Eduardo E. Quiroga Gómez-k idatzia
Ostirala, 2005(e)ko iraila(r)en 30-(e)an 12:49etan

There are no translations available.
En este artículo analizamos los tipos de ataques mas comunes a los que nos enfrentamos diariamente por la red y algunas recomendaciones para evitarlos.

A menudo nos preguntamos qué podemos hacer ante cada una de las amenazas que se encuentran en Internet.
Las amenazas a nuestra seguridad no las resuelve un solo programa por sofisticado y completo que nos parezca, aunque existen suites de seguridad que aglutinan varios modos de protección para nuestro equipo como antivirus, firewall, control de contenidos Web, antiespias etc.
Entre las suites de seguridad más utilizadas y reconocidas se encuentran las de Norton , Mcafee , Panda y Kaspersky .

En realidad, el asunto de la seguridad es algo que no sólo depende de todos los programas que "vigilan" nuestro equipo, sino también de nosotros mismos. Aquí el factor humano (o sentido común) es tan importante como las estrategias de seguridad que implementamos con los programas adecuados.

A continuación voy a describir lo que todos deberíamos tener instalado en nuestros equipos para poder usar nuestro PC y navegar mucho más seguros, aunque también hay que decir que por mucho que nos protejamos, todo sistema de seguridad es susceptible de ser vulnerable:

1. Un antivirus.

Los virus son programas que se introducen en nuestros ordenadores de formas muy diversas y que pueden producir efectos no deseados y nocivos. Una vez el virus se haya introducido en el ordenador, se colocará en lugares donde el usuario pueda ejecutarlos de manera no intencionada, ya que para que el virus actúe, es necesario que se ejecute el programa infectado o se cumpla una determinada condición. Es por esto por lo que en algunas ocasiones, los efectos producidos por un virus, se aprecian tiempo después de su ejecución.

Los medios de entrada más habituales para los virus son:

1. Las unidades de disco extraíbles (disquetes, CD-ROM, unidades ZIP, pendrives etc.)

2. Internet (navegando, mediante correo electrónico, al descargar archivos etc.)

3. Una red de ordenadores de una empresa en la que se comparten archivos de todo tipo, que si están infectados, pueden acabar extendiéndose por todos los equipos de la red.

Los archivos más susceptibles de infectarse son los que se encuentran en un medio de almacenamiento como los discos duros o disquetes. Más concretamente serán infectados todos aquellos archivos, ficheros o documentos que tengan la característica de ser programas. A pesar de que estos son los mas normales, también existen virus que se encargan de infectar ficheros que no son programas, como por ejemplo ficheros que contienen macros. Estas macros son programas que el usuario puede incluir dentro de un determinado tipo de archivos y que permiten la ejecución de otros programas u otras órdenes que pueden ser letales para nuestro equipo.

Debido a todo esto, un antivirus es el sistema defensivo contra virus, gusanos, troyanos y otras amenazas por antonomasia. Hoy en día un ordenador sin antivirus o con uno no actualizado, está expuesto a todo tipo de ataques cuyos nefastos resultados van desde la pérdida de datos vitales hasta el espionaje de todo lo que hacemos con él.
Tener un antivirus se ha convertido en algo imprescindible para nuestro equipo, sobre todo si hablamos a nivel empresarial, aunque cada vez se está usando más a nivel personal, ya que el gasto que supone un antivirus no es comparable a lo que nos puede suponer el recuperar los datos perdidos por culpa de un virus.

Existe una amplia gama de modelos de antivirus entre los que elegir, y los precios son muy interesantes debido a la competencia. Además de los antivirus de pago, existen muchos otros antivirus gratuitos, que si bien no tendrán una base de datos de virus tan amplia como los otros, ofrecen una excelente protección contra muchos de los virus que circulan por la red.
De todas formas, elijamos un antivirus profesional o uno gratuito, lo importante es que nuestro ordenador cuente con uno de estos programas, ya que siempre será mejor que no contar con ningún sistema de protección.

Estaremos aún más seguros bajo la vigilancia de dos antivirus, aunque antes de aventurarnos, debemos informarnos de las incompatibilidades de unas marcas con otras.

Lo que nunca debemos hacer es tener más de un antivirus activo, ya que podríamos tener serios problemas de seguridad e incluso colgar el ordenador.

Estas son algunas direcciones de programas antivirus donde podremos analizar nuestro equipo o-nline, probarlos, y si quedamos satisfechos comprarlos:

- Trend micro
- Bit Defender
- Kaspersky
- Norton
- Mcafee
- Panda
- AVG Antivirus
- Clam Win

2. Un cortafuegos o Firewall.

Cuando un ordenador accede a Internet se comunica mediante unas "puertas" llamadas puertos de conexión. Existen 65.535 canales por donde los datos pueden salir o entrar en nuestro ordenador, de manera que alguien puede intentar una intrusión por cualquiera de esos puertos. En realidad no es tan fácil la intrusión porque si intentamos acceder a un ordenador por un puerto y éste no está escuchando (listening), será imposible. Pero Windows abre por defecto varios puertos que dejan nuestros ordenadores muy vulnerables.

Un buen cortafuegos debe cerrar todos los puertos que no se estén usando e impedir cualquier conexión a través de ellos. Esto garantiza muchísimo nuestra seguridad.
Al contrario de lo indicado en los antivirus, nunca deben instalarse dos cortafuegos al mismo tiempo. La interferencia entre ambos puede ocasionar aperturas involuntarias de puertos que harían nuestro ordenador más inseguro.

Dos ejemplos de buenos cortafuegos son ZoneAlarm y Tiny , además de los de Norton, Panda y Mcafee mencionados anteriormente.

Funcionamiento de un Firewall

Un firewall consiste en un mecanismo basado en software o en hardware que se coloca entre dos redes, normalmente entre una LAN e Internet, y que permite ciertas conexiones y bloquea otras siguiendo unas reglas previamente configuradas.
Los firewalls como he comentado antes, pueden ser un programa especial que se instale en un PC, o bien un dispositivo hardware que realice esa función o que incluso puede venir implementado en ciertos dispositivos como los Routers.
Los firewalls personales como Zone Alarm, Tiny o BlackICE, son Firewalls basados en Software pero que solo protegen a la máquina que lo tiene instalado. Están diseñados para pequeñas redes o usuarios individuales.
A nivel personal o de una pequeña organización, si estos programas se complementan con otro tipo de software como un antivirus, conseguiríamos un nivel de seguridad más que aceptable.

Realmente todos tienen la misma finalidad, que es bloquear cierto tipo de tráfico en la red que se considera inapropiado. A pesar de eso existen dos maneras de bloquear ese tráfico, filtrando en la capa de red o en la capa de aplicación:

1. Un firewall de capa de red filtra los paquetes basándose en reglas predefinidas que indican direcciones destino u origen y un número de puerto.

2. Un firewall basados en una aplicación, actúa como Proxy e impide el tráfico entre dos redes pero permite que ciertas aplicaciones del interior de la red sean accesibles a determinado software del exterior.

Si queremos ver un Firewall en funcionamiento, en este enlace hay un video que muestra el funcionamiento de la red y cómo el Firewall acepta o rechaza los paquetes que le llegan según se le hayan establecido las reglas. Video Firewall

3. Un antispyware

El Spyware es un software espía creado con la finalidad de recoger información del usuario que lo tiene instalado y, en la mayoría de casos, sin que este usuario sea consciente de lo que está ocurriendo.
Existen varios tipos de spyware, por lo que los podemos llamar según la función que realice su

código malicioso:

- Adware: abren ventanas (pop-ups) en las que se muestra publicidad mientras ejecutamos aplicaciones.

- Spyware: pequeño programa que se instala en nuestro equipo para robar nuestros datos y espiar nuestros movimientos por la red, recopilando datos sobre las webs que visitamos.

- Hijackers: programa que redirige el navegador de Internet a páginas de su elección secuestrando la página de inicio o de búsqueda de nuestro navegador.

- Dialers: programa capaz de modificar el número de teléfono con el que nos conectamos a nuestro ISP (Proveedor de Servicios de Internet) para que llamemos a un número de tarificación adicional con el coste que eso supone. (906;806;807;etc).

Algunos se instalan automáticamente sin nuestro consentimiento, no están calificados como virus pero invaden nuestra intimidad y hacen peligrar en la mayoría de los casos la estabilidad del sistema y especialmente el funcionamiento del navegador o el cliente de correo electrónico, e incluso pueden llegar a recopilar información sobre nosotros y nuestro PC. Otros se instalan cuando descargamos extras para nuestro navegador como por ejemplo toolbars (barras de herramientas adicionales).

Hay ciertos programas que pueden recabar información de nuestros hábitos de navegación para elaborar complejas estadísticas de consumo, normalmente con fines comerciales.
La solución para librarnos de esos programas que recogemos a veces de forma involuntaria cuando instalamos un programa freeware, es instalar en nuestro ordenador un antispyware.

Existen algunos antivirus en el mercado que también detectan y eliminan esos programas spywares como por ejemplo PER Antivirus , que además de actualizar su base de datos de virus, también la actualiza con los spywares y adwares, dándonos la opción de eliminarlos si así lo deseamos.

Existen muchísimos programas que eliminan spyware, muchos de ellos específicos para alguno de ellos, pero lo ideal es complementar a nuestro antivirus con un programa anti-spyware como Ad-aware o SpyBot Search & Destroy , incluso sería conveniente tener instalados los 2, ya que hay veces en que lo que uno no es capaz de eliminar, el otro sí

que puede, además no dan problemas entre sí como sucedía con los antivirus y su interfaz puede ponerse en castellano.

4. Un programa para eliminar huellas en Internet.

Para conseguir información de nuestros equipos, no es necesario que se nos instale ningún spyware, simplemente al visitar determinadas Webs que tengan en su código Java, JavaScript, u otros lenguajes como éstos que tienen herramientas muy poderosas para saber datos nuestros.

Entre otras cosas, pueden obtener datos como nuestra IP, el tipo de navegador que utilizamos, el sistema operativo que tenemos, nuestras direcciones de correo electrónico, cuántas páginas hemos visitado antes de llegar a la página que nos espía, la dirección de al menos la última de esas páginas, el número de bits de clave secreta para el cifrado mediante SSL (protocolo que posibilita la transmisión cifrada y segura de información a través de la red), el tipo de monitor que usa, el nombre del ordenador, si pertenece a una red corporativa o no, etc.

Si saben nuestro correo electrónico pueden usarlo para enviarnos spam (publicidad no solicitada) de manera masiva. Además, muchos usuarios hacen coincidir su dirección de correo electrónico o el nombre de su PC con su nombre verdadero, por lo que de esta manera podrían llegar a conocer nuestra dirección, número de teléfono etc.
Algunas páginas han sido capaces de obtener contraseñas y otros datos relevantes simplemente robando las cookies(documento de texto en el que se almacenan nuestras preferencias sobre ciertas webs y sobre la conexión) almacenadas en nuestro disco duro.

Para evitar todo esto, es conveniente navegar a través de un Proxy o con un programa específico que impida todo esto. Si utilizamos un Proxy, podemos tener problemas porque son muy inestables, lentifican las conexiones y a veces no tendremos los permisos necesarios para utilizarlos.

Una opción podría ser usar un anonimizador de navegación como Anonymizer . Este programa es de pago, aunque podemos usarlo en su versión gratuita, pero estaremos muy limitados porque habrá páginas a las que no podamos acceder.

Otro programa muy interesante para navegar seguros es Proxomitron , que elimina código HTML malicioso impidiendo entre otras cosas la aparición las molestas ventanas de pop-ups, la ejecución de gusanos vía Web, y lo mejor de todo es que no necesita instalarse, por lo que no tocará nada de la configuración de nuestro equipo ni del registro.

5. Un programa que monitorice los puertos.

Cuando accedemos a Internet en nuestro ordenador se abren conexiones con el exterior, y estas a su vez se establecen por un puerto determinado cada una.
Conociendo los puertos de cada aplicación, podremos advertir cualquier anomalía inmediatamente, porque cuando nos infectamos con un troyano, éste debería abrir su correspondiente puerto y lo sabríamos porque el programa que monitoriza los puertos nos avisaría.
En este link podemos ver un listado de puertos en el que nos explican cómo saber si tenemos algún troyano en nuestro equipo y un listado de los puertos mas utilizados por los troyanos.
Estos programas nos pueden mostrar la IP del atacante, para así poder impedir que nuestro equipo se pueda conectar con esa dirección mediante reglas del firewall o en este mismo programa.
Además podríamos saber dónde están ubicados los servidores de las páginas Web que visitamos y el tipo de conexión que establecen con nuestros ordenadores, con lo que tendríamos controlado prácticamente el 100% del tráfico de Internet.

Un interesante programa de este tipo es Visualookout , aunque existen muchos programas similares a éste.

Tipos de ataques más comunes

A continuación encontrareis un listado con los ataques más comunes a los que nos enfrentamos diariamente en Internet ordenado por tipos:

Escaneo (Búsqueda):

El escaneo, como método de descubrir canales de comunicación susceptibles de ser explotados, lleva en uso mucho tiempo. La idea es escanear tantos puertos de escucha como sea posible, y guardar información de aquellos que sean receptivos o de utilidad para cada necesidad en particular.
Existen diversos tipos de Scanning según las técnicas, puertos y protocolos explotados:

- **TCP connect scanning**: forma básica de escaneo de puertos TCP para encontrar puertos abiertos por los que entrar.
- **TCP SYN scanning:** simula una conexión cliente-servidor en la que se envía un paquete SYN, si recibe respuesta, se corta la comunicación y se registra ese puerto como abierto.

- **TCP FIN Scanning- Stealth Port Scanning:** similar al anterior pero más clandestino.
- **Fragmentation scanning:** modificación de los anteriores, pero fragmentando los paquetes.
- **Eavesdropping-packet snnifing:** intercepta paquetes de la red sin modificarlos para, por ejemplo, averiguar passwords.
-

Snooping downlading: igual que el anterior, pero además intercepta archivos que pueden descargar.

Ataques de autentificación:

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo, para ello el atacante hace suplantación de la identidad. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password.

- **Spoofing-Looping:** consiste en hacerse pasar por otra persona para luego tomar acciones en su nombre. Existen varios tipos como el spoofing de IP, DNS, WEB etc.

- **Web Spoofing (Phising):** el atacante crea un sitio Web falso similar al original, permitiendo averiguar desde datos de la victima hasta claves de bancos.

- **IP Splicing-Hijacking:** consiste en suplantar a un usuario autorizado cuando este se identifica.
- **Utilización de BackDoors:** permite saltarse los métodos normales de autentificación.
- **Utilización de Exploits:** aprovechan fallos hardware o software para entrar en el sistema.
- **Obtención de Passwords:** obtención de contraseñas por prueba y error o mediante programas que utilizan unos diccionarios con millones de claves que van probando hasta dar con la clave correcta.

Denial of service (DOS):

Los protocolos existentes actualmente fueron diseñados para ser empleados en una comunidad abierta y con una relación de confianza mutua. La realidad indica que es más fácil desorganizar el funcionamiento de un sistema que acceder al mismo; así los ataques de Negación de Servicio tienen como objetivo saturar los recursos de la víctima de forma tal que se inhabilita los servicios brindados por la misma.

- **Jamming o Flooding:** desactiva o satura los recursos del sistema, como memoria, disco, etc.
- **Syn Flood:** se establece una conexión "a medias", de manera que el equipo queda pendiente de contestación del equipo hostil, con lo que se ralentiza el sistema.

- **Connection Flood:** hace que se supere el límite de conexiones dejando colgado al servidor de Internet.
- **Net Flood:** satura la línea con tráfico malicioso, impidiendo el tráfico útil de la red.
- **Land Attack:** consiste en mandar un paquete con la dirección y puerto de origen igual a la de destino, con lo que el sistema acaba colgándose.
- **Supernuke o Winnuke:** envío de paquetes manipulados al rango de puertos 137-139 que hace que se cuelgue el equipo.
- **Teardrop I y II-Newtear-Bonk-Boink:** impide que se puedan armar correctamente los fragmentos que forman un paquete, haciendo que se sature el sistema.

- **E-Mail Bombing-Spamming:** el primero consiste en saturar una cuenta de correo por el envío masivo de un mismo mensaje, y el spamming lo que hace es un envío masivo de un mail a miles de usuarios sin su consentimiento.

Ataques de modificación-daño:

- **Tampering o Data Diddling:** modificación desautorizada de los datos o el software instalado en el sistema víctima, incluyendo el borrado de archivos.

- **Borrado de Huellas:** consiste en eliminar todas las tareas que realizó el intruso en el sistema para impedir que sea localizado.
- **Ataques Mediante Java Applets:** aprovecha fallos de seguridad de las "Maquinas virtuales de java" para lanzar ataques.
- **Ataques Mediante JavaScript y VBscript":** se usa para, por ejemplo, enviar correos sin el conocimiento del usuario, lectura de directorios, archivos, ver el historial de paginas visitadas etc.
- **Ataques Mediante ActiveX:** manipula el código de ciertos exploradores, para que éste no solicite confirmación al usuario a la hora de descargar otro control activo de Internet, así pueden introducir código malicioso.
- **Ataques por Vulnerabilidades en los Navegadores:** permite acceder al buffer del equipo y ejecutar programas como por ejemplo format.com.

Explotación de errores de diseño, implementación y operación:

Muchos sistemas están expuestos a "agujeros" de seguridad que son explotados para acceder a archivos, contraseñas, u obtener privilegios. Estas vulnerabilidades están ocasionadas por fallos de programación en los sistemas operativos, aplicaciones de software, protocolos de red, navegadores de Internet, correo electrónico, etc.

Recomendaciones para evitar el contagio de virus y spyware

1) Tener siempre activo un programa antivirus y un antispyware; lo recomendable es no confiar en uno solo, pero usar más de uno no significa que debamos tenerlos a todos instalados, simplemente ejecutamos esos antivirus y antispywares en su opción de escaneo, sobre la carpeta que contenga los archivos a revisar.

2) Igual de importante que el tener el antivirus instalado es tenerlo actualizado al máximo. Actualmente, las actualizaciones son diarias en la mayoría de los programas, o como mínimo semanales, por lo que si el antivirus que tenemos no se actualiza con una frecuencia máxima de una semana, lo mejor sería cambiarnos a otro que tuviese actualizaciones diarias o varias semanales.
Lo mismo ocurre con un programa antispyware, debemos tenerlo lo mas actualizado posible, ya que así se corrigen agujeros de seguridad que pueden poner en riesgo nuestra seguridad. Muchos gusanos en la actualidad tienen éxito debido a la pereza de los usuarios a actualizar sus programas, por lo que una conciencia de renovación continua de los programas de nuestros ordenadores, en especial aquellos más delicados como navegadores, sistemas operativos, clientes de P2P y otros, es básica para estar seguros.

3) No abrir ningún mensaje ni archivo recibido a través del correo electrónico de fuentes desconocidas o muy poco conocidas. En el caso de personas conocidas, se deben tomar igualmente las precauciones correspondientes. Asegurarse con esa persona del envío, y nunca ejecutarlos antes de pasar el antivirus actualizado a estos archivos. Ante cualquier duda, simplemente se debe optar por borrar el mensaje y los archivos adjuntos.

4) Estar informado de cómo operan los virus, y de las novedades sobre estos, alertas y anuncios críticos, en la propia página Web del antivirus que tengamos instalado o en la dirección:
http://alerta-antivirus.red.es/portada/

5) No bajar nada de sitios Web de los que no tenga referencias de seriedad, o que no sean medianamente conocidos. Y si se bajan archivos, debemos hacer como con los archivos adjuntos, examinarlos con el antivirus antes de ejecutarlos o descargarlos.

6) Probar varios antivirus, firewalls, antispyware etc., descargando su versión trial (versión de prueba) que suele durar entre 15 y 30 días, con lo que podremos probar varios antes de decidirnos por comprar el que mas se adapte a nuestras necesidades.
Informarnos sobre su facilidad de uso y configuración, soporte posventa, características y rendimiento. Encontrar usuarios de esos programas que nos proporcionen su opinión sobre

este u otros programas similares. Lo mejor que podemos hacer es navegar en algún foro dedicado a seguridad o en los propios de la empresa del programa, donde podremos leer detalles importantes de funcionamiento de la gente que lo usa. Éstos incluso contestarán a las preguntas que les hagamos, y veremos las ventajas e inconvenientes de los propios usuarios.

Referencias

http://www.infospyware.com/index.htm
http://www.definicion.org
http://alerta-antivirus.red.es/portada/
http://www.softwaresecuritysolutions.com/
http://www.sin-espias.com/