Revista Digital Universitaria
10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

ARTICULO

LA SEGURIDAD INFORMÁTICA Y EL USUARIO FINAL

Jesús Ramón Jiménez Rojas
Consultor de seguridad independiente

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

Resumen

En el presente artículo se presentan las formas en que los virus informáticos se infiltran en los sistemas de computo, la manera en que se puede prevenir de su ataque y que esta haciendo al respecto el departamento de Seguridad En Computo la Universidad Nacional Autónoma de México.

Palabras clave: el usuario final, virus informáticos, software antivirus y contraseña

Introducción

Hoy en día, la seguridad informática se ha convertido en punto crítico de las comunicaciones realizadas a través de Internet, debido al gran número de amenazas contra los datos expuestos al viajar a través de este medio. Estas amenazas se presentan en distintas formas, tienen como propósito causar el mayor daño posible a la información almacenada en los sistemas. Las principales amenazas son: los virus informáticos, los gusanos de Internet, el spyware, caballos de Troya, el pharming, el pshishing scam, ataques de negación de servicio, entre otros.
Las organizaciones están invirtiendo una gran cantidad de recursos en infraestructura que permite mantener protegidos sus activos (información sensitiva), así como también se esfuerzan en contratar personal de Tecnologías de la Información, especializados en seguridad informática, que cuenta con los conocimientos necesarios para manejar dicha infraestructura.

¿Cuál es el verdadero problema? La respuesta es simple, se ha dejado de pensar en el eslabón más débil de la cadena de la seguridad informática: el usuario final. Las organizaciones tanto privadas como gubernamentales han ignorado por completo los problemas serios que están sufriendo los usuarios que poseen un conocimiento escaso de la seguridad informática mientras sus equipos se encuentran conectados a Internet.

Los distribuidores de los distintos sistemas operativos tampoco han tomado en cuenta que el usuario final paga las consecuencias de no tener un conocimiento técnico de todos los problemas que los afectan haciendo más fácil que un atacante realice sus actividades maliciosas.

Los usuarios finales están siendo víctimas de distintos delitos cibernéticos que afectan su economía o su privacidad, como el fraude en línea o el robo de información personal como contraseñas de correo electrónico. Todo esto se debe que no se ha invertido el suficiente esfuerzo ni los recursos necesarios para generar una verdadera campaña de información que permite llevar el conocimiento de la seguridad informática al usuario "casero" de forma simple y fácil de comprender.

Principales amenazas de seguridad

Los principales problemas a los que un usuario final podría estar expuesto al momento de realizar sus actividades cotidianas en Internet son los siguientes:

Virus informáticos

Son programas que tienen por objetivo alterar el funcionamiento de la computadora y en ciertos casos alterar la información, se propagan sin el consentimiento y conocimiento del usuario. Algunos de los virus informáticos requieren de la intervención del usuario para comenzar a propagarse, es decir, no pueden activarse por sí mismos, otros no la requieren y se activan solos.

En un principio, los virus se propagaban (y aún pueden propagarse de esta manera) a través del intercambio de dispositivos de almacenamiento como disquetes, memorias de almacenamiento (USBs), etc. Hoy en día, un equipo se puede infectar al abrir un archivo adjunto (ya sean documentos, imágenes, juegos, etc.) que llegue a través de un correo electrónico.

Los virus también se distribuyen a través de mecanismos de intercambio de archivos, es decir, aquellos que se suelen utilizar para distribuir software, música, videos, etc. Algunos ejemplos de estas redes son KaZaA, eDonkey, eMule, entre otras. Están diseñados en su mayoría para afectar al sistema operativo Windows de Microsoft, aunque no son exclusivos para éste.

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

El objetivo principal de los virus informáticos es el consumo de recursos y la afectación de datos en la computadora del usuario. La manera de erradicarlos y de protegerse contra éstos, es a través de un software antivirus. Un software antivirus es de poca ayuda si no se encuentra actualizado con las firmas más recientes, por lo que se debe actualizar constantemente a través de una conexión a Internet.

Gusano de Internet

Conocido también por su término en inglés Worm, es un programa que puede propagarse por sí mismo a través de la red tomando ventaja de una falla o hueco de seguridad (una vulnerabilidad) en el sistema operativo o en el software instalado en los equipos de cómputo y que tiene como propósito realizar acciones maliciosas.

Un gusano de Internet busca propagarse lo más rápido posible tratando de infectar el mayor número posible de equipos, lo que tiene como consecuencia el colapso de las comunicaciones en Internet. Una vez que ha infectado un equipo de cómputo, modifica ciertos parámetros en el mismo con el propósito de asegurarse de iniciar su actividad maliciosa cada vez que el usuario reinicie su equipo y para detener el funcionamiento del software de seguridad instalado (como los antivirus y firewalls) con el propósito de evitar su detección.

Ya en el sistema, el gusano de Internet intenta propagase a otros equipos que presenten el mismo problema (la misma vulnerabilidad), a través de ciertas rutinas programadas en el mismo. Estas rutinas consisten en generar direcciones IP (la forma en cómo se identifican los equipos en una red) de forma aleatoria y lanzar hacia ellas el código malicioso del gusano.

Los gusanos de Internet pueden estar diseñados para realizar ciertas actividades maliciosas, por ejemplo, una vez que se han infectado un gran número de sistemas con un gusano, éstos podrían lanzar un ataque contra algún sitio Web en particular. Estos ataques podrían ser los llamados Ataques de Negación de Servicio Distribuido ó DDoS que tienen como propósito saturar los servicios de Internet proporcionados por alguna organización (servidores de correo electrónico, servidores de páginas Web, etc.).

Caballos de Troya

Es aquel programa que se hace pasar por un programa válido cuando en realidad es un programa malicioso.

Se llama troyano, caballo de Troya o trojan horse (en inglés) por la semejanza con el caballo que los griegos utilizaron para disfrazar su identidad y ganar su guerra contra la ciudad de Troya. Así, un usuario podría descargar de un sitio Web de Internet un archivo de música que en realidad es un troyano que instala en su equipo un keylogger o programa que capture todo lo que escriba el usuario desde el teclado y después esta información sea enviada a un atacante remoto. La información podría incluir números de tarjetas de crédito, claves de acceso a banca electrónica, contraseñas de correo electrónico, etc.

Spyware

También conocido como programas espía y que se refiere a aplicaciones que recopilan información sobre una persona u organización, las cuales se instalan y se ejecutan sin el conocimiento del usuario. El objetivo principal del spyware es recolectar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas.

Cuando este tipo de software es instalado en un equipo podría enviar ventanas de mensajes emergentes, redirigir el navegador de Internet (Internet Explorer, Mozilla, Opera) a ciertos sitios, o monitorear los sitios Web que son visitados. En casos extremos, algunas versiones de spyware podrían estar acompañadas de más software malicioso.

Debido al procesamiento extra que genera el spyware, el equipo de cómputo podría disminuir su rendimiento, volviéndose extremadamente lento.

Pharming

Es una modalidad utilizada por los atacantes, consiste en suplantar el Sistema de Resolución de Nombres de Dominio (DNS, Domain Name System) con el propósito de conducir al usuario a una página Web falsa.

De esta forma, cuando introduzca en el navegador de Internet un determinado nombre de dominio que haya sido redireccionado (cambiado), por ejemplo http://www.seguridad.unam.mx, se accederá a la página Web que el atacante haya especificado para ese nombre de dominio.

El cambio de dirección de las páginas Web falsas o maliciosas comúnmente se realiza a través de código malicioso, para llevarlo a cabo este cambio se requiere que el atacante logre instalar en el equipo alguna aplicación o programa malicioso (por ejemplo, un archivo ejecutable .exe, .zip, .rar, .doc, etc.). La entrada del código malicioso en el sistema puede producirse a través de distintos métodos, siendo el más común a través de un correo electrónico, aunque puede realizarse también a través de descargas por Internet ó a través de unidades de almacenamiento removibles como los USBs, etc.

Phishing Scam

Es un conjunto de técnicas y mecanismos empleados por los atacantes con el propósito de robar información personal de un usuario y poder suplantar su identidad.

Este tipo de ataque consiste en la capacidad de duplicar una página Web para hacer creer al usuario que se encuentra accediendo a la página Web original y no a una página Web falsa alojada en un servidor controlado por él. Los sitios Web que comúnmente son falsificados pueden ser el del correo electrónico, de una institución financiera, de una tienda departamental, de una institución académica, etc.

Una vez que el intruso tiene implementado el sitio Web falso en Internet, comienza a realizar el envió masivo de correos electrónicos a una gran cantidad de direcciones. Los correos electrónicos, en el tema y cuerpo del mensaje, usualmente hacen referencia a que el usuario debe acceder al sitio Web de la organización en cuestión (correo electrónico, institución financiera, tienda departamental, etc.) para realizar cambios a su información personal. Los correos electrónicos contienen la dirección Web a la cual el usuario debe acceder para realizar estos cambios.

Comúnmente, el usuario accede a la página Web falsa e introduce sus datos personales. La información que intentan obtener comúnmente a través de estos ataques de phishing scam es: el nombre de usuario (conocido como login) utilizado, por ejemplo, para acceder a su correo electrónico, la contraseña relacionada con su cuenta de correo electrónico, números de su tarjeta de crédito, claves de acceso a su banca electrónica, números de seguro social, y cualquier otra información que les permita tener acceso a servicios privados del usuario con el propósito de obtener un beneficio propio, como por ejemplo, realizar un fraude a través de banca electrónica.

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

Ingeniería social

Consiste en que un atacante utiliza la interacción humana o comúnmente conocida como habilidad social para obtener información comprometedora acerca de una organización, de una persona o de un sistema de cómputo.

Un atacante hace todo lo posible para hacerse pasar por una persona modesta y respetable, por ejemplo, pretende ser un nuevo empleado, un técnico de reparación, un investigador, etc.; el atacante podría proporcionar credenciales para sustentar esta identidad. Dependiendo de las preguntas que el atacante realice, podría ser capaz de obtener información suficiente para introducirse a la red de la organización o a un equipo de cómputo. Si el atacante no puede obtener la información suficiente de una fuente, podría contactar otra fuente de la misma organización o familia o en su defecto confiar en la información obtenida de la primera fuente.

Los ataques de Ingeniería social pueden ser realizados a través de distintos métodos: sitios Web, llamadas telefónicas, correos electrónicos, de cara a cara, etc., por lo que se debe de poner mucha atención en esta técnica de ataque y no develar información que sólo el usuario debe conocer.

Buenas prácticas de seguridad

Los usuarios finales podrían realizar las siguientes acciones para poder mitigar los principales problemas de seguridad a los que están expuestos y mejorar la seguridad de su equipo así como de la información que manejan.

Utilizar una contraseña para iniciar sesión en un equipo de cómputo.

Las contraseñas representan el mecanismo de entrada para la mayoría de los sistemas informáticos, por lo que, si mantienen una configuración poco segura, ocasionarán que los sistemas puedan caer en manos de un intruso. Para un atacante/intruso resultará fácil apoderarse de un equipo si la contraseña resulta muy sencilla y fácil de descubrir ya que utilizan distintas herramientas de seguridad para realizar ataques de diccionario o de fuerza bruta que les permiten descubrir contraseñas débiles o nulas para acceder al equipo.

Las contraseñas que se utilice deben ser complejas

No sólo es de vital importancia establecer una contraseña sino que ésta debe estar catalogada como robusta, esto quiere decir que debe cumplir con ciertas características que la hacen difícil de descifrar. A continuación se mencionan algunas de estas características:

Nunca utilizar una contraseña en blanco para iniciar sesión en un equipo.

No se debe utilizar como contraseña información personal, como un nombre o apellido, el nombre de alguna persona cercana (el nombre de la esposa(o), padres, etc.), fecha de nacimiento, etc.

No utilizar palabras que aparece en un diccionario, como por ejemplo, puma, gato, casa, mamá, papá, entre otras.

La contraseña debe tener como mínimo 8 caracteres.

Debe estar conformada por letras mayúsculas, letras minúsculas, números y caracteres no definidos como lo son: . ! @ # $ % ^ & * ( ) _ + | ~ - = \ ` { } [ ] : " ; ' < > ? , . /.

Puede asociarse una palabra que sea fácil de recordar y convertirla en una contraseña robusta. Por ejemplo, la palabra seguridad podría ser convertida a una contraseña robusta de la siguiente forma S35ur1d@d

No deben compartirse o revelarse las contraseñas

La(s) contraseña(s) que se empleen para el correo electrónico, banca electrónica, inicios de sesión en PCs, etc. deben ser confidenciales. Una contraseña robusta lo deja de ser en el momento en que alguien más la conoce.
Aún cuando se sigan al pie de la letra las indicaciones para utilizar una contraseña robusta a menudo se tiene la costumbre de no resguardar de forma correcta la información confidencial como el NIP de las tarjetas de crédito o débito, o la(s) contraseña(s) del equipo de cómputo entre otras, ya sea escribiéndola en un post-it y pegándola sobre el monitor, pizarrón, en el refrigerador o en una agenda personal (la que puede extraviarse en cualquier momento o incluso ser robada, por mencionar algunas; con lo anterior se aumenta la probabilidad de que alguien más la halle y pueda acceder a un equipo y a la información personal y confidencial, con la que no solamente pueden usar los recursos de dicho equipo; borrar o cambiar información, sino también robar o emplear el chantaje de diversas formas.

Utilizar cuentas de usuario con privilegios limitados

La mayoría de los usuarios realizan las tareas cotidianas en su equipo de cómputo con cuentas de usuario que tienen privilegios administrativos, que pueden realizar cualquier acción, lo que representa un riesgo de seguridad muy alto. Estas tareas cotidianas consisten a menudo, en navegar en Internet, redactar documentos, editar imágenes, entre otras actividades, las cuales no requieren de una cuenta de este estilo.

Las cuentas con privilegios administrativos sólo son necesarias cuando se requiere instalar programas o modificar la configuración del equipo, por lo que una excelente recomendación es que se cree una cuenta de usuario con privilegios limitados, esto evitará que, en el caso de que se sufra un ataque por parte de amenazas como spyware, troyanos, virus o algún otro tipo de código malicioso, seas afectado en menor medida, debido a que la cuenta de usuarios no tiene permisos para realizar modificaciones en el equipo. Otra razón válida para utilizar cuentas de usuario limitadas, es que con esto se asegurará de no alterar la configuración del equipo de forma accidental.

Utiliza software de seguridad en tu equipo

Para que un equipo pueda estar protegido ante las distintas amenazas con que está plagado Internet es necesario que se tenga instalado un software que evite que la información sea dañada/alterada o que el equipo pueda ser controlado de forma remota por un atacante.

Debido al cambiante mundo de la tecnología y a la enorme cantidad de amenazas informáticas que van apareciendo y esparciéndose a través de la Internet, es importante que el equipo de cómputo cuente con al menos el siguiente software de seguridad en el momento en que se estén realizando las tareas cotidianas:

Software antivirus. Proporciona protección contra una gran diversidad de código malicioso, como lo son los virus y gusanos de Internet, y que pueden dañar seriamente los recursos informáticos así como la información, además de que puede distribuirlos e infectar a terceros sin darnos cuenta.

Software antispyware. Protege contra código malicioso como el spyware, que puede extraer información del equipo si se accede a sitios Web no confiables.

Firewall personal. Es un filtro que ayuda a seleccionar el tipo de conexiones y programas que saldrán o entrarán a/o desde el equipo, evitando accesos no autorizados al mismo y a la información.

Este software mantiene protegido al equipo, ya sea mientras se navegue en Internet o aun cuando se esté desconectado. Es importante mencionar que tanto éste, como cualquier otro software, no realizarán su función si no se actualiza o configura correctamente

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

Utiliza un navegador de Internet alternativo

Normalmente para acceder a los contenidos de Internet utilizamos un navegador/explorador de Internet, que es el programa con el que vemos las páginas y con el cual podemos obtener información. En la mayoría de los equipos de cómputo que tiene instalado el Sistema Operativo Windows (que corresponde aproximadamente a un 80% del total de equipos de cómputo) se utiliza el navegador predeterminado: Internet Explorer (IE de Microsoft Corp.).

Se ha comprobado que, aunque en los últimos años se han desarrollado nuevos y diversos navegadores de Internet, como Mozilla Firefox u Opera, entre otros, Internet Explorer continúa figurando como el más utilizado, lo que lo ha convertido en un blanco fácil para los intrusos que buscan beneficiarse de sus errores de programación (comúnmente conocidos como vulnerabilidades), que en algunos casos pueden activarse con el simple hecho de que navegues en una página Web maliciosa.

Al utilizar un navegador alternativo se disminuirán las probabilidades de que un atacante tenga éxito. Es probable que al emplear otro navegador la información que se visualice no se vea de la misma forma, ya que Internet Explorer agrega características que no todos los diseñadores de páginas Web utilizan para mejorar el aspecto de los sitios, debido a que no todas se consideran como un estándar. Es importante mencionar que esto no significa que los demás navegadores de Internet no presenten errores que puedan ser aprovechados por los atacantes, por lo que si se instala un navegador diferente también deberías actualizarlo constantemente.

Instalar una barra antiphishing

Conocidas también como scam blocker, estas herramientas están disponibles para los principales navegadores de Internet como Mozilla Firefox e Internet Explorer y ayudan a identificar sitios Web fraudulentos enviando una advertencia al usuario sobre este tipo de amenazas.

A continuación se listan los principales proveedores de barras antiphishing:

Netcraft
http://toolbar.netcraft.com/

Filtro de Suplantación de Identidad (Phishing) en Microsoft Internet Explorer 7
http://www.microsoft.com/danmark/windows/ie/default.mspx#ie7security

Cloudmark Anti-Fraud Toolbar
http://www.cloudmark.com/desktop/ie/

Filtro de Phishing en Firefox 2.0
http://www.mozilla.com/en-US/firefox/phishing-protection/

Earthlink Scamblocker
http://www.earthlink.net/software/free/toolbar/

Microsoft Phishing Filter Add-in for MSN Search Toolbar
http://addins.msn.com/phishingfilter/

Ser cuidadoso al navegar en sitios públicos

Nunca se deben utilizar equipos públicos o puntos de acceso inalámbricos para transacciones financieras, mucho menos si es una red pública localizada en algún restaurante u hotel, si se realiza por este medio, se debe estar seguro de utilizar un protocolo más confiable como WPA2.

Otra buena práctica es no enviar correos electrónicos con información confidencial, esta puede ser capturada por atacantes o quedar almacenada en el equipo, tampoco se deben guardar permanentemente las contraseñas del mensajero instantáneo.

Si se utiliza algún medio de almacenamiento (como USB, discos duros externos, etc.) en un equipo público, debe analizarse con un antivirus antes de volverlo a utilizar en un equipo personal.

Actualiza el sistema operativo del equipo

Existen distintos métodos para realizar la instalación de actualizaciones de seguridad en un equipo Windows o Linux que permiten mantenerlo al día y de esta forma protegerlo contra posibles ataques de código malicioso o por parte de atacantes desde Internet.

A través de las actualizaciones automáticas se descargarán e instalarán las actualizaciones de seguridad importantes, de forma automática y de acuerdo a la programación que se defina. Las actualizaciones de descargarán de forma automática mientras te encuentres conectado a Internet. Las actualizaciones automáticas es una característica que puede activarse hoy en día en casi cualquier sistema operativo.

No abrir archivos de extraña procedencia

Una gran diversidad de virus en el Internet se propaga a través del correo electrónico, adjuntando a estos un archivo infectado con lo cual se puedan seguir propagando.

La mayoría de los virus se propagan mediante archivos con doble extensión, por ejemplo archivo.doc.exe o con extensiones que pueden ejecutar código que ponen en riesgo la seguridad del equipo.

Es recomendable no abrir los archivos que presenten una o más de las siguientes características:

Archivos con doble extensión, por ejemplo, archivo.doc.src

Archivos con extensiones .exe, .src, .vbs, .pif, por mencionar algunos.

Archivos no solicitados, por ejemplo, el recibir un archivo de alguien desconocido

No abrir archivos comprimidos con contraseña, las cuales vienen en el texto del mensaje. Se está volviendo cotidiana esta técnica con la cual las firmas antivirus son evadidas.

Archivos de correo electrónicos extraños. Es común que los virus después de contaminar usen las libretas de direcciones del equipo infectado para seguir propagándose. Al recibir un correo electrónico de un contacto de confianza lo abrimos sin generar ninguna sospecha, por lo tanto, se recomienda verificar si este correo es "normal", es decir, preguntarnos si el usuario que mando el correo nos iba a mandar información, nos escribe continuamente, es de las personas que nos manda correo para divertirnos, etc. Esto puede evitar que nos contaminemos con un virus que es enviado por alguien de confianza cuyo equipo se infectó con un código malicioso.

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

No se deben abrir correos con ligas a supuestas tarjetas virtuales o videos animados, debido a que esto podría ser una forma de introducir un virus al equipo y comprometer la seguridad del mismo.

¿Qué está siendo la UNAM al respecto?

La Dirección General de Servicios de Cómputo Académico de la Universidad Nacional Autónoma de México a través del Departamento de Seguridad en Cómputo y UNAM-CERT, pone a disposición del público el Portal de Usuario Casero.

El Portal del Usuario Casero está dirigido a todo tipo de usuario de cómputo y tiene como finalidad proporcionar de manera dinámica y sencilla las herramientas básicas para proteger sus sistemas de información, con la idea de fortalecer y extender los beneficios de la cultura informática en nuestro país.

A través de éste portal, se enseñan aquellos términos y conceptos complejos para los especialistas en seguridad informática. El usuario no técnico, aquel que utiliza su computadora para leer correo electrónico, para labores escolares, en la comunicación con sus familiares mediante diversos mecanismos como el mensajero instantáneo, telefonía por Internet y demás, podrá conocer los principales riesgos y amenazas existentes en la red, y, lo más importante, la forma de protegerse.A través de este portal, será posible jugar y aprender fácilmente los términos de seguridad y puede accederse a través de:

http://www.seguridad.unam.mx/usuario-casero

El Portal del Usuario Casero pretende llegar al usuario final, considerando que éste cuenta con conocimientos básicos de cómputo, pero no los tiene en materia de seguridad, por ende, obtendrá información para mantener su equipo protegido contra las amenazas de seguridad actuales. Además, le informará sobra las interrogantes que día a día afecta y obstaculizan nuestra labor en la sociedad del conocimiento, por lo que se explicará de manera simple las diferentes amenazas de seguridad.

El sitio Web está destinado a proporcionar información sencilla y entendible sobre problemas de seguridad actuales, permitiendo al usuario mantenerse informado y así poder aplicar soluciones al momento de enfrentarse a algún problema de seguridad.

En el Portal de Usuario Casero se encontrará una amplia variedad de opciones con las cuales interactuar, consultar información novedosa sobre seguridad, al tiempo de aprender y divertirse a través de juegos en línea, videos interactivos, tiras cómicas y una amplia línea de seguridad educativa que la UNAM trabaja día con día, para hacer accesibles y entendibles las nuevas tecnologías de información

Bibliografía

Departamento de Seguridad en Cómputo
http://www.seguridad.unam.mx/windows

Portal del Usuario Casero
http://www.seguridad.unam.mx

Diccionario de términos de seguridad en cómputo
http://www.seguridad.unam.mx/usuario-casero/secciones/diccionario.dsc

Seguridad informática para niños: Portal del Usuario Casero
http://www.seguridad.unam.mx/usuario-casero/secciones/ninos.dsc