

Internet ¿seguro?

La rápida evolución de los ordenadores, y especialmente de Internet ha provocado, junto a innumerables beneficios, la aparición de nuevas figuras delictivas. Y la pregunta es: ¿Es Internet seguro?

Los virus informáticos

Hasta 1998 el riesgo informático más frecuente era que un virus informático contaminara nuestro ordenador. Estos virus son programas dañinos que tienen la capacidad de hacer copias de si mismos, afectando a cualquier ordenador que este conectado a un ordenador infectado. Internet ha permitido a los creadores de virus intercambiar conocimientos y colecciones de virus. Por ejemplo, podemos descargar programas de generación automática de virus para crear un virus con las características que deseamos. Con herramientas de este tipo el numero de virus se ha multiplicado exponencialmente. Hoy en día existen mas de 50.000 virus diferentes y aparecen entre 600 y 800 nuevos virus cada mes.

Pero además, Internet ha conectado entre si millones de ordenadores, con lo que un virus puede propagarse muy rápidamente por Internet. El virus "Melissa" contaminó a mediados de 1999 cuatro millones de ordenadores en todo el mundo en solo tres días. El virus "I Love You" contaminó en mayo de 2000 cuarenta millones de ordenadores en solo nueve horas, ¡noventa veces mas rápido!

Los antivirus no son suficientes en la era Internet

Algo esta fallando en la forma de luchar contra los virus, y son precisamente los antivirus. Un antivirus reconoce miles de virus

• Carlos Jiménez

Director general de Secuware



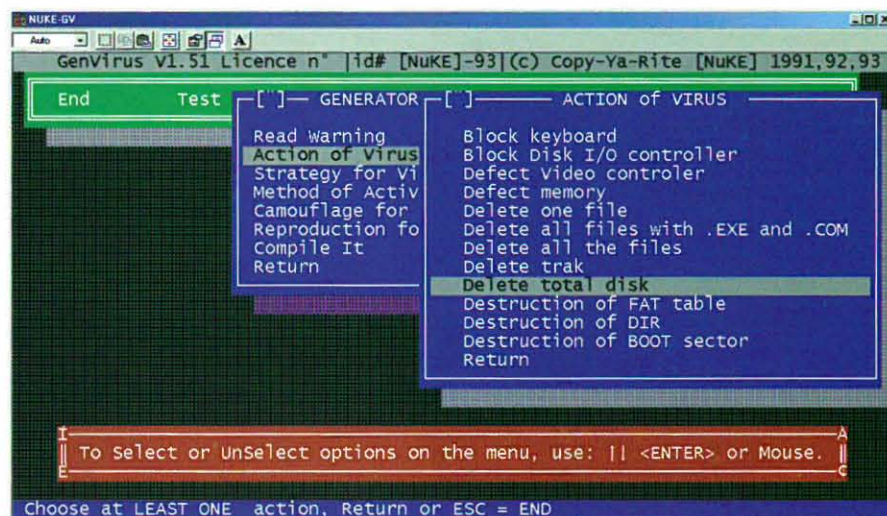
conocidos y si encuentra alguno de los que conoce lo neutraliza. Pero no sabe que hacer ante un nuevo virus. Por eso necesita actualizarse constantemente y tampoco nos protege si el virus llega antes a nuestro orde-

nador que al fabricante de antivirus. El virus "I Love You" se propagó mucho mas rápidamente del tiempo de reacción de cualquier fabricante de antivirus. Los futuros virus cuentan con mecanismos de propagación que convierten en inútiles a los antivirus.

El correo electrónico

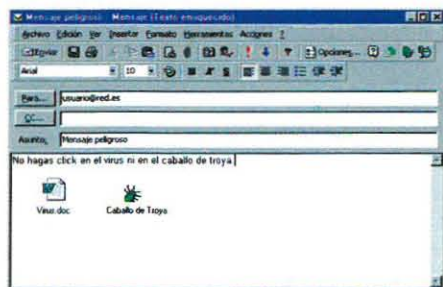
Todos utilizamos correo electrónico. Y conviene tener en cuenta algunos problemas asociados al correo electrónico:

- Falta de privacidad. Si no utilizamos cifrado, cualquiera que monitorice la red puede leer nuestros mensajes de correo.



Un programa generador de virus puede crear un virus en menos de 3 minutos.

Internet ha conectado entre sí a millones de ordenadores, con lo que un virus puede propagarse muy rápidamente



El correo electrónico es una vía de entrada frecuente para virus y caballos de Troya.

- Suplantación del remitente. Si no utilizamos firma digital, no podemos garantizar que el remitente de un mensaje es quien dice ser.
- Transmisión de virus. Nos enviamos mensajes que contienen archivos asociados que pueden contener virus o caballos de Troya. De hecho, la vía mas frecuente de contaminación por virus informáticos es recibir un correo que contiene el virus.
- Libelos por Internet. Los usuarios tendemos a creer en que la información que viene por el ordenador es tan fiable como la que vemos en el telediario. Pero esto no es así, cualquiera puede mandar un mensaje diciendo cualquier barbaridad y crear una cadena que difundirá el contenido de forma exponencial. Hace unos meses se dijo que explotaría una bomba en unos grandes

almacenes, pero mañana se podría desprestigiar a un candidato a unas elecciones generales. Por favor, no reenviéis este tipo de mensajes. Ninguno es cierto.

El control remoto de nuestro ordenador

En Internet existen caballos de Troya muy elaborados que permiten a un hacker tomar control remoto de nuestro ordenador. En el pasado BackOrifice y Netbus nos han demostrado hasta donde se puede llegar. El robo de nuestras contraseñas o la utilización de nuestro ordenador para atacar a otros ordenadores sin que nos demos cuenta son dos de los peligros de este tipo de programas.

La navegación por Internet

Cada día aparecen nuevos servicios por Internet, y nuevas empresas ofreciendo servicios hace tan solo un par de años imposibles sin la red. Es un fenómeno parecido al que se vivió en el oeste norteamericano: La fiebre del oro. Todo el mundo quiere encontrar oro en Internet. O al menos que su empresa crezca al ritmo que lo han hecho AOL, Yahoo, Amazon, entre otras. Las expectativas de negocio en los próximos años son espectaculares, ya podemos comprar o conseguir prácticamente cualquier información por Internet. Sin embargo este crecimiento acelerado y sin planificación tiene un aspecto peligroso: la seguridad ha sido uno de los aspectos mas descuidados. En los últimos años han



En Internet existen programas para robar las contraseñas de nuestro ordenador de forma remota.

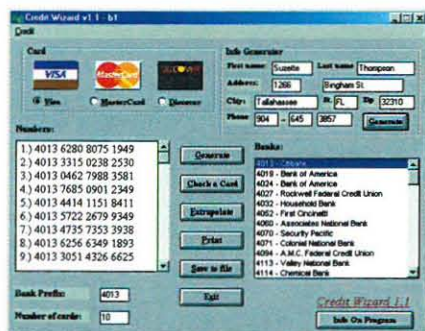
aparecido muchas vulnerabilidades que afectan a los servidores de Internet.

Denegar el servicio: consiste en dejar bloqueado el servidor de Internet que esta siendo atacado. Las perdidas económicas pueden ser enormes. Hace cuatro meses un grupo desconocido dejó bloqueados Yahoo, Amazon, y eBay entre otros. Amazon declaro que en 4 horas de inactividad, las perdidas representaban 17.000 millones de pesetas. En el mundo virtual en el que un banco no tiene oficinas, sino un servidor Web, el impacto de bloquear el servidor Web sería el mismo que el de cerrar todas las puertas de sus sucursales en el mundo físico.

Modificación de contenidos: Si capturan las contraseñas de administración o se conocen algunos trucos, es posible la modificación de las paginas Web o hacer que el DNS apunte a otra dirección IP. El resultado es que el servidor Web ya no presenta información correcta. Cada mes se vulneran unos 150 servidores en todo el mundo desde la NASA a la CIA han sufrido ataques de este tipo.

El fraude electrónico

Muchos de los modelos de negocio en Internet no tienen en cuenta que el fraude en los medios de pago en Internet no se puede acotar como se hace en el mundo físico. Y en Internet podemos encontrar pro-



Los programas de creación de tarjetas de crédito falsas aumentaran el fraude en los pagos virtuales.

gramas de generación de fraude para crear números falsos de tarjetas de crédito. Mientras que el fraude en el mundo real es menor del 10%, en Internet hay sitios de venta de música MP3 con fraudes mayores al 75%. ¡Solo dos personas de cada diez están pagando realmente!

La impunidad legal

Cualquiera de los delincuentes cibernéticos pueden ocultar su identidad de forma tan absoluta que hace imposible su localización. En el mundo físico hay huellas digitales o análisis de ADN para identificar al autor de un delito. Pero en la red solo circulan bits y son todos iguales: ceros y unos imparciales. Basta con ocultar la dirección IP de origen y ya no podremos identificar a un atacante.

Y además la red es multinacional, pero las leyes no. Hay países que carecen de legislación específica relativa al abuso informático, y sin embargo, y debido a que están conectados a Internet, pueden ser el origen de un ataque. La consecuencia es que el delito no puede ser perseguido fácilmente. El presunto creador del virus "I Love You" lo hizo en Filipinas que al carecer de legislación específica, no pudo poner a disposición judicial al autor.

La madre de todos los problemas

Todos los problemas que aparecen en este artículo y los que aparecerán en el futuro son muy pequeños en comparación con el mayor de los problemas: los usuarios no están preparados frente a estas amenazas. Cuando surge un problema se actúa de manera reactiva, nunca preventiva. Pero muchas de estas amenazas no tienen solución reactiva y la solución preventiva pasa por un cambio en los procedimientos que seguimos.

Los usuarios quieren utilizar el ordenador de la oficina con la misma libertad que lo hacen con el ordenador de su casa. Y no son conscientes de que si por negligencia se produce un fallo en la seguridad de la empresa, su propio empleo puede estar en juego. Dentro de un disquete puede

En Internet hay sitios de venta de música MP3 con fraudes mayores al 75%

circular una bomba lógica, algo preparado para que al llegar un día a una hora (por ejemplo, Viernes 13) se pierda toda la información de los ordenadores.

Se que os quedaréis intranquilos tras esta lectura, pero lo que pretendo es que al conocer los riesgos os planteéis que necesitáis cambiar la manera en la que utilizáis la informática. Quizás en un próximo artículo veamos las soluciones que el mercado ha creado y las que faltan por crear para contener estos problemas.

Más información cjimenez@secuware.com



Los cambios de paginas de servidores Web provocan importantes pérdidas y generan desconfianza en la seguridad de los servidores de Internet.