Tema 2

martes, 25 de septiembre de 2018 09:05

Seguridad Informatica VS Seguridad de la Informacion

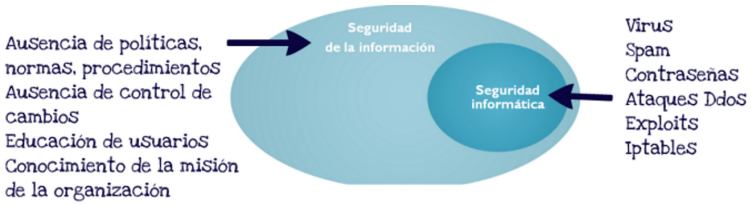
Muy a menudo se crean debates sobre los términos empleados ya que muchos provienen de otro lenguaje, como sabes no siempre las traducciones meramente de palabras son exactas. Por tal razón se tiene que tomar en cuenta el sentido de la palabra y el contexto.

Aunque, en algún momento podemos usar los términos de manera errada, debemos de tener en cuenta que no son los mismo.

La **Seguridad de la Informática** se le atribuye a una visión más general donde participa todas las áreas de negocios, desde la gerencia hasta los empleados de menor nivel y en muchos de los casos necesita ser impulsada desde los niveles superiores de mando.

Como bien hemos resaltado de que este término es más amplio, evalúa todos los riesgos de negocios incluye no solo las vulnerabilidades y un aspecto de las amenazas, sino el conjunto de los factores que determinan tales riesgo: activos, vulnerabilidades y amenazas.

En cambio la Seguridad Informática se relaciona más a los controles empleados para proteger la información de manera electrónica.



Piense como Hacker

Gran mayoría de los expertos en seguridad de la información tienen bien claro que en todos los casos se debe de pensar como quien puede perpetrar el ataque para detenerlo o incluso realizar pruebas de penetración o testeo que aseguren los sistemas y verifiquen que los controles son efectivos a la hora de contener algún ataque.

Si bien es cierto que como responsables de la seguridad informática se debe mantener un constante seguimiento a las actividades de los hackers y los nuevos métodos utilizados, es de mucha ayuda inscribirse en los foro de seguridad, hackers, listas de correos de los fabricantes para recibir información de los productos y nuevos parchos, las páginas dedicadas a proveer informaciones sobre vulnerabilidades etc.

Si nos preguntamos porque algunas personas se vuelven Hackers, no todos responderán de la misma forma, en muchos casos lo hacen por ego, por juego o incluso que hacer daño, hay otros por codicia o simplemente por una causa en común.

Ahora considere esto: no todos los piratas informáticos son maliciosos. **Hay diferentes tipos de piratas informáticos**, pero algunos de los etiquetas comunes incluyen lo siguiente:

White hats (Sombrero blanco): Este tipo de persona no es maliciosa ni intenta hacer daño a los sistemas, en su mayoría son personas del área de TI que hacen pruebas a los sistemas antes de la puesta en producción o algún consultor experto en seguridad contratado para realizar algunas tareas de mejora o testeo.

Black hats (Sombrero negro): Este tipo de persona es maliciosa e intenta entrar en computadoras y redes sin autorización. Mayormente son los que intentan el robo de identidad, piratería, fraude con tarjetas de créditos, etc. Las penas por este tipo de actividades son severas en todo el mundo.

Gray hats (Sombrero gris): Este tipo de persona son inexplicables, son personas sin afiliación a empresas, pero se arriesgan al infringir la ley al intentar hackear un sistema y luego lo notifica solo para hacerlo saber.

Amenazas de seguridad en los sistemas informáticos

Para combatir las diversas amenazas de seguridad que pueden ocurrir en un sistema informático, primero tenemos que clasificarlos. Entonces tenemos que definir cómo estas amenazas pueden ser entregado a la computadora de destino. Después podemos discutir cómo prevenir que ocurran esas amenazas y solucionarlos si ocurren. Empecemos con la amenaza informática más común.

El **software malicioso, o malware**, es un software diseñado para infiltrarse en un sistema informático y posiblemente dañarlo sin el conocimiento o consentimiento del usuario. El malware es un término amplio utilizado por los profesionales de la informática para incluir virus, gusanos, caballos de Troya, spyware, rootkits, adware y otros tipos de software no deseado.

Un virus es un código que se ejecuta en una computadora sin que el usuario lo sepa; infecta la computadora cuando se accede y se ejecuta el código. Para que los virus hagan el trabajo sucio, primero deben ser ejecutados por el usuario de alguna manera.

Un virus también tiene la capacidad reproductiva y puede propagar copias de sí mismo a lo largo de la computadora siempre que el usuario lo ejecute primero. Al infectar archivos a los que acceden otras computadoras, el virus también se puede propagar a esos otros sistemas.

Un **gusano (Worms)** es muy parecido a un virus, excepto que se autorreplica, mientras que un virus no.

Los **gusanos** aprovechan los agujeros de seguridad en los sistemas operativos y aplicaciones (incluidas las puertas traseras, que discutiremos más adelante). Buscan otros sistemas en la red o a través de Internet que ejecutan las mismas aplicaciones y se replican a esos otros sistemas. Con los gusanos, el usuario no necesita acceder y ejecutar el malware. Un virus necesita algún tipo de operación para llegar a donde quiere ir y necesita instrucciones explícitas para ser ejecutado, o debe ser ejecutado por el usuario. El gusano no necesita estas operaciones o instrucciones explícitas para ser ejecutado.

Los caballos de Troya, o simplemente troyanos, parecen realizar funciones deseadas pero en realidad están realizando funciones maliciosas detrás. Estos no son técnicamente virus y pueden descargarse fácilmente sin ser notados.

También se pueden transferir a una computadora a través de medios extraíbles, especialmente unidades flash USB. Un ejemplo de un troyano es un archivo que se encuentra dentro de un programa descargado, como un generador de claves (conocido como "keygen" utilizado como software pirateado) u otro ejecutable.

Si un usuario se queja de la lentitud del rendimiento del sistema y numerosas alertas del antivirus, y recientemente instaló un programa cuestionable desde Internet o desde una unidad flash USB, su computadora podría estar infectada por un troyano.

Ransomware es un tipo de malware que restringe el acceso a un sistema informático o archivos y exige que se pague un rescate. Bloquea el sistema de una o varias maneras e informa al usuario que para desbloquear la computadora y recuperar el acceso a los archivos, se debería realizar un pago a uno o varios servicios bancarios, a menudo en el extranjero.

El software espía (Spyware) es un tipo de software malicioso que se descarga involuntariamente de un sitio web o se instala junto con otro software de terceros. Por lo general, este malware recopila información sobre el usuario sin el consentimiento del usuario. El spyware podría ser tan simple como una pieza de código que registra a qué sitios web accedes, o llega hasta un programa que registra tus pulsaciones de teclas (conocidos como keyloggers).

El **adware** generalmente cae en el ámbito del spyware porque aparece publicidades basado en lo que ha aprendido de espiar al usuario.

Un **rootkit** es un tipo de software diseñado para obtener el control de nivel de administrador sobre un sistema informático sin ser detectado. El término es una combinación de las palabras "Root" (es decir, el usuario raíz en un sistema Unix / Linux o administrador en una Windows) y "kit" (es decir, kit de software).

Por lo general, el objetivo de un rootkit es realizar operaciones maliciosas en una computadora de destino en una fecha posterior, sin el conocimiento de los administradores o usuarios de esa computadora.

El **correo no deseado (Spam)** es el abuso de los sistemas de mensajería electrónica, como el correo electrónico, los mensajes de texto, las redes sociales, los medios de difusión, la mensajería instantánea, etc.

Los **spammers** envían mensajes masivos no solicitados indiscriminadamente, generalmente sin beneficio para el spammer real, porque la mayoría del spam se desvía o se ignora. Las empresas con ética cuestionable aprueban este tipo de marketing (generalmente configurado como un esquema de pirámide) para que las personas en la parte superior de la cadena de comercialización puedan beneficiarse; sin embargo, generalmente no vale la pena para la persona real que envía correo no deseado.

Puertas traseras: Usadas para garantizar el acceso remoto a un sistema.

Keyloggers: Registran todas las pulsaciones del teclado y las envían a un servidor remoto.

Proxy: Establecer un proxy entre la víctima y el pirata informático para filtrar todo el tráfico y redirigir determinadas webs.

Password Stealer: Se centran en el robo de contraseñas, especialmente de correo electrónico y bancarias.

Bancarios: Se centran en el robo de credenciales y datos bancarios como cuentas, tarjetas, etc.

Botnets: Estos troyanos crean una «red zombie» que es utilizada por el pirata informático para diferentes tareas, por ejemplo, ataques DDOS.

Downloaders: Son troyanos utilizados para descargar principalmente otras piezas de malware para infectar a los usuarios.

Exploits: Estas aplicaciones maliciosas se centran en explotar vulnerabilidades de programas conocidas. Llegan a los usuarios a través de internet y, al ejecutarse, buscan el programa vulnerable y utilizan dicha vulnerabilidad para su propia función, por ejemplo, para descargar una pieza de malware más compleja de forma oculta al usuario.

Rogue / Falsos antivirus: Los falsos antivirus son aplicaciones maliciosas que se hacen pasar, como su nombre indica, por antivirus y que muestran mensajes falsos sobre virus que el usuario tiene en su sistema.

Para eliminar dichos virus la víctima debe pagar una cantidad de dinero, en teoría, por una licencia y posteriormente el programa no hace nada más que seguir molestando al usuario y pidiendo dinero para mantener un sistema seguro.

Crack: Además de referirse a hackers con malas intenciones, son programas que monitorean las contraseñas en las aplicaciones de la máquina. Se conocen también como ladrones de contraseñas.

Rabbit: Reciben este nombre algunos gusanos informáticos, cuyos códigos malignos llenan el disco duro con sus reproducciones en muy poco tiempo y que también pueden saturar el ancho de banda de una red rápidamente.

Botnet: (Redes de Zombies). Los bots son propagados a través de Internet utilizando a un gusano como transporte, envíos masivos de ellos mediante correo electrónico o aprovechando vulnerabilidades en navegadores. Una vez que se logra una gran cantidad de sistemas infectados mediante Troyanos, se forman amplias redes que "trabajan" para el creador del programa. Aquí hay que destacar tres puntos importantes:
a) Este trabajo en red se beneficia del principio de "computación distribuida" que dice miles de sistemas funcionando juntos tienen una mayor capacidad de procesamiento que cualquier sistema aislado.
b) El creador del programa puede ser una red de delincuencia que ha armado su ataque, y que tienen estos programas trabajando en su beneficio.
c) El grupo "propietario de la red" de zombies puede alquilar a otros grupos su red para realizar alguna acción ilegal. El objetivo de las redes zombies puede ser realizar ataques de DDoS, distribución de SPAM, etc.

Bot: Es un programa robot, que se encarga de realizar funciones rutinarias, pero que también creaban cuentas en los diferentes sitios que otorgan e-mail gratuitos, para con estas cuentas realizar daños. También son programas que a través de órdenes enviadas desde otra computadora controlan el equipo personal de quien quieren afectar, es decir robotizándola.

Una **bomba lógica** es una parte de un código insertado intencionalmente en un programa informático que permanece oculto hasta cumplirse una o más condiciones preprogramadas, en ese momento se ejecuta una acción maliciosa. Por ejemplo, un programador puede ocultar una pieza de código que comience a borrar archivos cuando sea despedido de la compañía (en un disparador de base de datos, es decir, un trigger; que se dispare al cambiar la condición de trabajador activo del programador).

Zombi es la denominación asignada a computadores personales que, tras haber sido infectados por algún tipo de malware, pueden ser usados por una tercera persona para ejecutar actividades hostiles. Este uso se produce sin la autorización o el conocimiento del usuario del equipo. El nombre procede de los zombis o muertos vivientes esclavizados, figuras legendarias surgidas de los cultos vudú.

Botnets y Zombies

El malware puede ser distribuido a través de Internet por un grupo de computadoras comprometidas, conocido como **botnet**, y controlado por una computadora maestra (donde reside el atacante). Las computadoras comprometidas individuales en la botnet se llaman **zombies**.

Esto se debe a que desconocen el malware que se ha instalado en ellos. Esto puede ocurrir de varias maneras, incluida la distribución automática del malware de una computadora zombie a otra. Ahora imagine si todas las computadoras zombie tenían un virus específico u otro tipo de ataque cargado, y también se instaló una bomba lógica, lista para activar el malware en un momento específico. Si esto se hiciera en cientos o miles de computadoras, se podría implementar un ataque sincronizado de grandes proporciones en casi cualquier objetivo. A menudo, esto se conoce como ataque de denegación de servicio distribuido o DDoS, y generalmente se perpetúa en un servidor particularmente popular, que atiende muchas solicitudes. Si una computadora en su red está continuamente escaneando otros sistemas en la red, se está comunicando con un servidor IRC desconocido u otro servidor maestro desconocido, y / o tiene cientos de conexiones salientes a varios sitios web, es probable que la computadora sea parte de una botnet.

Este tipo de amenazas son contenidas con los firewall, permitiendo los puertos necesarios tanto de salida o de entrada de paquetes.

Intercepción activa

La interceptación activa normalmente incluye una computadora colocada entre el remitente y el receptor en un esfuerzo por capturar y posiblemente modificar la información. Si una persona puede espiar en la sesión de datos de su computadora, entonces esa información puede ser robada, modificada, o explotado de otras maneras. Ejemplos de esto incluyen robo de sesión y "man-in-the-" ataques medios (MITM).

Escalada de privilegios

La escalada de privilegios es el acto de explotar un error o error de diseño en un software o aplicación para obtener acceso a los recursos que normalmente se hubieran protegido de una aplicación o usuario. Esto da como resultado que el usuario gane privilegios adicionales, más de lo previsto originalmente por el desarrollador de la aplicación; para ejemplo, si un usuario regular gana control administrativo, o si un usuario en particular puede leer el correo electrónico de otro usuario sin autorización.

Se previene con los anti-rootkit.

Puertas traseras (Backdoors)

Las puertas traseras se utilizan en programas informáticos para eludir la autenticación normal y otros mecanismos de seguridad en su lugar. Originalmente, las puertas traseras fueron utilizadas por los desarrolladores como una funcion legítima de acceder a una aplicación, pero poco después fue implementado por atacantes que usarían puertas traseras para realizar cambios en los sistemas operativos, sitios web y dispositivos de red. O el atacante crearía una aplicación completamente nueva que actuaría como puerta trasera, por ejemplo, Back Orifice, que permite a un usuario controlar una computadora con Windows desde una ubicación remota. A menudo, es instalado a través de un caballo de Troya; este en particular se conoce como un troyano de acceso remoto, o RAT, como se mencionó anteriormente. Algunos gusanos instalan puertas traseras en las computadoras para que los spammers remotos puedan enviar correo electrónico no deseado desde las computadoras infectadas.

Bombas Lógicas

Una bomba lógica es un código que, que de alguna manera, se ha insertado en el software; está destinado a iniciar uno de muchos tipos de funciones maliciosas cuando se cumplen los criterios específicos.

Las bombas lógicas estan la línea entre el malware y un sistema de entrega de malware. De hecho, son programas no deseados, pero están destinados a activar virus, gusanos o troyanos en un momento específico. Los troyanos lanzados en una fecha determinada también se conocen como bombas de tiempo. La bomba lógica sigue el ritmo hasta que se cumplan la hora, la fecha y otros parámetros correctos.

Formas de envió software malicioso

El malware no es sensible (... todavía no) y no puede aparecer de la nada; necesita ser transportado y entregado a una computadora o instalado en un sistema informático de alguna manera. Esto se puede hacer de varias maneras.

La forma más simple sería para el atacantes es obtener acceso físico a una computadora desprotegida y realizar su trabajo malicioso localmente, Pero debido a que puede ser difícil obtener acceso físico, esto se puede hacer de varias otras formas, Algunos de los métodos enumerados a continuación también pueden ser utilizados por un atacante para simplemente obtener acceso a una computadora, realizar modificaciones, etc., además de entregar el malware.

El método que utiliza una amenaza para acceder a un objetivo se conoce como un vector de amenaza. Colectivamente, los medios por los cuales un atacante obtiene acceso a una computadora para entregar software malicioso se conocen como un vector de ataque. Probablemente el vector de ataque más común sea a través del software.

A través de software, mensajería y medios (CD, USB, Etc.)

El malware se puede entregar a través de software de muchas maneras diferentes. Una persona que envía un archivo comprimido por correo electrónico puede que ni siquiera sepa que el malware también existe en ese archivo. Los destinatarios del correo electrónico no tendrán idea de que existe malware adicional a menos que tengan un software para escanear sus archivos adjuntos de correo electrónico.

El malware también se puede entregar a través de FTP. Debido a que los servidores FTP son intrínsecamente inseguros, es más fácil de lo que piensas cargar archivos malicioso y otro software.

El malware a menudo se encuentra en redes P2P y torrents. Se debe tener mucho cuidado por los usuarios que usan estas tecnologías.

El malware también puede ser incorporado y distribuido por sitios web mediante el uso de código corrupto o descargas malas.

El malware incluso puede ser distribuido por publicidades.

Y, por supuesto, los medios extraíbles también pueden victimizar a una computadora. Los discos ópticos y las unidades flash USB se pueden manipular fácilmente para ejecutar malware automáticamente cuando se insertan en la computadora. (¡Aquí es cuando AutoRun no es tu amigo!) Los medios extraíbles también podrían tener virus o gusanos ocultos y posiblemente bombas lógicas configuradas para desactivar el malware en momentos específicos.

Prevención y solución de problemas de malware

Ahora que conocemos los tipos de malware y las formas en que estos pueden infectar una computadora, hablemos de cómo detenerlos antes de que sucedan, y cómo solucionarlos si suceden. Desafortunadamente, esto puede ocurrir.

Si un sistema se ve afectado por un malware, puede demorarse en verse o puede mostrar ventanas emergentes no deseadas y páginas de inicio incorrectas; o aplicaciones (y tal vez incluso todo el sistema) podría bloquearse o apagarse inesperadamente. A menudo, los usos de CPU de los malware y los recursos de memoria directamente o indirectos, puede hacer que el sistema sufra una degradación. En general, un técnico debe buscar un comportamiento errático desde el Computadora, como si tuviera una mente propia! Revisemos virus y spyware, miremos cómo prevenirlos, y finalmente discutir cómo solucionarlos si ocurren.

Prevención y solución de problemas de virus, trojanos y gusanos

Podemos hacer varias cosas para proteger un sistema informático de virus. Primero, cada la computadora debe tener software antivirus ejecutándose en ella. Kaspersky, McAfee, y Norton son ejemplos de fabricantes de software antivirus (AV), pero hay muchos otros, además de los fabricantes de sistemas operativos, a menudo incluyen software AV
con el sistema operativo u ofrecer descargas gratuitas. En segundo lugar, el software AV debe actualizarse, lo que significa que el software requiere una licencia actual; esto se renueva anualmente con la mayoría de los proveedores. Al actualizar, asegúrese de actualizar el motor AV y las definiciones Si lo estás haciendo manualmente. De lo contrario, configura el software AV para actualizar automáticamente a intervalos periódicos, por ejemplo, todos los días o todas las semanas. Es una buena idea programar análisis completos regulares del sistema dentro del software AV.

Mientras las definiciones se hayan actualizado, los sistemas antivirus generalmente ubican virus junto con otros programas maliciosos como gusanos y troyanos. Sin embargo, estos sistemas generalmente No ubican bombas lógicas, rootkits y actividad de botnets. AV es importante, pero no es una panacea.

A continuación, tenemos que asegurarnos de que la computadora tenga los últimos paquetes de servicio y actualizaciones disponibles. Esto va para el sistema

operativo y aplicaciones como Microsoft Office. Las puertas traseras en sistemas operativos y otras aplicaciones no son poco común, y los fabricantes de sistemas operativos a menudo publican correcciones para estas violaciones de seguridad. Windows ofrece el programa de actualización de Windows. Esto debería estar habilitado, y debe verificar las actualizaciones periódicamente o configurar el sistema para verificar actualizaciones automáticamente. Puede ser que su organización tenga reglas que gobiernan las funciones de actualización de Windows. Si es así, configure Actualizaciones automáticas de acuerdo con su política de la empresa.

Por ejemplo:

Windows 7 puede verificar si su computadora está actualizado yendo a Inicio> Todos los programas> Windows Update.
Lunix (Ubuntu, Centos) puede verificar si su computadora esta actualizada ejecutando desde la lineas de comandos, apt update o yum update.

También es importante asegurarse de que haya un firewall disponible, habilitado y actualizado. El firewall cierra todos los puertos de entrada a su computadora (o red) en un intento de Bloquear intrusos. Por ejemplo, el Firewall de Windows (disponible en el Panel de control) es una función incorporada basada en software incluida en la mayoría de las versiones de Windows. Mas en Linux se cuenta con iptables o SELinux.

Aquí hay algunos síntomas típicos de los virus:

■ La computadora funciona más lento de lo normal.
■ La computadora se bloquea con frecuencia o deja de responder por completo.
■ La computadora se reinicia por sí sola o se bloquea con frecuencia.
■ Los discos duros, la unidad óptica y las aplicaciones no son accesibles o no funcionan correctamente.
■Se producen sonidos extraños.
■ Recibe mensajes de error inusuales.
■ Se produce distorsión de visualización o de impresión.
■ Aparecen nuevos íconos o desaparecen íconos (y aplicaciones) antiguos.
■ Hay una extensión doble en un archivo adjunto a un correo electrónico que se abrió; para Ejemplo: .txt.vbs o .txt.exe.
■ Los programas antivirus no se ejecutarán o no podrán instalarse.
■ Los archivos se han dañado o las carpetas se crean automáticamente.
■ Las capacidades de restauración del sistema se eliminan o deshabilitan.

Prevención y solución de problemas de spyware

La prevención del software espía funciona de la misma manera que la prevención de virus cuando se trata de actualizar el sistema operativo y usar un firewall. Además, porque el spyware es tan común como los virus, las compañías antivirus y los fabricantes de sistemas operativos agregan antispyware.

Aquí hay algunas cosas más que puede hacer para proteja su computadora con la esperanza de spyware:
■ Use (o descargue) y actualice los programas anti-spyware incorporados, como Windows Defender o Microsoft Security Essentials. Asegúrate de mantener el antispyware actualizado.

■ Ajustar la configuración de seguridad del navegador web. Por ejemplo, deshabilitar (o limitar) las cookies, cree y configure zonas de confianza, active los filtros de phishing, restrinja los sitios web no deseados, active la comprobación automática de sitios web, desactive los scripts (como Java-Script y ActiveX), y haga que el navegador borre toda la memoria caché al salir.

■ Desinstale las aplicaciones innecesarias y desactive los servicios superfluos (por ejemplo, Servicios de escritorio remoto o FTP si no se utilizan).

■ Educar a los usuarios sobre cómo navegar la web de forma segura. La educación del usuario es en realidad ¡El método número uno para prevenir el malware!

Prevención y solución de problemas de rootkits

Un rootkit instalado con éxito permite a los usuarios no autorizados obtener acceso a un sistema y actuar como usuario root o administrador. Los rootkits se copian a una computadora como un archivo binario; Este archivo binario puede ser detectado por firmas y heurísticas.

Programas que Se pueden usar para detectar rootkits que incluyen lo siguiente:

■ GMER: http://www.gmer.net/
■ TDSSKiller: http://support.kaspersky.com/viruses/disinfection/5350
■ Revelador de rootkit de Microsoft Sysinternals: http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx (para mayores Sistemas de Windows)
■ chkrootkit: www.chkrootkit.org/ (para sistemas Linux / OS X)