IT Security

Il problema della sicurezza informatica

Come proteggere un sistema informatico e i suoi dati

L'insieme delle tecnologie e dei processi utilizzati per garantire la protezione di reti, sistemi operativi, programmi e dati da attacchi, danni o accessi non autorizzati prende il nome di **IT Security**. Il funzionamento dei programmi e la riservatezza delle informazioni conservate nei nostri computer e trasferite attraverso la Rete Internet sono continuamente esposti a differenti tipi di insidie, i rischi legati alla perdita dei dati e alla sottrazione fraudolenta delle informazioni sensibili sono sempre più probabili, e dunque lo scopo dell'IT Security è quello di minimizzare la vulnerabilità di sistemi, dati, informazioni e reti e garantire la protezione di un sistema informatico e dei dati in esso contenuti o scambiati nelle comunicazione informatiche.

Cosa è necessario proteggere?

Nell'ambito della IT security è fondamentale proteggere l'insieme delle componenti essenziali del computer (sistemi operativi, programmi, dati) e le reti che mettono in connessione i singoli dispositivi informatici.

Da cosa proteggersi?

Le minacce a cui sono esposti sistemi operativi e dati sono essenzialmente di due tipi: gli **eventi accidentali,** ovvero le conseguenze di eventi non prevedibili e legati a situazioni casuali quali, ad esempio, gli eventi atmosferici che determinano l'interruzione dell'erogazione di energia elettrica e possono avere delle conseguenze sugli hard disk con danni conseguenti su sistemi operativi e dati in essi contenuti, e gli **eventi indesiderati,** ovvero, le operazioni compiute da soggetti intenzionati a danneggiare il funzionamento dei dispostovi o a sottrarre informazioni e dati.

A seconda del tipo di minaccia, è possibile attivare diversi livelli di protezione, tramite diversi strumenti. Tali misure possono essere di due tipi: attive o passive.

Cos'è un attacco informatico?

Tra tutti gli eventi che possono compromettere la sicurezza del tuo computer o del tuo smartphone, i più pericolosi sono senza dubbio i cosiddetti **attacchi informatici**.

Attraverso la Rete Internet, infatti, è possibile compromettere, anche in maniera grave, il funzionamento di un PC o di un altro dispositivo, violando l'integrità, la riservatezza e la disponibilità dei dati e delle informazioni immagazzinate. L'autore di un attacco di questo tipo prende il nome di **hacker**.

Cosa si intende per MALWARE?

L'espressione malware indica un qualsiasi software creato allo scopo di causare danni ad un dispositivo su cui viene eseguito e sui dati che vi sono immagazzinati.

Virus

È un piccolo programma che contiene una sequenza di istruzioni in grado di attivare automaticamente azioni che danneggiano un computer. È pericoloso per la sua tendenza ad "infettare" altri programmi ed altri dispositivi creando copie di sé stesso.

Worm

Modifica il Sistema Operativo del computer, facendo in modo di essere eseguiti automaticamente all'avvio, rallentando il sistema con operazioni inutili e dannose.

Trojan horse (cavallo di troia)

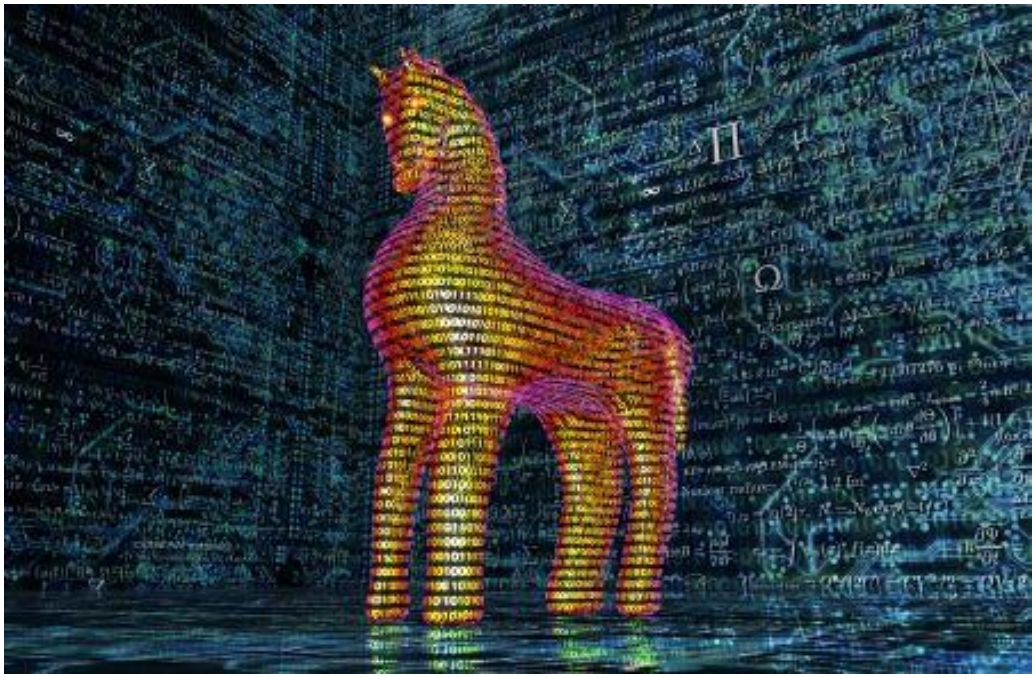
È un programma che l'utente scarica da internet perché ha funzionalità utili e richieste, ma che, una volta eseguito, avvia istruzioni dannose per i file del sistema operativo senza che l'utente se ne accorga.

Spyware

Sono software usati per spiare le informazioni del sistema sul quale sono installati: abitudini di navigazione, password e altri dati sensibili.

Zip Bomb

La zip bomb è un programma che disattiva le difese del PC per consentire a un altro virus di infettarlo.



Come possiamo difenderci?

L’unico computer totalmente e assolutamente sicuro è quello spento, non collegato a Internet e chiuso a chiave in una cassaforte!

Non è dunque possibile annullare completamente i rischi relativi alla sicurezza del nostro Pc (o altro dispositivo), ma è possibile utilizzare strumenti e procedure che rendano minimi tali rischi.

I software maligni (malware) vengono diffusi principalmente tramite la Rete internet (e-mail, condivisione di file in reti P2P e siti Web non attendibili), ma possono essere introdotti anche attraverso i dispostivi di memoria esterni, come chiavi USB.

Il principale strumento per la difesa dei dispositivi e dei loro dati è il buon senso dell’utente. In effetti, la colpa dell’elevata diffusione di malware è da attribuire soprattutto a chi utilizza il PC, che troppo spesso non si cura delle basilari misure di sicurezza che comunque ha a disposizione e potrebbe facilmente impostare. La protezione dei computer passa essenzialmente dalla presenza di dispositivi di difesa aggiornati e funzionanti come **firewall e antivirus**.

Guido Mondelli

Docente formatore informatico

www.informarsi.net