

Be Wary of the Dangers of Internet Intrusion

Scrutinizing the security of these web assets on the network for possible vulnerabilities is overriding. All modern database systems may be accessed all the way to specific ports and anyone can attempt unswerving connections to the databases effectively to evade the security apparatus used by the operating system. Acunetix Web Vulnerability Scanner guarantees website security by automatically checking for SQL injection, Cross site scripting and other troubles in the web. It verifies password strength on authentication pages and mechanically inspects the web applications. When the scan is complete, the software creates thorough reports and locates where the vulnerabilities come from.

This technique allows only certain predefined IP addresses to access the web site. Usually this method is used to curb the audience of the web site to precise physical areas or user communities. A widespread use would be a library that purchases a web-enabled database. The license for the record or database might denote that only users on a particular campus can access a source as a result, the web site's IP address limitations would be set to contradict everyone. A good number of web servers hold up very granular levels of IP restrictions. IP address restrictions are an uncomplicated way to confine a web sites, but are fully dependent on being able to classify the restricted audience by series of IP addresses.

A Computer Virus is a kind of "Malware" (or malicious software for short) that continuously attempts to spread itself from one file to another.

Computer viruses works a lot like human viruses as they are programs designed to propagate and create copies in the computers hard disk memory and infect other computers as well. This occurs beyond the users awareness.

The belief that viruses are programs designed to destroy or delete hard disk data is a misconception. Because technically speaking, viruses are only designed to make copies of itself and the damage it causes is most often incidental.

Therefore the damage caused by viruses is somewhat "unintentional" and caused by the continuous increase of infected files in the system.

Viruses are acquired when an infected file (or the virus itself) is introduced to the system. This commonly occurs when you get an infected removable storage device from other people or and through an e-mail attachment. The virus installs itself in your system and usually remains hidden to prevent detection.

One of the symptoms of having a virus is the sudden drop in the performance of the computer speed. This is due to the virus taking up too much space in your hard disk memory.

Another is the disability of certain functions of your computer, viruses can infect important files of your operating system disabling some of the system's functions in the process, leaving it open to other malware attacks.

The best way of combating computer virus is preventing it from getting into your system.

This also applies in the prevention of malwares that can disable your antivirus once it infiltrates your computer. The most popular tool for virus prevention is a virus scanner, it works to scan a file if it is harmful or not. If it detects a speck of malicious code it neutralizes it and gives you and option to delete the file or clean the file (options vary with the virus scanner).

Another tool which is equally as effective as the virus scanner is 'common sense'. Never run or open any file sent from the email or from other people unless you are sure that it does not contain virus, it is est to delete it right away. Beware of the hazards of downloading stuff from the internet, chances are, you are downloading a malware.

About the Author

Jon Caldwell is a professional content manager. Much of his articles can be found at <http://guidetowebsecurity.com>

Source: www.isnare.com

Source: <http://articles.exospy.com>