CIERRE LAS PUERTAS Y PROTEJA SU COMPUTADORA DE LA EXPLORACIÓN DE PUERTOS Y VIRUS MALICIOSOS

Una vez que se liquida la seguridad de su sistema, el intruso puede inspeccionar sus archivos, tratar de violar las contraseñas o transferir los archivos de su PC. Por consiguiente, sus datos confidenciales como la información financiera o de las tarjetas de crédito se exponen al robo. El intruso también puede secretamente convertir su PC en servidor de Internet, usando su conexión de forma gratuita.

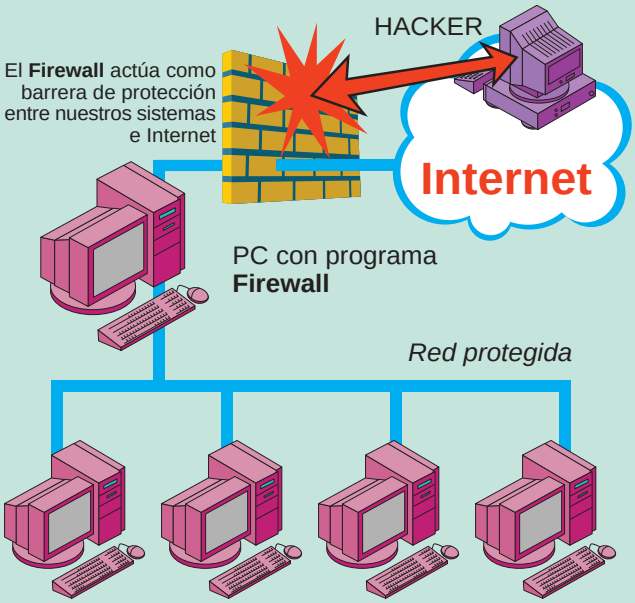
Por: Ramiro Mora
Ingeniero Electrónico

Antivirus y Firewall, imprescindibles en su PC

La computadora de su hogar tiene múltiples puertos, cada uno con una función importante. Existen puertos internos y externos que conectan los dispositivos periféricos como las pantallas, teclados e impresoras, y hay otra clase de puerto (identificado con diferentes números) que se utiliza en las redes TCP/IP, conecta los archivos y controla los paquetes de datos específicos que entran y salen de su computadora (por ejemplo a Internet). Esta clase de puertos exponen su computadora a intrusos indeseados. Los hackers pueden utilizar fácilmente software para explorar los puertos y encontrar aberturas vulnerables en su sistema operativo. Los análisis de puerto se pueden hacer de forma rápida y aleatoriamente. Por esta razón, su PC puede estar en peligro cada vez que se conecta a Internet.

Una vez que se compromete la seguridad de su sistema, el intruso puede inspeccionar sus archivos, tratar de violar las contraseñas o transferir los archivos de su PC. Por consiguiente, sus datos confidenciales como la información financiera o de las tarjetas de crédito se exponen al robo. El intruso también puede secretamente convertir su PC en servidor de Internet, usando su conexión de forma gratuita.

Para evitar estos ingresos no deseados es necesario contar con algún software adicional como son los llamados antivirus y firewalls personales, los que protegerán contra sitios, personas inescrupulosas y programas intrusos mientras navegamos por Internet.



Firewall y antivirus

Un sistema básico de seguridad es un Firewall o cortafuegos. Un firewall es un sistema de defensa que se basa en la instalación de una "barrera" entre nuestra PC y la Red, por la que circulan todos los datos. Este tráfico es autorizado o denegado por el firewall, siguiendo las instrucciones que hayamos configurado.

El firewall puede formar parte de nuestra red corporativa o Intranet, dependiendo si la conexión se realiza desde la oficina y si se trata de una conexión doméstica; el firewall es un programa adicional instalado en nuestra computadora.

El funcionamiento de este tipo de programas se basa en el "filtrado de paquetes". Todo dato o información que circule entre nuestra PC y la Red es analizado por el programa (firewall) con la misión de permitir o denegar su paso en ambas direcciones (Internet-->PC ó PC--->Internet). Comprender este proceso es muy importante, ya que si autorizamos a un determinado servicio o programa, el firewall no indicará si es correcto o incorrecto, o talvez siendo correcto, los paquetes que están entrando o saliendo puedan contener datos perniciosos para el sistema o la Red, por lo que se deberá ser cuidadoso respecto a las autorizaciones que otorguemos.

Como ejemplo tomemos el Correo Electrónico. Si autorizamos en nuestro firewall a que determinado programa de correo acceda a Internet, y al recibir nuestros mensajes, uno trae adjunto un virus, por ejemplo el virus tipo gusano, el firewall no nos defenderá del virus, ya que hemos autorizado a que ese programa acceda a la Red. Lo que sí puede suceder es que si al ejecutar el adjunto, el gusano intenta acceder a la Red por algún puerto que no esté previamente aceptado por nosotros, no le permitirá propagarse. Ahora bien, si hace uso del mismo programa cliente de correo, se propagará inevitablemente.

La misión del firewall es la de aceptar o denegar el tráfico, pero no el contenido del mismo. Este programa funciona en principio, denegando cualquier tráfico que se produzca mediante el cierre de todos los puertos de nuestro PC. En el momento en que un determinado servicio o programa intente acceder a Internet o a nuestro PC el firewall nos hará conocer al respecto, y podremos en ese momento aceptar o denegar dicho tráfico.

Una vez que se compromete la seguridad de su sistema, el intruso puede inspeccionar sus archivos, tratar de violar las contraseñas o transferir los archivos de su PC. Por consiguiente, sus datos confidenciales como la información financiera o de las tarjetas de crédito se exponen al robo. El intruso también puede secretamente convertir su PC en servidor de Internet, usando su conexión de forma gratuita.

Elección del programa adecuado

Después de conocer los conceptos básicos de seguridad nos toca elegir un firewall y un antivirus apropiado. En el mercado local existen muchos a disposición y otros tantos que pueden ser descargados de Internet, los precios suelen ser muy variados, dependiendo del tipo de versión que se requiera, pero también existen otros gratuitos.

En www.kerio.com encontramos un buen firewall, muy recomendado por los usuarios domésticos por la facilidad de configuración y una interfase amistosa que ofrece. Por su parte Sygate.com pone a disposición otro sistema de protección con características similares al anterior.

Una buena combinación puede ser Norton Antivirus 2004 y el Firewall ZoneAlarm de Zone Labs. Algunos firewalls son mejores que otros y este último es considerado uno de los más seguros, pero también se puede probar el Sygates FW Personal o el nuevo Tiny Firewall.

Lo importante es que una vez realizada la elección de antivirus y firewall, se proceda a la prueba. Para ello existen diversos sitios web que realizan pruebas de seguridad de la computadora como http://www.grc.com. Para la verificación de puertos se puede acceder a http://scan.sygatetech.com

Para la elección de un antivirus, se recomienda Sophos Antivirus (http://www.sophos.com), AVG Antivirus System (http://www.grisoft.com) o PC – Cillin (http://www.antivirus.com) fuera de los tradicionales Norton o Mcafee que son muy populares entre los usuarios.

En http://www.microsoft.com/latam/seguridad/proteccion/default.asp, Microsoft pone a disposición de sus clientes una serie de consejos de seguridad para sus diferentes versiones de Windows, las que permitirán tener una mayor y mejor compresión sobre este aspecto que muchas veces puede resultar indispensable al momento de presentarse un problema de intrusión o de infección.

Finalmente los programas más recomendados para este 2004 son:

- Norton Internet Security, con su filtrado de sitios no adecuados para los hijos y su AntiVirus 2004
- Zone Alarm Pro y Norton Personal Firewall 2004 ■

WEBSITES

www.mcfee.com	*www.agnitum.com*
www.symantec.com	*www.keiro.com*
www.zonelabs.com	*www.sygate.com*
www.tinysoftware.com	*www.grisoft.com*