Sicurezza informatica

Con il termine **sicurezza informatica** si intende quel ramo dell'informatica che si occupa delle misure, di carattere organizzativo e tecnologico, tese ad assicurare a ciascun utente autorizzato tutti e soli i servizi previsti per quell'utente, nei tempi e nelle modalità previste. Il raggiungimento della disponibilità dipende da diversi fattori che interferiscono tra utente e sistema, quali: robustezza del software di base e applicativo, affidabilità delle apparecchiature e degli ambienti in cui essi sono collocati.

Il sistema informatico deve essere in grado di impedire l'alterazione diretta o indiretta delle informazioni, sia da parte di utenti non autorizzati, sia da eventi accidentali; inoltre deve impedire l'accesso abusivo ai dati.

L'interesse per la sicurezza dei sistemi informatici è cresciuto negli ultimi anni proporzionalmente alla loro diffusione ed al loro ruolo occupato nella collettività. Molti ex-hacker/cracker sono oggi dirigenti di società di sicurezza informatica o responsabili di questa in grandi multinazionali. Ciò sembra mostrare che per capire le strategie migliori di sicurezza informatica è necessario entrare nella mentalità dell'attaccante per poterne prevedere ed ostacolare le mosse.

Perdita di dati

 Le cause di probabile perdita di dati nei sistemi informatici possono essere molteplici, ma in genere vengono raggruppate in due eventi:

- Eventi indesiderati
- Eventi accidentali

Eventi indesiderati

Tra i due eventi sopra citati, quelli indesiderati sono quelli per lo più inaspettati, anche se è prudente aspettarsi di tutto, e sono i cosiddetti attacchi da parte di utenti non autorizzati al trattamento di dati o all'utilizzo di servizi. Alcuni degli eventi indesiderati che si possono subire possono essere:

- Attacchi hacking
- Uso delle proprie autorizzazioni per l'accesso a sistemi da parte di utenti non autorizzati.

Attacchi Hacking

Gli attacchi hacking, spesso conosciuti sotto il nome di attacchi hacker, vengono fatti tramite la rete internet, da parte di utenti chiamati appunto dalla società "hacker", che tramite l'uso di software particolari, a volte creati da loro stessi, si intrufolano abusivamente all'interno del sistema, riuscendo ad ottenere piena disponibilità della macchina, per gestire risorse e dati senza avere i giusti requisiti richiesti.

Accesso a sistemi da parte di utenti non autorizzati

Questo tipo di attacco sostanzialmente è simile al precedente, ma ha una forma diversa. Questo attacco consiste nell'uso non autorizzato di sistemi e di dati altrui, ma a differenza di un attacco hacker stavolta viene usata la macchina e non la rete.

 Effetti

La pericolosità degli attacchi in quanto tale, consiste non solo nella presa di possesso di requisiti, dati e servizi altrui, ma anche causa all'utente cosiddetto "derubato" una sorta di insicurezza a far fede sui sistemi informatici che spesso fanno parte della nostra vita quotidiana.

Eventi accidentali

Gli eventi accidentali non fanno riferimento ad un attacco da parte di terzi, ma fanno riferimento a eventi causati accidentalmente dall'utente stesso, tipo: uso difforme dal consigliato di un qualche sistema, incompatibilità di parti hardware, guasti imprevisti, ecc… Tutti eventi che comunque compromettono la sicurezza del sistema.

I principali aspetti di protezione del dato sono:

- La confidenzialità: protezione dei dati e delle informazioni scambiate tra un mittente e uno o più destinatari nei confronti di terze parti. Tale protezione deve essere realizzata a prescindere dalla sicurezza del sistema di comunicazione utilizzato: assume anzi particolare interesse il problema di assicurare la confidenzialità quando il sistema di comunicazione utilizzato è intrinsecamente insicuro (come ad esempio la rete internet).

- L'integrità dei dati: protezione dei dati e delle informazioni nei confronti delle modifiche del contenuto, accidentali oppure effettuate da una terza parte, essendo compreso nell'alterazione anche il caso limite della generazione ex novo di dati ed informazioni.

- La disponibilità: misura l'attitudine di un'entità ad essere in grado di svolgere una funzione richiesta in determinate condizioni ad un dato istante, o durante un dato intervallo di tempo, supponendo che siano assicurati i mezzi esterni eventualmente necessari.

La protezione dagli attacchi informatici viene ottenuta agendo su più livelli: innanzitutto a livello fisico e materiale, ponendo i server in luoghi il più possibile sicuri, dotati di sorveglianza e/o di controllo degli accessi; anche se questo accorgimento fa parte della sicurezza normale e non della "sicurezza informatica" è sempre il caso di far notare come spesso il fatto di adottare le tecniche più sofisticate generi un falso senso di sicurezza che può portare a trascurare quelle semplici.

Il secondo livello è normalmente quello logico che prevede l'autenticazione e l'autorizzazione di un'entità che rappresenta l'utente nel sistema. Successivamente al processo di autenticazione, le operazioni effettuate dall'utente sono tracciate in file di log. Questo processo di monitoraggio delle attività è detto audit o accountability.

Per evitare invece gli eventi accidentali, non esistono soluzioni generali, ma di solito è buon senso dell'utente fare una copia di backup del sistema, fare backup periodico di dati e applicazioni in modo da poter fronteggiare qualsiasi danno imprevisto.

Tipi di sicurezza

Quando si parla di sicurezza informatica si distinguono i concetti di *sicurezza passiva* e di *sicur ezza attiva.*

Per **sicurezza passiva** si intendono le tecniche e gli strumenti di tipo difensivo, ossia quel complesso di soluzioni tecnico-pratiche il cui obiettivo è quello di impedire che utenti non autorizzati possano accedere a risorse, sistemi, impianti, informazioni e dati di natura riservata.

Si deduce che il concetti di sicurezza passiva è molto generale, ad esempio, per l'accesso a locali protetti, l'utilizzo di porte ad accesso blindate, congiuntamente all'impiego di sistemi di identificazione personale, sono da considerarsi componenti di sicurezza passiva.

Per **sicurezza attiva** si intendono, invece, tutte quelle tecniche e gli strumenti mediante i quali le informazioni ed i dati di natura riservata sono resi intrinsecamente sicuri, proteggendo gli stessi sia dalla possibilità che un utente non autorizzato possa accedervi (confidenzialità), sia dalla possibilità che un utente non autorizzato possa modificarli (integrità).

Sicurezza passiva e sicurezza attiva sono fra loro complementari ed entrambe indispensabile per raggiungere il desiderato livello di sicurezza di un sistema.

Le possibili tecniche di attacco sono molteplici, perciò è necessario usare contemporaneamente diverse tecniche difensive per proteggere un sistema informatico, realizzando più barriere fra l'attaccante e l'obiettivo.

Spesso l'obiettivo dell'attaccante non è rappresentato dai sistemi informatici in sé, quanto piuttosto dai dati in essi contenuti, quindi la sicurezza informatica deve preoccuparsi di impedire l'accesso ad utenti non autorizzati, ma anche a soggetti con autorizzazione limitata a certe operazioni, per evitare che i dati appartenenti al sistema informatico vengano copiati, modificati o cancellati.

Principali tecniche di difesa

- **Antivirus**: consente di proteggere il proprio personal computer da software dannosi conosciuti come virus. Un buon antivirus deve essere costantemente aggiornato ad avere in continua esecuzione le funzioni di scansione in tempo reale. Per un miglior utilizzo l'utente deve avviare con regolarità la scansione dei dispositivi del PC (dischi fissi, CD, DVD e dischetti floppy), per verificare la presenza di virus, worm. Per evitare la diffusione di virus è inoltre utile controllare tutti i file che si ricevono o che vengono spediti tramite posta elettronica facendoli verificare dall'antivirus correttamente configurato a tale scopo.
- **Antispyware**: software facilmente reperibile sul web in versione freeware, shareware o a pagamento. È diventato un utilissimo tool per la rimozione di "file spia", gli spyware appunto, in grado di carpire informazioni riguardanti le attività on line dell'utente ed inviarle ad un'organizzazione che le utilizzerà per trarne profitto.
- **Firewall**: installato e ben configurato un firewall garantisce un sistema di controllo degli accessi verificando tutto il traffico che lo attraversa. Protegge contro aggressioni provenienti dall'esterno e blocca eventuali programmi presenti sul computer che tentano di accedere ad internet senza il controllo dell'utente.
- **Firma digitale**, **Crittografia**: è possibile proteggere documenti e dati sensibili da accessi non autorizzati utilizzando meccanismi di sicurezza specifici quali: la crittografia, la firma digitale, e l'utilizzo di certificati digitali e algoritmi crittografici per identificare l'autorità di certificazione, un sito, un soggetto o un software.
- **Backup**: più che un sistema di difesa si tratta di un utile sistema per recuperare dati eventualmente persi o danneggiati. Il backup consiste nell'esecuzione di una copia di sicurezza dei dati di un personal computer o comunque di dati considerati importanti onde evitare che vadano perduti o diventino illeggibili.
- **Honeypot**: un honeypot (letteralmente: "barattolo del miele") è un sistema o componente hardware o software usato come "trappola" o "esca" a fini di protezione contro gli attacchi di pirati informatici. Solitamente consiste in un computer o un sito che sembra essere parte della rete e contenere informazioni preziose, ma che in realtà è ben isolato e non ha contenuti sensibili o critici; potrebbe anche essere un file, un record, o un indirizzo IP non utilizzato.

- **Intrusion Detection System** (IDS): è un dispositivo software e hardware (a volte la combinazione di tutti e due) utilizzato per identificare accessi non autorizzati ai computer. Le intrusioni rilevate possono essere quelle prodotte da cracker esperti, da tool automatici o da utenti inesperti che utilizzano programmi semiautomatici. Gli IDS vengono utilizzati per rilevare tutti gli attacchi alle reti informatiche e ai computer. Un IDS è composto da quattro componenti. Uno o più sensori utilizzati per ricevere le informazioni dalla rete o dai computer. Una console utilizzata per monitorare lo stato della rete e dei computer e un motore che analizza i dati prelevati dai sensori e provvede a individuare eventuali falle nella sicurezza informatica. Il motore di analisi si appoggia ad un database ove sono memorizzate una serie di regole

utilizzate per identificare violazioni della sicurezza.

- **Network Intrusion Detection System** (NIDS): sono degli strumenti informatici, software o hardware, dediti ad analizzare il traffico di uno o più segmenti di una LAN al fine di individuare anomalie nei flussi o probabili intrusioni informatiche. I più comuni NIDS sono composti da una o più sonde dislocate sulla rete, che comunicano con un server centralizzato, che in genere si appoggia ad un Database. Fra le attività anomale che possono presentarsi e venire rilevate da un NIDS vi sono: accessi non autorizzati, propagazione di software malevolo, acquisizione abusiva di privilegi appartenenti a soggetti autorizzati, intercettazione del traffico (sniffing), negazioni di servizio (DoS).
- **Steganografia**: La steganografia si pone come obiettivo di mantenere nascosta l'esistenza di dati a chi non conosce la chiave atta ad estrarli, mentre per la crittografia è non rendere accessibili i dati nascosti a chi non conosce la chiave. La crittanalisi è l'attacco alla crittografia, che mira ad estrarre i dati cifrati senza chiave. L'obiettivo della steganalisi non è quindi quello di estrarre i dati nascosti, ma semplicemente di dimostrarne l'esistenza.

- **Sistema di autenticazione**: potrebbe rivelarsi utile, in particolare nelle aziende, l’utilizzo di software per l’autenticazione sicura con un secondo elemento di autenticazione basato su un insieme di caratteri disposti in uno schema suddiviso in file e colonne conosciute dall’utente che dovrà poi inserirle in una combinazione di valori per dimostrare di essere in possesso dei dati corretti. Altro sistema, più sofisticato, è quello del riconoscimento dell’utente tramite l’utilizzo dell’impronta digitale come forma di autenticazione.

MALWARE

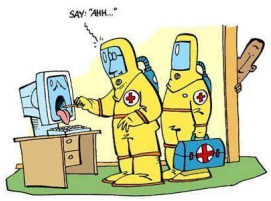
Il termine malware deriva dalla contrazione delle parole inglesi malicious e software e ha dunque il significato latterale di “ programma malvagio “, in italiano è anche detto codice malvagio.

Si definisce malware un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito.

Si distinguono molte categorie di malware, anche se spesso questi programmi sono composti di più parti interdipendenti e rientrano pertanto in più di una classe.

- **Virus**: sono parti di codice che si diffondono copiandosi all'interno di altri programmi, o in una particolare sezione del disco fisso, in modo da essere eseguiti ogni volta che il file infetto viene aperto. Si trasmettono da un computer a un altro tramite lo spostamento di file infetti ad opera degli utenti.
- **Worm**: questi malware non hanno bisogno di infettare altri file per diffondersi, perché modificano il sistema operativo della macchina ospite in modo da essere eseguiti automaticamente e tentare di replicarsi sfruttando per lo più Internet. Per indurre gli utenti ad eseguirli utilizzano tecniche di ingegneria sociale, oppure sfruttano dei difetti di alcuni programmi per diffondersi automaticamente. Il loro scopo è rallentare il sistema con operazioni inutili o dannose.
- **Trojan horse**: software che oltre ad avere delle funzionalità "lecite", utili per indurre l'utente ad utilizzarli, contengono istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore. Non possiedono funzioni di auto-replicazione, quindi per diffondersi devono essere consapevolmente inviati alla vittima. Il nome deriva dal famoso cavallo di Troia.

- **Backdoo**r: letteralmente "porta sul retro". Sono dei programmi che consentono un accesso non autorizzato al sistema su cui sono in esecuzione. Tipicamente si diffondono in abbinamento ad un trojan o ad un worm, oppure costituiscono una forma di accesso di emergenza ad un sistema, inserita per permettere ad esempio il recupero di una password dimenticata.
- **Spywar**e: software che vengono usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato. Le informazioni carpite possono andare dalle abitudini di navigazione fino alle password e alle chiavi crittografiche di un utente.



La classificazione qui sopra esposta non è da ritenersi esaustiva vista la rapida evoluzione in questo campo.

Importante sottolineare che un malware è caratterizzato dall'intento doloso del suo creatore, dunque non rientrano nella definizione di questo termine i programmi contenenti bug, che costituiscono la normalità anche quando si sia osservata la massima diligenza nello sviluppo di un software.

Nell'uso comune il termine virus viene utilizzato come sinonimo di malware el'equivoco viene alimentato dal fatto che gli antivirus permettono di rilevare e rimuovere anche altre categorie di software maligno altre ai virus propriamente detti.

I VIRUS

Il termine virus indica una porzione di codice che ha la caratteristica di auto replicarsi ed inserire se stesso in file eseguibili preesistenti sul sistema.

Come stato precedentemente detto i virus fanno parte della famiglia dei malware, anche se in realtà i virus più recenti mescolano le caratteristiche di diversi tipi di malware con lo scopo di diventare più difficili da individuare e più efficaci nel diffondere l'infezione.

Il ciclo di vita di un virus è caratterizzato da tre attività fondamentali:

- **creazione** del virus: è il momento in cui il virus viene creato dal programmatore e immesso nei primi sistemi;

- **epidemia**: è il momento in cui il virus passa da un computer all'altro allargando il suo raggio d'azione;

- **disattivazione**: è il momento in cui il virus viene eliminato, ovvero viene rimosso da tutti i computer.

La fase in cui il virus si propaga è a sua volta scandita da diversi momenti:

- **infezione**: quando il virus individua un potenziale sistema ospite, verifica che questo non sia già infettato da una copia di sé e, nel caso sia libero, lo infetta. Il virus resta poi latente per un certo periodo in cui l'unica attività che effettua è tentare di replicare l'infezione, passando da un ospite all'altro;

- **attivazione**: al verificarsi di un certo evento, detto trigger, il virus scatena l'azione vera e propria per la quale è stato progettato, che viene chiamata payload e in genere è distruttiva e mira alla cancellazione dei dati e all'indisponibilità del sistema in generale.

Anche la fase di disattivazione è articolata:

- **riconoscimento**: il virus viene identificato e viene riconosciuta la stringa identificativa che lo contraddistingue;

- **estirpazione**: utilizzando un antivirus, il virus viene rimosso.

I virus possono essere classificati in base a diverse caratteristiche, tra cui la più significativa è l'ambiente attraverso cui si propaga l'infezione e si sviluppa il virus. Sono distinguibili in questa ottica diverse tipologie di virus:

- i **boot virus**, che infettano il Boot Sector o il Master Boot Record dei dischi in modo da essere caricati all'avvio del sistema;

- i **file virus**, che infettano, con modalità molto varie, i file eseguibili e utilizzano lo scambio di questi ultimi per propagare l'infezione;

- i **macrovirus**, che sono scritti in VBA (Visual Basic for Application) un linguaggio per la scrittura di macro negli ambienti applicativi Office;

- i **network virus**, che si diffondono sfruttando le vulnerabilità dei protocolli di Internet.

ANTIVIRUS

La diffusione delle connessioni internet su larga scala ha sicuramente facilitato la diffusione dei virus informatici, divenendo internet il mezzo principale attraverso il quale si trasmette il virus dannoso. L'uso delle comunicazioni e-mail e la navigazione su alcuni siti internet possono portare direttamente il virus sul nostro computer, introducendo una serie di problematiche, non sempre riconosciute dall'utente.

Purtroppo, a molti di noi è già capitato di essere contagiati da un virus informatico. E' sicuramente tutti noi che abbiamo avuto ospite il virus sul nostro computer abbiamo sperimentando un certo grado di frustrazione e rabbia verso il sistema operativo o generalmente nei confronti del computer che all'improvviso è diventato inspiegabilmente lento (nei casi migliori), rallentando le proprie prestazioni, non eseguendo un dato programma oppure bloccarsi e riavvirsi continuamente.

Per cui, sarebbe opportuno cercare di proteggere il proprio computer dai virus informatici, evitando almeno un pò di arrabbiarci con il nostro computer. A questo punto, un antivirus aggiornato sarebbe una scelta utile e molto saggia che ci dice se il nostro computer è stato infettato oppure no.

Un **antivirus** è un software che ha la funzione di rilevare la presenza di virus informatici o altri programmi dannosi sul computer (vedi malware) ed eliminarli. Il suo compito principale sarebbe quello di identificare e impedire che programmi appositamente creati, detti appunto virus informatici, possano installarsi e diffondersi nel sistema operativo e nei files, distruggendo, cancellando o modificando la funzione degli stessi. Per cui, un buon antivirus è capace di rimuovere i virus già presenti sul nostro pc e prevenire dagli attacchi. Può essere preinstallato sul nostro pc, ma possiamo anche acquistarlo e installarlo successivamente.

Le parti che compongono un antivirus sono:

- Il file delle firme: è la parte fondamentale di un antivirus perchè contiene tutte le firme dei virus conosciuti.

- Il binario che svolge la funzione di ricercare il virus all'interno del personal computer.

- Il binario che serve ad attivare l'antivirus ogni volta che un nuovo file nel computer viene creato.

- Il binario che ha il compito di eseguire gli aggiornamenti dei file delle firme e dei binari dell'antivirus.

Esistono diversi modi in base ai quali funziona un buon antivirus. Ogni virus informatico possiede il proprio schema di funzionamento che è dato dalle istruzioni presenti nella c.d. "firma del virus". Per cui, uno dei principali modi di funzionamento di un antivirus sarebbe quello di cercare se uno determinato schema specifico per ogni virus sia presente all'interno della memoria RAM e/o all'interno dei file del computer. Questo tecnica di funzionamento dell'antivirus viene chiamata scanning e rappresenta la tecnica centrale di funzionamento di un buon antivirus. In pratica, l'antivirus cerca una determinata sequenza di byte, che è identificata come dannosa per il computer e poi eliminarla.

Questa tecnica di lavoro dell'antivirus è molto soddisfacente perchè è fondata sul continuo aggiornamento degli schemi che l'antivirus è in grado di riconoscere. Tale aggiornamento è eseguito solitamente da un gruppo di persone che sono specializzati nell'individuazione dei nuovi virus presenti oppure anche dopo una segnalazione degli utenti.

Un altro modo di funzionamento dell'antivirus è riconosciuto nella c.d. "ricerca euristica", chiamata anche la tecnica del "behaviour cheking". Questa tecnica si basa sulla possiblità di individuare comportamenti dei vari programmi presenti nel pc che sono considerati sospetti e come tali tipiche del comportamento di un programma dannoso, come il virus informatico.

Definire un ulteriore modo di funzionamento dell'antivirus è possibile. Si tratta della tecnica di "integrity cheking". Quando l'antivirus viene installato memorizza una serie di informazioni sui

file presenti nel computer. Lavora sul principio in base al quale ogni file infettato sembra molto diverso rispetto al file originale. Per cui, ogni cambiamento di un qualsiasi aspetto del file viene segnalato all'utente, in quanto possibile risultato dell'opera di un virus.

In generale, i professionisti della sicurezza informatica consigliano assolutamente la presenza di un antivirus sul nostro personal computer, soprattutto quando siamo utenti frequenti della rete Internet. Un buon antivirus deve essere costantemente aggiornato nella sua funzione, in modo da avere continua esecuzione della scansione in tempo reale. La scansione dovrebbe essere eseguita su tutti i dispositivi del pc, come dischi fissi, CD, DVD, ma non solo. Ogni volta che viene ricevuto un file tramite posta elettronica sarebbe opportuno avere un antivirus in grado di eseguire la scansione anche di ciò che viene ricevuto dall'esterno.

Il software usato per proteggere il nostro computer da possibili attacchi dei virus deve soddisfare alcuni criteri considerati importanti sia dai produttori dei software sia dagli utenti.

- Spazio occupato dall'antivirus. Un antivirus per essere considerato abbastanza soddisfacente, prima di tutto, deve occupare il minimo spazio possibile all'interno della memoria RAM o dell'hard disk, ovvero si dovrebbe cercare di minimizzare le dimensioni dello spazio richieste per far funzionare le applicazioni dell'antivirus.

- Basso profilo. Questo aspetto descrive l'impatto dell'antivirus sulle attività svolte dall'utente. Un buon antivirus dovrebbe funzionare adeguatamente senza interrompere il lavoro svolto dall'utente, ovvero il funzionamento dell'antivirus deve essere del tutto impercettibile dall'utente.

Conoscendo quanto un virus informatico possa essere dannoso per il buon funzionamento del sistema operativo e per la sicurezza dei file da noi creati e delle informazioni in questi contenute, è fondamentale anche sapere quali sono i limiti dell'antivirus presente nel nostro computer, in modo da poterlo rafforzare quando possibile o almeno evitando comportamenti informatici considerati a rischio.

Come abbiamo visto, l'antivirus possiede una serie di "firme di virus", che rappresentano il suo punto di forza, ma anche il suo punto debole. Da una parte, l'antivirus contiene le "firme dei virus" che permettono all'antivirus di svolgere la sua funzione di eliminazione dei virus riconosciuti. Dall'altra parte, però, l'antivirus riesce ad agire solo su quei virus che riconosce, lasciando la strada aperta a tutti i nuovi virus, che sono appunto quei virus che l'antivirus non riconosce come dannosi per il computer, permettendo il passaggio libero. In pratica, l'antivirus per quanto aggiornato possa essere, elimina solo quei software che riconosce come dannosi per il personal computer, lasciando passare una serie di altri software che possono essere anche dannosi, ma finchè non vengono riconosciuti come tali possono circolare liberamente nel computer. Bisogna tener conto del fatto che, ogni giorno per motivi diversi vengono creati virus nuovi che tentano di raggirare la barriera imposta dall'antivirus.

Inoltre, l'antivirus agisce riconoscendo tutti i virus solamente quando quest'ultimi siamo già entrati nel computer e hanno infettato un dato file, procedendo solo a questo punto con l'eliminazione del virus.

Uno dei punti deboli di un antivirus maggiormente segnalati dagli utenti è sicuramente l'utilizzo di una grande quantità di risorse del computer da parte dell'antivirus, il che comporta un rallentamento delle prestazioni del pc non insignificanti.

Poi c'è il problema del c.d. "falso positivo". Questo fenomeno si verifica quando un antivirus considera un file o un programma come dannosi quando in realtà non lo so. Per cui, se un file contiene delle istruzioni molto simili a quelli presenti nel virus riconosciuto come dannoso, allora può succedere che non si riesca ad aprire lo stesso file, considerandolo come infettato.

FIREWALL

Avere un antivirus buono e aggiornato rappresenta un punto in favore per gli utenti di fronte alle trappole virali, ma in molti casi tale protezione informatica può essere insufficiente. Per cui, affidarsi solo ed esclusivamente ad un buon antivirus possa esporre gli utenti a rischio non sempre riconosciuto. I professionisti del computer consigliano che, attualmente sarebbe opportuno agire con una protezione ulteriore, usando un mezzo aggiuntivo con buone caratteristiche prottetive. Si tratta della possibilità di utilizzare anche il firewall.

Il **firewall** è uno strumento di protezione informatica che permette di bloccare i virus ancora prima che questi ultimi entrano all'interno del computer. Per cui, indipendentemente se un virus è riconosciuto oppure no, il firewall ha il compito di impedire che questo entri nel proprio computer, evitando che il virus possa infettare il computer.

Letteralmente, il termine firewall fa riferimento a tutte quelle strutture che sono utilizzate per impedire la diffusione del fuoco all'interno di una data struttura. Nel contesto informatico, il termine firewall contiene tutta una serie di funzioni che appunto, servono a prottegere un dominio o una rete privata dalle "fiamme" derivanti dalla globale rete Internet.

La rete informatica può essere suddivisa in due domini:

- esterna, che comprende l'intera Internet e

- interna, chiamata anche LAN (Local Area Network), che comprende un numero limitato di un insieme di computer.

La funzione del firewall viene intesa come la possibilità di tener fuori dalla propria rete LAN tutte le problematiche che possono derivare dalla globale rete Internet oppure in senso inverso conservare l'integrità della rete LAN impedendo l'accesso non autorizzato dall'esterno.

Possiamo dire che, l'antivirus agisce correttamente solamente su quei virus che sono già presenti nel nostro computer, distruggendoli. Mentre, il firewall agisce ad un livello che è da considerarsi come precedente al livello del funzionamento dell'antivirus, impedendo l'entrata del virus stesso all'interno della struttura del computer, indipendentemente se tale virus è nuovo oppure di vecchia data.

Alcuni firewall sono costruiti in maniera tale da agire come una sorta di filtro sulle connessioni. Svolgono la propria funzione controllando, modificando e monitorando le informazioni che derivano dall'esterno, innalzando il livello di sicurezza del nostro computer e generalmente della LAN di cui facciamo parte. Il filtraggio dei contenuti avviene in modo da seguire alcune "politiche" di sicurezza informatica, vietando anche l'accesso ad alcuni siti internet, come per

esempio quelli con contenuti non adatti per i minori, quelli con contenuti non in linea con l'attività lavorativa (quando si tratta di una LAN aziendale) oppure generalmente un qualsiai sito non accettabile per motivi di censura per un qualsiasi motivo.

POSSIBILI MODI PER PREVENIRE L'IMPATTO DEI MALWARE INFORMATICI

In generale, esistono diverse strategie semplici che possiamo perseguire per ottenere una buona protezione del nostro computer. Sono:

- Cercare delle informazioni riguardanti i concetti di virus, antivirus e firewall e capire come ognuno di essi funziona, quali sono i punti di forza e quelli di debolezza.

- Installare un potente antivirus (Norton, McAfee, Panda, F-Secure, Trend, ecc.) e mantenerlo continuamente aggiornato grazie agli aggiornamenti disponibili sui siti dei produttori.

- Installare un potente firewall (Norton Personal Firewall, ZoneAlarm, Sygate Personal Firewall, ecc.) e configurarlo continuamente.

- Fare attenzione quando si naviga su internet e quando si vuole scaricare qualcosa, (soprattutto da dei siti con fonte non attendibile). Anche se il nostro antivirus ha già controllato il file eseguito, dichiarando che non è stato rilevato nessun virus informatico, questo non vuol dire che non c'è ne sia assolutamente nessuno, perchè come si sa l'antivirus protegge solo dai virus che riconosce come tali.

- Fare la scansione di qualsiasi file, programma o e-mail ricevuto dall'esterno e prima di avviare un CD/DVD.

- Fare attenzione quando si ricevono delle e-mail da una fonte sconosciuta, soprattutto se hanno un allegato sarebbe meglio non aprirle affatto.

... e tanti altri modi e strategie per proteggere il nostro computer da danni irreversibili che possono danneggiare delle informazioni importanti contenute nel nostro computer.

"scarica tesina in pdf "