SEGURIDAD EN LAS REDES

La **seguridad** de **redes** consiste en las políticas y prácticas adoptadas para prevenir y supervisar el acceso no autorizado, el uso indebido, la modificación o la denegación de una **red** informática y sus recursos accesibles. ... La **seguridad** de la **redes** está presente en organizaciones, empresas y otros tipos de instituciones.

CUAL ES SU IMPORTANCIA

Un buen sistema de **seguridad.** Evita ataques informáticos. Asegura los datos, evita su robo o la pérdida de los mismos. Evita la pérdida de las configuraciones. Minimiza el spam que se recibe.

COMO PROTEJO UNA RED

Antivirus, Firewall, Anti-spyware: pueden ayudar a **proteger** nuestra **red** inalámbrica al detectar programas espías que intenten alojarse en nuestro ordenador. acceso de ordenadores específicos: Es importante restringir el acceso a ordenadores específicamente, ya sea por dirección IP, MAC.

Protección del Software

Protección del Hardware

Protección de la Red

VIRUS INFORMATICO

Un **virus informático** es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más "benignos", que solo se caracterizan por ser molestos.

Los virus informáticos tienen, básicamente, la función de propagarse a través de un software, no se replican a sí mismos por que no tienen esa facultad como el gusano informático, son muy nocivos y algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

El funcionamiento de un virus informático es conceptualmente simple. Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario. El código del virus queda residente (alojado) en la memoria RAM de la computadora, aun cuando el programa que lo contenía haya terminado de ejecutarse. El virus toma entonces el control de los servicios básicos del sistema operativo,

infectando, de manera posterior, archivos ejecutables que sean llamados para su ejecución. Finalmente se añade el código del virus al del programa infectado y se graba en disco, con lo cual el proceso de replicado se completa.

Historia

El primer virus que atacó a una máquina IBM Serie 360 (y reconocido como tal), fue llamado Creeper, creado en 1972. Este programa emitía periódicamente en la pantalla el mensaje: «I'm a creeper... catch me if you can!» *(soy una enredadera, agárrenme si pueden)*. Para eliminar este problema se creó el primer programa antivirus denominado *Reaper* (cortadora).

Sin embargo, el término virus no se adoptaría hasta 1984, pero éstos ya existían desde antes. Sus inicios fueron en los laboratorios de *Bell Computers*. Cuatro programadores (H. Douglas Mellory, Robert Morris, Víctor Vysottsky y Ken Thompson) desarrollaron un juego llamado *Core Wars*, el cual consistía en ocupar toda la memoria RAM del equipo contrario en el menor tiempo posible.

Después de 1984, los virus han tenido una gran expansión, desde los que atacan los sectores de arranque de disquetes hasta los que se adjuntan en un correo electrónico.

Virus informáticos y Sistemas Operativos

Los virus informáticos afectan en mayor o menor medida a casi todos los sistemas más conocidos y usados en la actualidad.

Las mayores incidencias se dan en el sistema operativo Windows debido, entre otras causas, a:

- Su gran popularidad, como sistema operativo, entre los ordenadores personales, PC. Se estima que, en el 2007, un 90% de ellos usa Windows. Esta popularidad basada en la facilidad de uso sin conocimiento previo alguno, facilita la vulnerabilidad del sistema para el desarrollo de los virus, y así atacar sus puntos débiles, que por lo general son abundantes.

- Falta de seguridad en esta plataforma (situación a la que Microsoft está dando en los últimos años mayor prioridad e importancia que en el pasado). Al ser un sistema muy permisivo con la instalación de programas ajenos a éste, sin requerir ninguna autentificación por parte del usuario o pedirle algún permiso especial para ello (en los Windows basados en NT se ha mejorado, en parte, este problema).
- Software como Internet Explorer y Outlook Express, desarrollados por Microsoft e incluidos de forma predeterminada en las últimas versiones de Windows, son conocidos por ser vulnerables a los virus ya que éstos aprovechan la ventaja de que dichos programas están fuertemente integrados en el sistema operativo dando acceso completo, y prácticamente sin restricciones, a los archivos del sistema.
- La escasa formación de un número importante de usuarios de este sistema, lo que provoca que no se tomen medidas preventivas por parte de estos, ya que este sistema está dirigido de manera mayoritaria a los usuarios no expertos en Informática. Esta situación es aprovechada constantemente por los programadores de virus.

En otros sistemas operativos como Mac OS X, GNU/Linux y otros basados en Unix las incidencias y ataques son prácticamente inexistentes. Esto se debe principalmente a:

- Tradicionalmente los programadores y usuarios de sistemas basados en Unix/BSD han considerado la seguridad como una prioridad por lo que hay mayores medidas frente a virus tales como la necesidad de autenficación por parte del usuario como administrador o *root* para poder instalar cualquier programa adicional al sistema.
- Los directorios o carpetas que contienen los archivos vitales del sistema operativo cuentan con permisos especiales de acceso, por lo que no cualquier usuario o programa puede acceder fácilmente a ellos para modificarlos o borrarlos. Existe una jerarquía de permisos y accesos para los usuarios.
- Relacionado al punto anterior, a diferencia de los usuarios de Windows, la mayoría de los usuarios de sistemas basados en Unix no pueden normalmente iniciar sesiones como usuarios Administradores o por el superusuario *root*, excepto para instalar

o configurar software, dando como resultado que, incluso si un usuario no administrador ejecuta un virus o algún software malicioso, éste no dañaría completamente el sistema operativo ya que Unix limita el entorno de ejecución a un espacio o directorio reservado llamado comúnmente *home*.

- Estos sistemas, a diferencia de Windows, son usados para tareas más complejas como servidores que por lo general están fuertemente protegidos, razón que los hace menos atractivos para un desarrollo de virus o software malicioso.

Métodos de propagación

Existen dos grandes clases de contagio. En la primera, el usuario, en un momento dado, ejecuta o acepta de forma inadvertida la instalación del virus. En la segunda, el programa malicioso actúa replicándose a través de las redes. En este caso se habla de gusanos.

En cualquiera de los dos casos, el sistema operativo infectado comienza a sufrir una serie de comportamientos anómalos o imprevistos. Dichos comportamientos pueden dar una pista del problema y permitir la recuperación del mismo.

Dentro de las contaminaciones más frecuentes por interacción del usuario están las siguientes:

- Mensajes que ejecutan automáticamente programas (como el programa de correo que abre directamente un archivo adjunto).
- Ingeniería social, mensajes como *ejecute este programa y gane un premio*.
- Entrada de información en discos de otros usuarios infectados.
- Instalación de software pirata o de baja calidad.

En el sistema Windows puede darse el caso de que el ordenador pueda infectarse sin ningún tipo de intervención del usuario (versiones Windows 2000, XP y Server 2003) por virus como Blaster, Sasser y sus variantes por el simple hecho de estar la máquina conectada a una red o a Internet. Este tipo de virus aprovechan una vulnerabilidad de desbordamiento de búfer y puertos de red para infiltrarse y contagiar el equipo, causar inestabilidad en el sistema, mostrar mensajes de error,

reenviarse a otras máquinas mediante la red local o Internet y hasta reiniciar el sistema, entre otros daños. En las últimas versiones de Windows 2000, XP y Server 2003 se ha corregido este problema en su mayoría.

Métodos de protección y tipos

Los métodos para disminuir o reducir los riesgos asociados a los virus pueden ser los denominados activos o pasivos.

Activos

- **Antivirus**: los llamados programas antivirus tratan de descubrir las trazas que ha dejado un software malicioso, para detectarlo y eliminarlo, y en algunos casos contener o parar la contaminación. Tratan de tener controlado el sistema mientras funciona parando las vías conocidas de infección y notificando al usuario de posibles incidencias de seguridad.

- **Filtros de ficheros**: consiste en generar filtros de ficheros dañinos si el ordenador está conectado a una red. Estos filtros pueden usarse, por ejemplo, en el sistema de correos o usando técnicas de firewall. En general, este sistema proporciona una seguridad donde no se requiere la intervención del usuario, puede ser muy eficaz, y permitir emplear únicamente recursos de forma más selectiva.

Pasivos

- Evitar introducir a tu equipo medios de almacenamiento removibles que consideres que pudieran estar infectados con algún virus.
- No instalar software "pirata".
- Evitar descargar software de Internet.
- No abrir mensajes provenientes de una dirección electrónica desconocida.
- No aceptar e-mails de desconocidos.

- Generalmente, suelen enviar "fotos" por la Web, que dicen llamarse "mifoto.jpg", tienen un icono cuadrado blanco, con una línea azul en la parte superior. En realidad, no estamos en presencia de una foto, sino de una aplicación Windows (*.exe). Su verdadero nombre es "mifoto.jpg.exe", pero la parte final "*.exe" no la vemos porque Windows tiene deshabilitada (por defecto) la visualización de las extensiones registradas, es por eso que solo vemos "mifoto.jpg" y no "mifoto.jpg.exe". Cuando la intentamos abrir (con doble clik) en realidad estamos ejecutando el código de la misma, que corre bajo MS-DOS.

Tipos de virus e imitaciones

Existen diversos tipos de virus, varían según su función o la manera en que éste se ejecuta en nuestra computadora alterando la actividad de la misma, entre los más comunes están:

- Troyano: que consiste en robar información o alterar el sistema del hardware o en un caso extremo permite que un usuario externo pueda controlar el equipo.
- Gusano: tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.
- Bombas Lógicas o de Tiempo: son programas que se activan al producirse un acontecimiento determinado. La condición suele ser una fecha (Bombas de Tiempo), una combinación de teclas, o ciertas condiciones técnicas (Bombas Lógicas). Si no se produce la condición permanece oculto al usuario.
- Hoax: los hoax no son virus ni tienen capacidad de reproducirse por si solos. Son mensajes de contenido falso que incitan al usuario a hacer copias y enviarla a sus contactos. Suelen apelar a los sentimientos morales ("Ayuda a un niño enfermo de cáncer") o al espíritu de solidaridad ("Aviso de un nuevo virus peligrosísimo") y, en cualquier caso, tratan de aprovecharse de la falta de experiencia de los internautas novatos.

Acciones de los virus

- Unirse a un programa instalado en el ordenador permitiendo su propagación.

- Mostrar en la pantalla mensajes o imágenes humorísticas, generalmente molestas.
- Ralentizar o bloquear el ordenador.
- Destruir la información almacenada en el disco, en algunos casos vital para el sistema, que impedirá el funcionamiento del equipo.
- Reducir el espacio en el disco.

La ciberseguridad se compone de tres **fases**; prevención, localización y reacción. Durante la primera **fase**, se debe eliminar o disminuir en la medida de lo posible cualquier margen de riesgo que pueda existir.