) di fornire ad ignoti utenti i propri dati personali. Questo per un duplice motivo:

1. Non possiamo sapere chi c'é dall'altra parte della tastiera.
2. I nostri dati potrebbero essere utilizzati come punto di partenza per ricavare le nostre password .

SCEGLIERE UNA PASSWORD SICURA E NON COMUNICARLA A NESSUNO

1. Per creare una password sicura bisogna seguire i seguenti accorgimenti:
    - La password deve essere della lunghezza massima permessa dal sistema ed almeno di sei caratteri. Infatti, i programmi utilizzati per forzare le password richiedono, per riuscire nell'opera, un tempo direttamente proporzionale alla lunghezza delle password da violare.
    - La password non deve essere un termine di senso compiuto contenuto in un dizionario poiché esistono dei programmi che, supportati dalla potenza di calcolo degli elaboratori, provano tutte le parole contenute in un dizionario.
    - É preferibile che la password non contenga esclusivamente lettere minuscole o maiuscole ma che le contenga entrambe possibilmente unitamente a simboli alfanumerici come, ad esempio, asterischi e trattini. In questo modo, i programmi di forzatura delle password dovranno provare tutte le combinazioni di caratteri possibili richiedendo così, nel caso venga adottata una password lunga, molto tempo per trovarla.
    - La password non deve essere in alcun modo collegata alla vita privata del titolare ed a ciò che lo circonda. Non deve quindi essere costituita dalla targa della sua auto, dalla sua squadra del cuore, dal suo nome, dalla sua data di nascita etc. Questo perché i primi tentativi fatti da chi vorrà indovinare la password saranno legati alla vita privata del titolare della stessa.
    - La password non deve essere scritta da nessuna parte. A cosa serve scegliere una password inattaccabile se viene scritta su un post-it che viene lasciato attaccato al monitor o sul tappetino del mouse? Per creare una password che possa essere ricordata facilmente si può utilizzare la così detta "frase password" composta dalla prima lettera di ogni parola che compone una frase. Per esempio, dalla frase "Nel Mezzo Del Cammin Di Nostra Vita" si ricava la password NMDCDNV la quale ,per risultare più difficile da indovinare, sarà composta sia da lettere maiuscole che da lettere minuscole: nmdcDNV.
    - É preferibile utilizzare una password diversa per ogni applicazione. Infatti, nel caso in cui fosse scoperta i danni derivati sarebbero minori.
    - La password di default, assegnata dai sistemi la prima volta che vengono utilizzati, deve essere sostituita subito.
    - La password deve essere cambiata periodicamente.
    - Non comunicare a nessuno la propria password! Se vi é la necessità di comunicarla a qualcuno per qualsiasi motivo, bisogna cambiarla non appena possibile.

UTILIZZARE SOFTWARE DI CIFRATURA PER LE COMUNICAZIONI RISERVATE

Quando si inviano dati riservati é opportuno affidarsi ad un software di cifratura che permetta di crittare i messaggi da noi trasmessi. Questo perché, se anche il messaggio venisse intercettato, senza la chiave utilizzata per crittare il documento si avrebbero solo una serie di caratteri privi di alcun senso compiuto. Vi sono numerosi programmi che offrono questo tipo di protezione, prelevabili dalla rete Internet, disponibili gratuitamente. Le considerazioni ed i consigli elencati in questo articolo sono sicuramente basici eppure se ognuno di noi si attenesse a queste elementari "misure di sicurezza" nell'utilizzo e nell'interazione con la rete Internet assisteremmo ad una drastica riduzione dei crimini informatici e soprattutto dei danni da essi arrecati.

Buona navigazione a tutti.

06/08/2013