MANUAL DE SEGURIDAD DE USUARIOS

Categoría de este documento.

Este documento es un anteproyecto de INTERNET. Los anteproyectos de INTERNET son documentos de trabajo de Internet Engineering Task Force (IETF), sus áreas y sus grupos de trabajo. Note que otros grupos pueden también distribuir documentos de trabajo como anteproyectos de INTERNET.

Los anteproyectos de INTERNET son documentos borradores validos para un máximo de 6 meses y pueden ser actualizados, reemplazados o quedar obsoletos por otros documentos en cualquier momento. Es inapropiado su uso como material de referencia o cita de otra forma que no sea como trabajo en desarrollo.

Para conocer el estado actual de cualquier anteproyecto de INTERNET se puede consultar el listado "lid-abstracts.txt" contenido en el Directorio Internet-Drafts Shadow en ftp.ietf.org (Costa este EU) o nic.nordu.net (Europa) o ftp.isi.edu (Costa oeste EU).

Sumario.

El Manual de Seguridad de Usuarios es el complemento del Manual de Seguridad de Sitios (Site Security Handbook). Está dirigido a proporcionar a los usuarios la información que necesitan para mantener la seguridad de sus redes y sistemas.

Nota:

Este documento ha sido traducido y revisado tratando de respetar al máximo posible la redacción de los autores, no obstante en algunos casos se han adecuado algunas expresiones y términos a formas con las cuales nuestro país está más familiarizado, con vistas a lograr una mayor comprensión.

Departamento de Seguridad Informática
Dirección de Protección, MININT

Tabla de Contenido

Primera Parte: Introducción.

Este documento ha tenido la intención de proporcionar a los usuarios finales de redes y sistemas de computadoras una guía sobre qué ellos pueden hacer para guardar sus datos y comunicaciones privadas y sus sistemas y redes seguras. La primera y segunda parte de este documento se refiere a "usuarios corporativos" en pequeñas, medias y grandes corporaciones o sitios académicos. La tercera parte está dirigida a usuarios que administran sus propias computadoras.

Los administradores de redes y sistemas pueden usar este documento como fundamentación de las normas de seguridad de usuarios de un sitio específico, sin embargo debe ser consultado primero el Manual de Seguridad de Sitios (RFC 2196).

Se incluye como apéndice al final de este documento un glosario de términos que introduce nociones de seguridad de redes de cómputo para aquellos que no estén familiarizados con ellos.

1. Léame.

Antes de conectarse a Internet debe obtenerse la política de seguridad del sitio que se va a utilizar como proveedor y leerla. Una política de seguridad es el establecimiento formal de las reglas a que los usuarios que tienen acceso a los activos de información y tecnologías de un sitio deben atenerse. Como usuario usted está obligado a seguir la política creada por los dirigentes y administradores de su sitio.

Una política de seguridad existe para proteger el hardware, el software y los datos de un sitio. Ella explica cuales son los objetivos de la seguridad de un sitio, que pueden y que no pueden hacer los usuarios, que hacer cuando surge un problema de seguridad y quien debe ser contactado y generalmente informa a los usuarios cuales son las "reglas del juego".

2. Los cables tienen oídos.

Es algo más fácil escuchar furtivamente una comunicación sobre redes de datos que una conversación telefónica. Cualquier enlace entre computadoras puede potencialmente ser inseguro, tal como lo puede ser cualquiera de las computadoras a través de las cuales fluyen los datos. Toda la información que pasa por las redes puede ser escuchada furtivamente.

La información que pasa por una red puede ser leída no solo por aquellos a quien va dirigida, sino también por otros. Esto puede suceder con el correo personal y con la información sensible que es accesada mediante la transferencia de ficheros o el Web. Por favor vea las secciones "Navegación Segura en el Web" (3.2) y "Trampas del Correo Electrónico" (3.3) para información específica sobre la protección de su privacidad.

Como usuario, su mayor preocupación debe ser, en primer lugar, protegerse contra la divulgación de su(s) cuenta(s) de computadora y en segundo lugar proteger su privacidad.

A menos que se tomen las debidas precauciones, cada vez que usted se conecte en una red, a cualquiera de los servicios que ésta ofrece, su contraseña o información confidencial puede ser robada. Esto puede entonces ser usado para ganar acceso ilícito al sistema que usted ha accesado. En algunos casos las consecuencias son obvias: Si alguien gana acceso a su cuenta bancaria usted podrá descubrir por sí mismo la pérdida de algún dinero, rápidamente. Lo que no es tan obvio es que aquellos servicios que no son de naturaleza financiera pueden también ser abusados, alcanzando un alto costo. ¡Usted debe sentirse responsable si su cuenta ha sido obtenida por otra persona!

Muchos servicios de redes implican conexiones remotas. En estos casos al usuario se le solicita su identificación y contraseña. Si esta información es enviada a través de la red sin cifrar, el mensaje puede ser interceptado y leído por otros. Esto no es realmente un gran problema cuando usted está conectado mediante un servicio de discado (dial-in), en el cual hace una llamada telefónica y se conecta, debido a

que las líneas telefónicas son más difíciles de escuchar furtivamente que las comunicaciones de Internet.

El mayor riesgo aparece cuando se usan programas para conectarse en una red. Muchos de los programas más populares que son utilizados para conectarse a servicios o para transferir ficheros (tales como telnet y ftp respectivamente) envían su nombre y contraseña y a continuación los datos sin ningún tipo de cifrado.

La precaución que normalmente es tomada contra la escucha furtiva de contraseñas por grandes instituciones es la utilización de sistemas de contraseñas desechables (de una sola vez – one time passwords). Hasta hace poco tiempo esto resultaba muy caro y complicado para pequeñas empresas y sistemas particulares, sin embargo el incremento del número de productos lo ha hecho posible sin el empleo de algún hardware extraordinario, usando técnicas de cifrado. Un ejemplo de tales técnicas es "Secure Shell" (SSH), que está gratis y comercialmente disponible para diferentes plataformas. Muchos productos (incluyendo SSH) también permiten cifrar los datos antes de ser enviados a través de la red.

Segunda Parte: Usuarios finales en redes administradas centralmente.
Las siguientes reglas básicas proporcionan un sumario de los más importantes aspectos discutidos en la segunda parte de este documento:

- Conozca quien es su punto de contacto de seguridad.
- Conserve secretas las contraseñas.
- Use un protector de pantalla con contraseña o desconéctese de la red cuando abandone su puesto de trabajo.
- No brinde a nadie acceso físico a su computadora o a su red.
- Conozca que software está corriendo y sea muy cauteloso con el software de origen desconocido. Piense detenidamente antes de ejecutar un software descargado.
- No cree pánico. Consulte su punto de contacto de seguridad si es posible antes de difundir alarma.
- Reporte los problemas de seguridad tan pronto como sea posible a su punto de contacto.

3. ¡Mire hacia fuera!

3.1 El peligro de descargar (downloading)

Una abundancia creciente de software gratis está siendo disponible en Internet. Mientras este excitante desarrollo es uno de los aspectos más atractivos del uso público de redes, se debe mostrar suma cautela. Algunos ficheros pueden ser peligrosos. La descarga de ficheros parece ser el mayor riesgo.

Asegúrese de guardar todos los ficheros descargados de forma que pueda recordar su origen. No confunda, por ejemplo, un programa descargado con un programa común por el hecho de que tengan el mismo nombre.

Los programas pueden usar la red sin que usted se percate de ello. Algo para tener en mente es que si una computadora está conectada, cualquier programa tiene la capacidad de usar la red, con o sin conocimiento suyo. Por ejemplo:

¡Usted descarga un programa de juego de un servidor de ficheros anónimos y lo ejecuta!. Así aparece en pantalla el juego en cuestión, pero sin que usted sé de cuenta éste transfiere todos sus ficheros, uno a uno, a través de Internet hacia la máquina de un cracker!

Muchos ambientes corporativos prohiben explícitamente la descarga y corrida de software de Internet.

3.2 Navegación Segura en el Web.

El mayor riesgo al navegar por Internet es la descarga de ficheros. Los navegadores permiten "bajar" cualquier fichero de Internet. Vea "El peligro de descargar" (3.1).

Los navegadores pueden estar descargando ficheros aún cuando esto no es totalmente obvio. Así, el riesgo de ficheros descargados puede estar presente aún si usted no lo está haciendo abiertamente. Cualquier fichero que usted tenga cargado en la red debe ser considerado peligroso (incluso aquellos que están en el caché del navegador). No lo ejecute por accidente, ya que pueden ser programas maliciosos. (recuerde que los programas son también ficheros. Se puede creer que se ha descargado un fichero texto, cuando de hecho este fue un "Caballo de Troya", un script, etc.).

Los navegadores pueden descargar y ejecutar programas en su nombre. Usted puede deshabilitar esta posibilidad. Si la desactiva asegúrese que entiende las consecuencias. Debe leer la guía de seguridad que acompaña a su navegador Web tanto como la política de seguridad de su compañía. Usted debe conocer que programas descargados pueden representar un riesgo al ejecutarse en su máquina. (Vea "A fin de cuentas, "¿qué programa es este?").

Las páginas Web frecuentemente incluyen formularios. Sepa que, al igual que en el correo electrónico, los datos enviados desde un navegador Web a un servidor Web no están seguros. Algunos mecanismos han sido creados para prevenir esto, más notablemente el Secure Sockets Layer (SSL). Esta facilidad ha sido incorporada a muchos navegadores. El cifra los mensajes que se envían entre el navegador Web del usuario y el servidor Web de forma que nadie en el camino puede leerlos.

3.3 Trampas del Correo Electrónico.

A los mensajes recibidos por la vía del correo electrónico se aplican todas las afectaciones normales relativas a los mensajes recibidos por cualquier otra vía. Por ejemplo, el remitente puede no ser quien dice ser. Si no se emplea un software de seguridad para el correo electrónico

es muy difícil determinar con seguridad quien envió el mensaje. Esto significa que el correo electrónico no es una vía conveniente para conducir muchos tipos de negocios. Es muy simple falsear un mensaje de correo electrónico para hacer aparecer que proviene de cualquier otra persona.

Otro aspecto de seguridad que debe ser considerado al usar el correo electrónico es la privacidad. Los mensajes pasan a través de Internet de computadora a computadora. Como los mensajes se mueven entre computadoras y se colocan en un buzón de usuario para ser leídos, son potencialmente visibles por otros. Por esta razón es sabio pensar dos veces antes de enviar información confidencial o estrictamente personal por el correo electrónico. No deben ser enviados nunca números de tarjetas de créditos ni otros datos sensibles a través de correo electrónico no protegido. (Refiérase a "Los cables tienen oídos").

Para enfrentar este problema hay programas disponibles, algunos de los cuales están integrados a los paquetes de correo electrónico.

Un servicio que le gusta mucho utilizar a los usuarios de correo electrónico es el despachador (forwarding) de correo. Este debe ser utilizado muy cautelosamente. Imagine el siguiente escenario:

Un usuario tiene una cuenta con un proveedor privado de servicios de Internet y desea recibir todo su correo allí. El convenia que se despache su correo de trabajo a su dirección particular. Todo los mensajes que recibirá en el trabajo serán transferidos a través de Internet hasta encontrar su cuenta particular. En todo este trayecto los mensajes son vulnerables para ser leídos. Un correo sensible enviado a su trabajo puede ser leído por un curioso (snoop) de la red en cualquiera de las muchas etapas del camino recorrido a través de Internet.

Observe que el correo enviado o recibido en su trabajo no debe ser privado. Verifique que su empleador, como empleador puede (en algunos casos) legalmente leer su correo y hacer uso de él. El estatus legal del correo electrónico depende de las leyes de protección de la información establecidas en cada país.

Muchos programas de correo permiten incluir ficheros en los mensajes. Los ficheros que van con el correo son ficheros iguales que cualquier otro. Cualquier forma en que un fichero pueda llegar a una computadora es un posible peligro. Si el fichero anexado es simplemente un texto, perfecto, sin embargo él puede ser más que un texto. Si el fichero anexado es en sí mismo un programa o un script ejecutable, deben ser aplicadas precauciones extremas antes de correrlo. (Vea la sección "El peligro de descargar").

3.4 Contraseñas.

Las contraseñas pueden ser fácilmente adivinadas por un intruso a menos que se tomen las debidas precauciones. Las contraseñas deben estar formadas por una mezcla de números, letras mayúsculas y minúsculas y signos de puntuación. Hay que evitar el empleo de palabras reales o combinaciones de palabras en cualquier idioma, números de matriculas de autos, nombres y así sucesivamente. La mejor contraseña es una secuencia artificial (por ejemplo un acrónimo de una frase que usted no olvidará) tal como "2B*Rnot2B" (To be or not to be) pero por supuesto ¡no utilice ésta contraseña!.

Resista la tentación de escribir su contraseña y si lo hace, consérvela con usted hasta que la memorice y entonces destrúyala. Nunca deje una contraseña pegada a un terminal o escrita en una mesa. Usted debe tener diferentes contraseñas para diferentes cuentas, pero no tantas que no pueda recordarlas. Debe cambiar sus contraseñas periódicamente.

Nunca debe salvar sus contraseñas en scripts o procedimientos de conexión ya que pueden ser usadas por cualquiera que tenga acceso a su máquina.

Asegúrese de que realmente se ha conectado con su sistema. El solo hecho de que en pantalla aparezca un prompt solicitándole su contraseña no significa que usted debe introducirla. Evite solicitudes inusuales e inmediatamente repórtelas a su punto de contacto de seguridad. Si nota algo extraño durante la conexión, cambie su contraseña.

A menos que se haya tomado la precaución de cifrar su contraseña cuando ésta es enviada por la red, usted debe, si es posible, utilizar contraseñas desechables (one time passwords) cada vez que se conecte a un sistema a través de la red (algunas aplicaciones se encargan de esto por usted). Vea "Los cables tienen oídos" para más información sobre los riesgos asociados con la conexión mediante una red.

3.5 Virus y otros males.

Los virus son esencialmente partes de software no deseados que se introducen en las computadoras. Que puede hacer un virus una vez que ha entrado en su máquina depende de algunos factores: ¿Que tiene programado hacer el virus? ¿Qué parte del sistema de cómputo ha atacado el virus?

Algunos virus son "bombas de tiempo" que se activan solo cuando se da una condición determinada, tal como una cierta fecha. Otros se mantienen latentes en el sistema hasta que un determinado programa es activado. Hay aún otros que están continuamente activados, explotando cada oportunidad para hacer daño. Un virus más sutil puede simplemente modificar la configuración de un sistema y ocultarse.

Sea cauteloso acerca de que software instala en su sistema. Utilice software procedente de "fuentes confiables" si es posible. Revise la política de su sitio antes de la instalación de cualquier software: Algunos sitios solo autorizan a los administradores para instalar software a fin de evitar problemas de seguridad y de mantenimiento de sistemas.

Los sitios administrados centralmente tienen su propia política y herramientas para el tratamiento de la amenaza de los virus. Consulte la política del sitio o solicite del administrador de su sistema los procedimientos correctos para mantenerse libre de virus.

Si una herramienta de detección de virus indica que su sistema tiene un problema usted debe reportarlo. Esto debe ser notificado a los administradores de sistemas del sitio así como a las personas que usted considere que le pasaron el virus. Es importante mantener la calma. Un susto por virus puede causar más retraso y confusión que un actual ataque por virus. Antes de anunciar el virus ampliamente, asegúrese de verificar su presencia mediante una herramienta de detección de virus, si es posible, con la asistencia de personal técnicamente competente.

Los programas "Caballos de Troya" y los "Gusanos" son con frecuencia catalogados como virus. Los "Caballos de Troya" son tratados en la sección "A fin de cuentas, ¿qué programa es este?. Los "Gusanos" deben ser considerados un tipo de virus para el propósito de esta sección.

3.6 Módems.

Se debe ser muy cuidadoso al adicionar algo a una computadora, y especialmente cualquier equipo que permita flujo de datos. En un ambiente de cómputo centralmente administrado usted debe solicitar permiso antes de conectar cualquier cosa a su computadora.

Los módems representan un riesgo especial de seguridad. Muchas redes son protegidas por un conjunto de medidas diseñadas para prevenir un asalto frontal desde redes públicas. Si su computadora está conectada a una red, usted debe poner cuidado cuando también esté usando un módem. Es enteramente posible usar el módem para conectarse a una red remota mientras "aun" está conectado a la red "segura". Su computadora puede actuar ahora como un hueco en la defensa de su red. De esta forma puede facilitar la entrada de usuarios no autorizados a la red de su organización a través de su computadora.

Asegúrese de que usted sabe lo que está haciendo si deja un módem conectado y activa su computadora para permitir llamadas de computadoras remotas. Cerciórese de que está empleando todos los mecanismos de seguridad correctamente. Muchos módem contestan llamadas por defecto, por eso debe desconectar la auto respuesta a menos que este preparado para tener la respuesta de su computadora a los que llaman. Algunos softwares de acceso remoto requieren eso. Compruebe que ha conectado todos los mecanismos de seguridad de su software de acceso remoto antes de permitir que su computadora sea accesada por teléfono.

Observe que tener un número no registrado no lo protege de alguien que irrumpa en su computadora a través de la línea telefónica. Es muy fácil probar muchas líneas telefónicas para detectar módems y entonces lanzar un ataque.

3.7 Terminales abandonadas.

No deje una computadora o terminal enlazada y salga a caminar. Utilice protectores de pantalla con contraseña siempre que sea posible. Estos pueden ser puestos de forma tal que se activen después que la computadora ha estado inactiva por un tiempo.

Siniestros como este pueden ser vistos: no es raro que alguien esté merodeando para borrar su trabajo. Si se mantuvo enlazado alguien puede venir y realizar un daño por el cual usted deberá sentirse responsable. Por ejemplo, imagine los problemas que confrontará si fuera enviado en su nombre un correo sucio o indecente al director de su empresa o su cuenta fuera usada para la transferencia ilegal de pornografía.

Cualquiera que pueda lograr acceso físico a su computadora puede casi con certeza introducirse en ella, por lo tanto, sea cauteloso con respecto a quien le da acceso a su máquina. Si no es posible garantizar la seguridad física de su máquina, sería prudente cifrar los ficheros de datos que se encuentran en su disco duro. Si es factible, también es sensato cerrar la puerta de la oficina donde se encuentra la computadora.

3.8 Protección de ficheros.

Los ficheros de datos y directorios en sistemas compartidos requieren cuidado y mantenimiento. Hay dos categorías de tales sistemas:

- Ficheros para compartir.

Los ficheros compartidos pueden ser visibles por cualquiera o por un grupo restringido de otros usuarios. Cada sistema tiene una manera diferente de especificar esto. Es imprescindible entender como se controlan los permisos de acceso y la implementación de esos controles sin fallos.

- Ficheros protegidos.

Estos incluyen aquellos ficheros a los cuales solo usted debe tener acceso, pero que están disponibles para cualquiera que tenga privilegios de administrador. Un ejemplo de esto son los ficheros asociados con la entrega de correo electrónico. Usted no desea que otros usuarios lean

su correo, por tanto asegúrese que los ficheros tienen establecidos los permisos necesarios correspondientes.

3.9 Cifrar todo.

Adicionalmente, hay ficheros que son privados. Usted puede tener ficheros a los cuales no desea que nadie más tenga acceso. En este caso es prudente cifrar los ficheros. De esta forma, aún si su red es vulnerada o el administrador del sistema le da acceso a un extraño, su información confidencial no estará disponible. El cifrado es también muy importante si usted comparte una computadora con otra(s) persona(s). Mediante la salva de respaldo de los datos y el empleo del cifrado, esta clase de uso compartido debe ser segura.

Antes de cifrar los ficheros se debe consultar la política de seguridad de su sitio. Algunos empleadores y países prohiben expresamente la conservación y/o transferencia de ficheros cifrados.

Tenga cuidado con las contraseñas y llaves que utilice para cifrar ficheros. Busque una forma segura, no solo para protegerlas de ojos curiosos, sino también para su conservación segura, ya que si las pierde no tendrá posibilidad de descifrar sus datos. Por ello pudiera ser prudente guardar más de una copia. Esto incluso podría ser un requerimiento de su institución, si por ejemplo ésta tiene una política definida al respecto. Esto protege contra la posibilidad de que la única persona que conoce una frase de paso pueda abandonar la institución o ser víctima de un accidente.

Los programas de cifrado están fácilmente disponibles, aunque su calidad puede variar en un amplio rango. PGP (Pretty Good Privacy) por ejemplo ofrece una fuerte capacidad de cifrado. Muchos softwares de aplicación común incluyen la posibilidad de cifrado de datos, aunque por lo general estas facilidades de cifrado son muy frágiles.

No debe sentirse intimidado por el software de cifrado. Softwares fáciles de usar están disponibles.

3.10 Destruya lo desechable.

Usted se sorprenderá de las cosas que encuentra en el cesto de la basura: Notas de reuniones, planes de trabajo viejos, listas internas de teléfonos, listados de programas de computadora, correspondencia con los clientes e incluso análisis de mercado. Todo esto puede ser muy valioso para los competidores o incluso para un periodista aventurero que busque una primicia. ¡La amenaza del “buceo” en la basura es real, tómelo seriamente!. Destruya todos los documentos potencialmente útiles antes de botarlos.

Debe estar consciente también que el borrado de un fichero en muchos casos no lo elimina. La única forma de estar seguro que un disco duro viejo no contiene datos valiosos debe ser reformateándolo.

3.11 A fin de cuentas, ¿qué programa es este?

Los programas se han vuelto mucho más complejos en los últimos años y tienden a extenderse frecuentemente de forma tal que pueden ser más peligrosos. Esta extensión hace las aplicaciones más flexibles, poderosas y habituales. Ellos también exponen a los usuarios finales a toda clase de riesgos.

Un programa puede tener asociados (plug-in) módulos. Usted no debe confiar en un programa asociado simplemente porque esté considerando confiable el programa a que aquel esta asociado. Por ejemplo: Algunas páginas Web sugieren que el usuario descargue un programa asociado para ver o usar alguna porción contenida en la misma. Considere: ¿Qué es este programa asociado?, ¿Quién lo escribió?, ¿Hay seguridad si se incluye en su navegador?

Algunos ficheros son “documentos compuestos”. Esto quiere decir que en lugar de utilizar un solo programa, el necesariamente correrá algunos programas en interés de ver o editar un documento. Una vez más, sea cuidadoso al descargar componentes de aplicaciones. Justo por el hecho de que estén integrados a productos que son bien conocidos no significa que ellos puedan ser confiables. Considere la recepción de un mensaje de correo que solo puede ser leído si se descarga un componente especial. ¡Este componente puede ser un programa sucio que puede borrar su disco duro!

Algunos programas son descargados automáticamente cuando se esta accediendo a las páginas Web. Desde que existen algunas salvaguardas para asegurar que estos programas pueden ser usados de forma segura, quiere decir que ha habido imperfecciones de seguridad en el pasado. Por esta razón, algunos sitios administrados centralmente demandan que ciertas capacidades de navegación sean inhabilitadas.

4. La paranoia es buena.

Mucha gente no se da cuenta, pero la ingeniería social es una herramienta que muchos intrusos utilizan para ganar acceso a los sistemas de cómputo. La impresión general que las personas tienen de las penetraciones a los sistemas de cómputo es que son resultado de imperfecciones técnicas explotadas por los intrusos. La gente también tiende a pensar que las brechas son puramente técnicas. Sin embargo, la verdad es que la ingeniería social juega un gran papel ayudando al atacante a deslizarse a través de las barreras de seguridad. Esto frecuentemente resulta un sencillo escalón hacia el sistema protegido si el atacante no tiene acceso autorizado a todo el sistema.

La ingeniería social puede ser definida, en este contexto, como el acto de ganar la confianza de usuarios legítimos de computadoras hasta el punto en que ellos revelan secretos del sistema o dan alguna ayuda, no intencionada, para ganar acceso no autorizado a su(s) sistema(s). Usando la ingeniería social un atacante puede ganar información valiosa y/o asistencia que puede ayudarlo a violar con facilidad las barreras de seguridad. Ingenieros sociales habilidosos pueden aparentar ser genuinos y sin embargo realmente ser completamente falsos.

Muchas veces los atacantes usando la ingeniería social trabajan por vía telefónica, lo cual no solo les proporciona un escudo para proteger su identidad, sino además hace la tarea sencilla ya que el atacante puede aparentar ser alguien en particular, con muchas oportunidades de obtener su objetivo.

Hay diversos tipos de ingeniería social. Estos son algunos ejemplos de los más comúnmente utilizados:

- Un atacante puede simular ser un legítimo usuario final que es nuevo en el sistema o simplemente que no es muy bueno en computación. Este atacante puede dirigirse al administrador del sistema y a otros usuarios finales pidiéndoles ayuda. Este "usuario" puede haber perdido su contraseña o sencillamente no se puede enlazar al sistema y necesita el acceso urgentemente. Los atacantes pueden también haber tenido conocimiento para identificarse a sí mismo como alguna persona muy importante dentro de la empresa, exigiéndole fuertemente al administrador lo que ellos necesitan. En tales casos el administrador (o pudiera ser un usuario final) puede sentirse amenazado por la autoridad que llama y ceder a sus demandas.

- Los atacantes que operan mediante llamadas telefónicas pueden no haber visto nunca antes la pantalla del display de su sistema. En tales casos la estrategia que usa es dar detalles vagos y llevar al usuario a revelar más información sobre el sistema. El atacante puede aparentar estar realmente perdido a fin de que el usuario sienta que está ayudando a una muchacha en apuros. Con frecuencia, esto hace que la gente se salga de sus normas habituales para ayudar y en este caso puede entonces revelar secretos al estar desprevenido.

- Un atacante puede también tomar ventaja de los problemas del sistema que se ponen a su atención. El ofrecimiento de ayuda a un usuario es una manera efectiva de ganar su confianza. Un usuario que está frustrado con problemas está expuesto a obtener más que alegría cuando alguien llega a ofrecerle alguna ayuda. El atacante puede llegar haciéndose pasar por un administrador de sistema o técnico de mantenimiento. Este atacante obtendrá frecuentemente información valiosa debido a que el usuario piensa que es correcto revelar secretos a los técnicos. La visita al sitio puede representar un mayor riesgo para el atacante ya que él puede no disponer de un fácil y rápido escape, sin embargo el riesgo puede ser muy fructífero si el atacante logra obtener acceso directo al sistema por un usuario ingenuo.

- A veces los atacantes pueden ganar acceso a un sistema sin un conocimiento previo de algún secreto del sistema ni de las terminales de acceso. De la misma forma que uno no debe pasar el equipaje de otra persona a través de los controles aduanales, ningún usuario debe teclear comandos en nombre de algún otro. Cuidado con los atacantes que emplean a usuarios como sus propios dedos controlados remotamente para teclear comandos que pueden dañar al sistema. Estos atacantes explotarán software con problemas o agujeros del sistema aun sin acceso directo al sistema. Los comandos tecleados por el usuario final pueden causar daño al sistema, abrir su propia cuenta para el acceso del atacante o crear un hueco que permita la entrada del atacante (algún tiempo después) al sistema. Si usted no está seguro de los comandos que le han sido indicado teclear, no siga simplemente las instrucciones. Usted nunca sabe a que y a donde esto puede conducirlo.

Para protegerse de ser víctima de la ingeniería social, algo importante a recordar es que las contraseñas son secretas. La contraseña de su cuenta personal debe solo ser conocida por usted. Los administradores de sistemas que necesitan hacer algo en su cuenta no requieren su contraseña. Como administradores, los privilegios que ellos tienen les permitirán trabajar en su cuenta sin necesidad de que usted les revele su contraseña. Un administrador no debe tener que preguntarle a usted su contraseña.

Muchos trabajos de mantenimiento requerirán privilegios especiales no otorgados a usuarios finales. Los usuarios deben resguardar el uso de sus cuentas y mantenerlas para su propio uso. Las cuentas no deben ser compartidas, ni siquiera temporalmente con el personal de mantenimiento o el administrador. Los administradores de sistemas tendrán sus propias cuentas para trabajar con ellas y no necesitarán acceso a un sistema mediante la cuenta de un usuario final.

Los técnicos de mantenimiento de sistemas que llegan a un sitio deben estar acompañados por el administrador local del sitio (que usted debe conocer). Si el administrador del sitio no le es familiar o si el técnico viene solo, es recomendable hacer una llamada al administrador del sitio que usted conoce para chequear si el técnico debe estar ahí. Sin embargo, muchas personas no hacen esto por no parecer paranoicos y porque esto resulta embarazoso al mostrar falta de confianza con estos visitantes.

A menos que usted esté muy seguro de que la persona con quien está hablando es quien pretende ser, ninguna información secreta debe ser revelada a la misma. A veces, los atacantes son buenos simulando por teléfono la voz de alguien que usted conoce, por eso siempre es bueno chequear doblemente la identidad de esta persona. Si usted es incapaz de hacer esto, la conducta más sensata es no revelarle ningún secreto. Si usted es un administrador de sistemas, debe contar con procedimientos de seguridad para la asignación y reasignación de contraseñas a los usuarios, y seguir tales procedimientos. Si es un usuario final no habrá ninguna necesidad para usted de tener que revelar secretos del sistema a nadie más. Algunas empresas asignan una cuenta común para múltiples usuarios. Si usted pasa a formar parte de uno de tales grupos,

asegúrese de conocer al resto de los integrantes de forma que pueda decir si alguien que pretende serlo es genuino.

Tercera Parte: Usuarios que administran computadoras con acceso a redes.

Los usuarios de computadoras independientes o los que administran su propia red tienen muchas de las mismas preocupaciones que los usuarios de una red administrada centralmente. El siguiente es un sumario de advertencias adicionales que se brindan en la Tercera Parte:

- Lea los manuales para saber como activar los dispositivos de seguridad y entonces actívelos.
- Considere cuan privados deben ser sus datos y correos. ¿Ha invertido en software privado y sabe como usarlo todavía?
- Prepárese para lo peor en progreso.
- Manténgase informado sobre las nuevas amenazas

5. Elabore su propia política de seguridad.

Usted debe decidir por anticipado que riesgos son aceptables y entonces respaldar esta decisión. Puede ser sensato simplemente evitar descargar cualquier software de la red que provenga de un origen desconocido a una computadora que conserve registros de negocios, otros datos valiosos y datos que potencialmente sean dañados si la información fuera perdida o es robada.

Si la máquina tiene propósitos múltiples, por ejemplo, recreación, correspondencia y alguna contabilidad casera, quizás se arriesgue a descargar alguna aplicación. En este caso corre el riesgo de adquirir algún software que no es exactamente lo que aparenta ser.

Puede ser que valga la pena la instalación de software privado en una computadora si ésta es compartida por múltiples usuarios. De esta forma, un amigo de un compañero de cuarto no tendrá acceso a sus datos privados.

6. Las cosas malas pasan.

Si usted conoce que sus ficheros han sido modificados o averigua de algún modo que su cuenta ha sido usada sin su conocimiento, debe informar inmediatamente a su punto de contacto de seguridad. En muchos casos usted no sabrá quien es su punto de contacto de seguridad: Intente llamar al servicio de ayuda de su proveedor de servicios de Internet como un primer paso.

6.1 Como prepararse para lo peor en progreso.

- Lea toda la documentación de usuario cuidadosamente. Cerciórese de esto cuando los servicios se estén ejecutando en su computadora. Si hay servicios de red activados, asegúrese de que estén correctamente configurados (establecidos todos los permisos tales como los de prevención de conexiones anónimas o invitadas y otros similares). Entienda como configurar adecuadamente y emplear de forma segura estos mecanismos.

- Salve los datos de usuario. Esto es siempre importante. La salva está normalmente concebida como una forma de asegurar que usted no perderá su trabajo si falla un disco o si comete un error y borra un fichero. La salva también es crítica para asegurar que los datos no se perderán durante un incidente de seguridad. Una de las amenazas más malignas y desdichadamente más comunes presentes en los Virus y Caballos de Troya es el borrado de los discos duros.

- Obtenga software de chequeo de Virus y herramientas de auditoría de seguridad. Entienda como utilizarlos e instálelos antes de conectarse a una red pública. Muchas herramientas de seguridad requieren ser corridas en un sistema "limpio" con el fin de poder realizar una comparación con el estado actual del sistema. Esto en algunos trabajos es necesario hacerlo por anticipado.

- Actualice regularmente el software de la red. Con cada nueva versión de software que salga es prudente actualizar. De igual forma las vulnerabilidades de seguridad deberán ser fijadas. Mientras más espere para hacerlo, mayor será el riesgo de que las vulnerabilidades de seguridad del producto comiencen a conocerse y ser explotadas por algún atacante de red. ¡Manténgase al día!

- Averigüe a quien contactar si sospecha de un problema. ¿Su proveedor de servicios de Internet tiene algún contacto de seguridad o servicio de ayuda? Investigue esto antes de que el problema pase, así no perderá tiempo tratando de descifrar que problema ocurre. Guarde la información de contacto, tanto en línea como fuera de línea para una fácil solución.

Hay 3 maneras de evitar los problemas con los virus:

1. No sea promiscuo.

Sea todo lo cauteloso posible acerca del software que instala en su sistema. Si no conoce o no está seguro del origen de un programa, es prudente no correrlo. No ejecute programas o los copie usando viejos disquetes a menos que los haya formateado antes, especialmente si los viejos disquetes han sido usados para obtener software de una feria comercial y de otros lugares potencialmente vulnerables para la seguridad.

Casi todo el riesgo de ser infectado por virus puede ser eliminado si usted es extremadamente cuidadoso sobre que ficheros están guardados en su computadora. Vea la sección 3.1: "El peligro de descargar" para más detalles.

2. Examine regularmente.

Realice a su computadora un chequeo periódico. Hay excelentes detectores de virus y herramientas de auditoría de seguridad disponibles hoy en día para la mayoría de las plataformas. Uselas, y si es posible, instálelas para que corran automática y regularmente.

3. Advierta lo inusual.

No es cierto que una diferencia que usted no pueda detectar no es una diferencia, no obstante esta es una buena regla empírica. Usted debe conocer la forma en que trabaja su sistema. Si hay un cambio inexplicable (por ejemplo, ficheros que usted cree deben existir no están o nuevos ficheros extraños están apareciendo y el espacio de disco se desvanece) usted debe revisar la presencia de virus.

La mejor manera de evitar problemas con virus es mantener los ficheros importantes salvados. De esta forma si el problema empeora usted puede siempre restaurar su sistema al estado que tenía antes de ser afectado.

Debe tomarse algún tiempo en familiarizarse con las herramientas de detección de virus disponibles para su tipo de computadora. Usted debe usar una herramienta actualizada en tiempo (es decir no más vieja que 3 meses). Es muy importante chequear su computadora si está utilizando software gratis o disquetes usados por otras personas para transferir ficheros, etc.

6.2 Que hacer si sospecha de un problema.

Si usted sospecha que su computadora tiene un virus, que un programa maligno está corriendo o que un sistema ha sido vulnerado, la más sabia actitud es en primer lugar desconectar el sistema de todas las redes. Si está disponible algún software de detección de virus o de auditoría, debe usarlo.

El chequeo manual de corrupción del sistema de ficheros, intromisión o de sustituciones maliciosas es una tarea muy tediosa. Afortunadamente hay muchos programas de detección de virus disponibles para computadoras PC's y Macintosh, así como programas de auditoría de seguridad para sistemas UNIX. Si se baja software de la red, es prudente utilizar regularmente detectores de virus y herramientas de auditoría.

Si comienza a detectarse que un sistema está siendo atacado, es el momento para una limpieza general. Idealmente, un sistema debe ser reconstruido como consecuencia de un incidente. Esto quiere decir borrar todo en el disco duro, posteriormente instalar el sistema operativo y todo el software adicional que el sistema necesita. Lo mejor en este caso es instalar el sistema operativo y el software adicional desde los disquetes originales o desde CD-roms, en vez de hacerlo desde los soportes de salva. La razón para esto es que un sistema puede haber sido vulnerado algún tiempo atrás, de forma tal que el sistema o los programas salvados puedan también incluir algún virus o fichero alterado. La restauración de un sistema por causa de un incidente es tediosa, pero vale la pena hacerlo. No olvide reinstalar todos los mecanismos de seguridad que estaban instalados antes del incidente. Obtenga estos de una fuente verificada y confiable.

6.3. Correo Electrónico.

Recuerde ser cuidadoso con el correo salvado. Copias del correo enviado o recibido (o en realidad cualquier fichero en general) guardados en un lugar proporcionado por un proveedor de servicios de Internet puede ser vulnerable. El riesgo es que alguien pueda acceder a la cuenta y leer esos mensajes. Guarde sus ficheros de correo, particularmente los ficheros sensibles en su propia máquina.

7. Solo en casa.

Un sistema en la casa (o una máquina independiente, en general) puede ser vulnerado desde Internet si el usuario es despreocupado. Los ficheros pueden ser robados, alterados o destruidos. El sistema en sí mismo, si es comprometido, puede ser accesado nuevamente algún tiempo más tarde. Esta sección describe los aspectos y las recomendaciones más relevantes para un usuario de Internet desde la casa, o desde una máquina independiente, en general.

7.1. Cuídese de los demonios.

Una máquina independiente que utilice PPP para conectarse directamente a Internet se está convirtiendo en algo muy común. Estos sistemas están bajo el mayor riesgo si corren cierta clase de programas llamados "servicios". Si usted corre un servicio, de hecho está haciendo disponible su computadora a otros a través de la red. Algunos servicios incluyen:

- Servidores de ficheros (tal como el servidor NFS, una PC compartiendo ficheros)
- Un servidor FTP.
- Un servidor Web.

Hay, en general, dos tipos de programas que operan en Internet: **Clientes** (como los programas navegadores del Web y los de correo) y **Servidores** (como los servidores Web y de correo).

La mayoría del software que corre en los sistemas independientes son del tipo clientes, pero de forma incrementada el software servidor está siendo disponible en plataformas tradicionalmente clientes (por ejemplo las PC's). El software servidor que corre en "el fondo" es conocido como un "demonio". Muchos programas de software servidor de Internet que corren como "demonio" tienen nombres que terminan en 'd', tales como "inetd" (Internet Daemon) y "talkd" (Talk Daemon). Cuando son instalados, estos programas esperan por clientes para demandar algún servicio a través de la red.

Hay cuatro cosas muy importantes a tener en cuenta sobre las implicaciones de seguridad corriendo estos servicios en una computadora independiente . Lo primero y más importante:

- Si un servidor no está configurado apropiadamente es muy vulnerable para ser atacado en la red. En esto es vital, si usted corre servicios, familiarícese con la configuración apropiada. Esto frecuentemente no es fácil y puede requerir entrenamiento y experiencia técnica.

- Todo software tiene imperfecciones y las imperfecciones explotadas debidamente pueden ser usadas para violar la seguridad de cómputo. Si usted corre un servidor en su máquina independiente, tiene que estar alerta. Esto requiere trabajo: Usted tiene que estar en contacto con el suministrador del software para obtener las actualizaciones de seguridad. Es altamente recomendado mantenerse al tanto de los aspectos de seguridad a través de los foros de seguridad en línea. Vea SSH para una lista de referencias.

Si descubre imperfecciones de seguridad en su software servidor, usted necesitará parar el uso de este software o aplicar los "parches" que eliminen las vulnerabilidades. El suministrador del software, si es una empresa o proveedor serio, le entregará información y medios actualizados para corregir los defectos de seguridad. Estos "parches" deben ser instalados tan rápido como sea posible.

- Es una regla práctica que mientras más viejo sea el software mayor será la posibilidad de que tenga vulnerabilidades conocidas. ¡Esto no quiere decir, por supuesto, que se deba confiar de forma simplista en nuevo software de marca! Con frecuencia se requiere de tiempo para descubrir, incluso defectos obvios de seguridad, en los servidores.

- Algunos servidores se inician sin ninguna advertencia. Pudiera haber navegadores de Web y clientes de Telnet en común uso con el inicio automático de servidores FTP, si no está explícitamente configurado para no hacer esto. Si estos servidores no están por sí mismos configurados apropiadamente, todo el sistema de ficheros de la computadora puede ponerse a la disposición de cualquiera en Internet.

En general, cualquier software PUEDE iniciar un demonio de red. La forma de asegurarse de esto es conocer los productos que está utilizando. Lea el manual y si le surge cualquier duda, llame a la empresa suministradora o envíe un mensaje al autor del software "gratis" para determinar si usted está actualmente corriendo un servicio por el uso de este producto.

Un usuario corriendo un servicio remoto en su máquina independiente enfrenta riesgos muy serios. Este servicio permite al usuario conectarse a su máquina desde otras computadoras en Internet, lo que puede ser muy conveniente. Sin embargo el peligro es que alguien observará secretamente la conexión y entonces está en capacidad de hacerse pasar por este usuario si decide hacerlo en el futuro. Vea "Los cables tienen oídos" donde se sugieren las precauciones a tomar en las conexiones remotas.

Si es posible, active todas las opciones de conexión relacionadas con la seguridad en su software servidor. Usted necesita revisar sistemáticamente estos registros (logs) en interés de ganar algún beneficio de ello. También debe estar consciente que los registros frecuentemente crecen muy rápidamente en tamaño, de manera que necesita estar al tanto de que ellos no llenen su disco duro.

7.2. Visitando Sitios.

Las conexiones remotas permiten a un usuario el acceso a un lugar físicamente distante desde el confort de su propia casa.

Más y más empresas están ofreciendo a sus empleados la posibilidad de trabajar desde su casa con acceso a su cuenta de computadora a través de una conexión telefónica. A medida que la conveniencia de la conectividad de Internet tiende a la disminución de los costos y a las posibilidades de una amplia diseminación, las empresas pueden permitir conexiones remotas a sus sistemas por la vía de Internet. Los clientes de las empresas con acceso a Internet pueden también ser provistos con conexiones a cuentas remotas. Estas empresas incluyen proveedores de servicios de Internet, y hasta los bancos. Los usuarios deben ser muy cuidadosos al hacer conexiones remotas.

Como fue discutido en la sección "Los cables tienen oídos" las conexiones a Internet pueden ser escuchadas furtivamente. Si usted pretende utilizar un servicio remoto, verifique que la conexión puede ser realizada de forma segura y cerciórese de utilizar tecnologías/herramientas seguras.

Las conexiones pueden ser aseguradas con el empleo de tecnologías tales como contraseñas desechables, shell seguro (SSH) y Secure Sockets Layer (SSL). Las contraseñas desechables hacen inservible una contraseña husmeada por un intruso, mientras que el shell seguro cifra los datos que se envían por la conexión. Por favor refiérase a "Navegación segura en el Web" para una discusión sobre el SSL. Servicios seguros como esos están disponibles en los sistemas a los cuales usted se conecta de forma remota.

7.3. ¡Cosa segura!

La administración de su propia computadora significa que usted selecciona que software está corriendo en ella. El software de cifrado proporciona protección para los datos. Si usted guarda los registros de negocios y otros datos sensibles en su computadora, el cifrado lo ayudará a guardarlos de forma segura. Por ejemplo, si usted corre un servicio de red desde su casa y dejó de establecer restricciones en un directorio privado, un usuario remoto (autorizado o no) puede ganar acceso a los ficheros en ese directorio privado. Si los ficheros están cifrados, el usuario no podrá leerlos. ¡Pero como todas las formas de cifrado corriendo en cualquier sistema, las llaves y contraseñas deben en primer lugar mantenerse seguras!

8. Una nota final.

Este documento ha brindado al lector una introducción tan concisa y detallada como ha sido posible. En el presente los asuntos de seguridad se ponen viejos muy rápidamente y aun cuando el esfuerzo ha estado dirigido hacia una discusión general, los ejemplos empleados pueden no ser relevantes en el futuro en la medida que Internet y la industria de las computadoras continúen creciendo.

Tal como los propietarios de casas están ahora tomando mayores precauciones, con el costo conveniente, para proteger sus casas en el mundo cambiante en que vivimos, los usuarios de redes de computadoras no deben ignorar la seguridad. Esto puede ser incomodo, pero siempre es mejor estar seguro que lamentarse.

Referencias:

(GLOSSARY) Malkin, G, “Internet User’s Glossary”, RFC 1983, Agosto 1996
(RFC 2196) Fraser, Barbara, “Site Security Handbook”, Septiembre 1997

Autores: Erik Guttman (Sun Microsystems), Lorna Leong (COLT Internet), Gary Malkin (Bay Networks)

Apéndice: Glosario de Términos de Seguridad.

Acceptable Use Policy (Política de uso aceptable).
Un conjunto de reglas y normas que especifican en mayor o menor detalle la expectativa relacionada con el uso apropiado de los sistemas o redes.

Account (Cuenta)
Ver (Computer) Account

Anonymous and Guest Log In (Conexión anónima e invitada)
Los servicios pueden hacerse disponibles sin ninguna clase de autenticación. Esto es muy común, por ejemplo, con el protocolo FTP para permitir accesos anónimos. Otros sistemas

proporcionan una cuenta especial llamada "Guest" para brindar acceso, normalmente restringiendo los privilegios de esa cuenta.

Auditing Tool (Herramienta de Auditoría)
Herramientas para el análisis de sistemas de cómputo o redes referidas a su estado de seguridad o en relación con el conjunto de servicios proporcionado por ella. COPS (Computer Oracle Password and Security Analyzer) y SATAN (Security Administrator's Tool for Analyzing Networks) son ejemplos famosos de tales herramientas.

Centrally-Administered Network (Red centralmente Administrada)
Una red de sistemas bajo la responsabilidad de un simple grupo de administradores que no están distribuidos, sino que trabajan centralmente para cuidar de la red.

Client (Cliente)
En dependencia de cómo se mire, un cliente puede ser un sistema de cómputo que un usuario final emplea para acceder servicios anfitrión (hosted) en otro sistema de cómputo llamado un Servidor. "Cliente" puede también referirse a un programa o a parte de un sistema que es empleado por un usuario final para acceder a servicios proporcionados por otro programa (por ejemplo, un navegador Web es un cliente que accede a páginas proporcionadas por un Servidor Web)

Common Account (Cuenta Común)
Una cuenta común es aquella que es compartida por un grupo de usuarios en contraposición a una cuenta normal que está disponible para un solo usuario. Si la cuenta es divulgada, es muy difícil o imposible conocer cual de los usuarios fue el responsable.

Compound Documents (Documentos Compuestos)
Un "documento" es un fichero utilizado por un software de aplicación para salvar información de usuario. Un documento "compuesto" es un fichero que contiene datos que pueden requerir la utilización de una variedad de programas para interpretarlos y manipularlos. Estos programas pueden ser utilizados sin el conocimiento del usuario.

(Computer) Account Cuenta (de Computadora.)
Este término describe la autorización de acceso a un sistema de cómputo específico o a una red. Cada usuario final tiene que usar una cuenta, que consiste muy probablemente de una combinación de nombre de usuario y contraseña u otra forma de establecer que el usuario final es la persona que tiene asignada esa cuenta.

Configuring Network Services (Servicios de Configuración de red)
La parte del trabajo de un administrador relacionada con la especificación de las condiciones y detalles de los servicios de red que gobiernan el suministro del servicio. En relación con un servidor Web, esto incluye para quien están disponibles las páginas Web y que clase de información es registrada para revisar el uso del servidor Web.

Cracker
Este término se utiliza para nombrar a los atacantes, intrusos u otras personas que no respetan las reglas e intentan transguedir los mecanismos de seguridad y/o atacan individuos u organizaciones.

Daemons (Demonios)
Estos son procesos que corren en los sistemas de cómputo para proporcionar servicios a otros sistemas de computo o procesos. Típicamente, los demonios son considerados "Servidores".

Decrypting (Descifrado)
El proceso contrario al cifrado de un fichero o mensaje para recuperar el texto original en interés de usarlo o leerlo.

Dial-in Service (Servicio de discado)
Una manera de proporcionar acceso a sistemas de cómputo o redes a través de una red de telecomunicaciones. Una computadora usa un módem para hacer una llamada telefónica a otro módem, que a su vez proporciona "servicio de acceso a red". Vea también PPP.

Digital Signature (Firma Digital)
Este es un mecanismo que asigna una "firma" a un fichero o a un mensaje de correo, permitiendo a otros verificar el dato "firmado". La firma solo puede ser generada por alguien que mantiene algún dato privado. Las firmas digitales proporcionan verificación de la fuente de los datos (aunque no necesariamente el contenido) y su autenticidad.

Downloaded Software (Software Descargado)
Paquetes de software recuperados de Internet (usando, por ejemplo, el protocolo FTP).

Downloading (Descargar)
El acto de traer ficheros desde un servidor a la red.

Email Packages (Paquetes de Correo Electrónico)
Para comunicarse a través del correo electrónico, un usuario final usualmente hace uso de un cliente de correo que le proporciona la interfaz de usuario para crear, enviar, recuperar y leer correo electrónico. Varios paquetes de correo electrónico diferentes brindan el mismo conjunto de funciones básicas, sin embargo tienen diferentes interfaces de usuario y quizás funciones extras especiales. Algunos paquetes de correo electrónico ofrecen posibilidades de cifrado y de firma digital.

Email Security Software (Software Seguro de Correo)

Software como el PGP brindan funciones de seguridad tales como el cifrado (y el descifrado) para posibilitar a los usuarios finales proteger los mensajes y documentos antes de su envío por una red posiblemente insegura.

Encrypting/Encryption (Cifrado)
El acto de aplicación de un algoritmo criptográfico específico a los datos para prevenir ojos curiosos. El cifrado emplea algoritmos matemáticos y secretos (usualmente representados por contraseñas o frases de paso que son conocidas por las partes que se comunican) para brindar protección.

Encryption Software (Software de Cifrado)
El software que actualmente brinda la necesaria utilidad a los usuarios finales de cifrar los mensajes y ficheros. PGP es un ejemplo.

End User (Usuario Final)
Un individuo que hace uso de sistemas de cómputo y redes.

Files (Ficheros) –Programas, datos, texto, etc.-
Los ficheros incluyen datos de usuario, pero también programas, el sistema operativo de la computadora y los datos de configuración del sistema.

File Server (Servidor de Ficheros)
Un sistema de cómputo que brinda una forma de compartir y trabajar ficheros almacenados en el sistema entre usuarios con acceso a estos ficheros a través de una red.

File Transfer (Transferencia de Ficheros)
El proceso de transferir ficheros entre dos sistemas de cómputo a través de una red, usando protocolos tales como FTP o HTTP.

Fixes, Patches and installing Them (Arreglos, Parches y su instalación)
Los vendedores, en respuesta a las vulnerabilidades de seguridad descubiertas, proporcionan conjuntos de ficheros que tienen que ser instalados en los sistemas de cómputo. Estos ficheros "arreglan" o "remiendan" el sistema de cómputo o los programas y remueven las vulnerabilidades de seguridad.

FTP (File Transfer Protocol)-Protocolo de transferencia de ficheros-
Un protocolo que permite la transferencia de ficheros entre un cliente FTP y un servidor FTP.

Group of Users (Grupo de Usuarios)
El software de seguridad frecuentemente permite establecer permisos para un grupo (de usuarios) en contraposición a los permisos individuales.

Help Desk (Buró de Ayuda o asistencia)

Una entidad de apoyo que puede ser llamada en busca de ayuda con un problema de computación o comunicaciones.

Internet
Una colección de redes interconectadas que utilizan un conjunto común de protocolos llamados TCP/IP para permitir la comunicación entre los sistemas de cómputo conectados.

Key Escrow (Cesión de claves)
Las claves son empleadas para cifrar y descifrar ficheros. Estas claves son legítimamente usadas por las partes que se les ha otorgado el derecho a compartir datos. Si las claves están disponibles para terceras partes, esto es conocido como cesión de claves. Esto puede ser usado para prevenir pérdidas de claves o para permitir que terceras partes (por ejemplo agencias de gobierno) dispongan de acceso a datos cifrados.

Keys Used to Encrypt and Decrypt Files (Claves usadas para cifrar y descifrar ficheros)
Para hacer uso del cifrado, un usuario final tiene que dar algo secreto, en la forma de algún dato, usualmente llamado una clave. Hay dos clases de claves criptográficas. Las claves simétricas permiten a cualquiera que las posea tanto cifrar como descifrar datos. La criptografía de claves públicas proporciona un par de claves, una para cifrar y la otra para descifrar los datos. La criptografía de claves públicas tiene la ventaja que no todas las partes en comunicación necesitan conocer la misma clave secreta.

Log In, Logging into a System (Conexión, Conectarse a un sistema)
Esta es una acción realizada por un usuario final, cuando él se autentifica a sí mismo ante un sistema de cómputo.

Log In Prompt (Paso a la conexión)
Los caracteres que son mostrados en pantalla al conectarse a un sistema para preguntar por el nombre de usuario y la contraseña.

Logged In (Conectado)
Si un usuario final ha demostrado exitosamente tener acceso legítimo a un sistema, se considera conectado.

Masquerade (Suplantación). Vea Remote Log In.
Cualquiera que pretenda ser alguien que no es, en interés de obtener acceso a una cuenta de computadora se dice que está haciendo una suplantación. Esto puede ser realizado proporcionando un nombre de usuario falso o robando la contraseña de otra persona y conectándose como élla.

Network File System (NFS, ficheros compartidos en PC´s, etc) Sistema de Ficheros en Red.
NFS es una aplicación y un protocolo apropiado que brinda una manera de compartir ficheros entre clientes y servidores Hay otros protocolos que brindan acceso a ficheros a través de redes. Estos proporcionan similares funcionalidades, sin embargo no interoperan entre sí.

Networking Features of Software (Facilidades de software en red)
Algunos softwares tienen facilidades que hacen uso de la red para recuperar o compartir datos. Puede no ser obvio que el software tiene facilidades de red.

Network Services (Servicios de Red)
Servicios que no son proporcionados en el sistema de cómputo local en que el usuario final está trabajando, sino en un servidor localizado en la red.

One-Time Password System (Sistema de contraseña de una sola vez o desechable)
En lugar de utilizar una misma contraseña una y otra vez, una contraseña diferente es usada en cada subsecuente conexión. Una parte de la contraseña frecuentemente es un PIN, que el usuario tiene memorizado, mientras que la otra parte puede ser generada por algún hardware (Token). Ambas partes tienen que ser utilizadas juntas. Aun si la contraseña es transmitida por la red y robada, el atacante no se beneficiará con el conocimiento de la contraseña. Esto es especialmente importante para protocolos como FTP y Telnet donde las contraseñas son transmitidas sin cifrar a través de la red.

Passphrase (Frase de Paso)
De similar función que las contraseñas, las frases de paso son contraseñas que permiten espacios en ellas.

Password-Locked Screensaver (Protector de pantalla con contraseña)
Un protector de pantalla oculta lo que normalmente muestra un monitor. Un protector de pantalla con contraseña solo puede ser desactivado si es suministrada la contraseña del usuario final. Esto previene contra la conexión a un sistema no autorizada y oculta el trabajo que actualmente se está haciendo de alguien que esté pasando.

Permissions (Permisos)
Otra palabra para los controles de acceso que son usadas para controlar el acceso a ficheros y otros recursos.

PGP – Pretty Good Privacy (Intimidad algo buena)
PGP es un paquete de aplicación que proporciona herramientas para cifrar y firmar digitalmente ficheros en sistemas de cómputo. Es especialmente útil para cifrar y/o firmar ficheros y mensajes antes de enviarlos a través del correo electrónico.

Plug-in Modules (Módulos Conectados)

Componentes de software que se integran a otro software (tales como los navegadores Web) para proporcionar facilidades adicionales.

Point-of-Contact, Security (Punto de Contacto de Seguridad)
En caso de brechas o problemas de seguridad, muchas organizaciones designan un punto de contacto que puede alertar a otros y tomar las acciones apropiadas.

PPP- Point to Point Protocol (Protocolo Punto a Punto)
En la actualidad, muchos servicios de discado proporcionan un mecanismo para establecer una conexión PPP a través de una línea telefónica. La conexión PPP puede entonces ser usada sobre el protocolo TCP/IP para cualquier comunicación adicional, haciendo los sistemas de cómputo conectados (Por ejemplo, una PC de usuario final) parte de Internet.

Privacy Programs (Programas Privados)
Otro término para software de cifrado que pone de relieve el uso de este software para proteger la confidencialidad y por consiguiente la privacidad de los usuarios finales que lo utilizan.

Remote Access Software (Software de Acceso Remoto)
Este software permite a una computadora usar un módem para conectarse a otro sistema. También permite a una computadora "atender" llamadas en un módem (esta computadora proporciona "servicios de acceso remoto"). El software de acceso remoto puede proporcionar acceso a una computadora independiente o a una red.

Remote Log In (Conexión Remota)
Si un usuario final utiliza una red para conectarse a un sistema, este acto es conocido como conexión remota.

Security Features (Características de Seguridad)
Estas son características que proporcionan protección o que posibilitan a usuarios finales y administradores fijar la seguridad de un sistema, por ejemplo, auditándolo.

Server (Servidor)
Un servidor es un sistema de cómputo, o un conjunto de procesos en un sistema de cómputo, proporcionando servicios a clientes a través de una red.

Shareware
Shareware es el software que no es gratis pero que suministrado a bajo precio actualmente contribuye al esfuerzo de los programadores y les posibilita mejorar el software o su generalización.

Sharing Permissions (Compartiendo Permisos)

Muchos sistemas de cómputo permiten a los usuarios compartir ficheros sobre una red. Estos sistemas invariablemente proporcionan un mecanismo para controlar quien tiene permiso para leer o sobrescribir estos ficheros.

Site (Sitio)
En dependencia del contexto en que este término se utilice, puede ser aplicado a sistemas de cómputo que están agrupados en un área geográfica, organizados jurisdiccionalmente o formen parte de redes. Un sitio se refiere típicamente a una red bajo una común administración.

SSH- Secure Shell
De forma similar al SSL, la entrada del SSH proporciona un protocolo entre un cliente y un servidor para acceder a sistemas de cómputo de forma remota asegurando al mismo tiempo las comunicaciones y brindando un fuerte mecanismo para autenticación de usuarios y confidencialidad

SSL- Secure Sockets Layer
Este protocolo brinda servicios de seguridad a diferencia de otros protocolos inseguros que operan sobre redes. Estos servicios pueden incluir privacidad (cifrado de datos) y autenticación. El SSL es usado típicamente por un navegador Web para cifrar los datos que son enviados y descargados de un servidor Web. El SSL también permite a un navegador Web verificar si se está comunicando con un servidor Web que ha sido "certificado".

Systems Administrator (Administrador de Sistemas)
La persona que mantiene el sistema y cuenta con privilegios de administración. Con el fin de evitar errores y equivocaciones cometidos por estas personas, mientras no actúan como administradores, debe limitarse el tiempo en que ellos actúan como tales al mínimo.

System Administrator Privileges (Privilegios de Administración de Sistemas)
Los administradores de sistemas tienen más derechos (mayores permisos) en la medida en que su trabajo compromete el mantenimiento de los ficheros del sistema.

System Files (Ficheros del Sistema)
El conjunto de ficheros en un sistema que no pertenecen a usuarios finales, los cuales gobiernan el funcionamiento del sistema. El sistema de ficheros tiene un gran impacto en la seguridad del sistema.

Telnet
Un protocolo que hace posible el acceso remoto a otro sistema de cómputo a través de la red.

Terminal
Un dispositivo que se conecta a un sistema de cómputo en interés de proporcionar acceso a éste a usuarios y administradores.

Threats (Amenazas)
El potencial de que una vulnerabilidad existente pueda ser explotada comprometiendo la seguridad de los sistemas o redes. Aun si una vulnerabilidad es desconocida, representa una amenaza, por definición.

Trojan Horse (Caballo de Troya)
Un programa que lleva consigo un medio que posibilita a su creador el acceso al sistema.

Trusted Source (Fuente Confiable)
Una fuente de software descargado que es confiable en el sentido que el software obtenido de ella no debe ser malicioso.

Virus
Un programa que se reproduce a sí mismo en un sistema de cómputo incorporándose en otros programas que comparten en estos sistemas.

Virus Detection Tool (Herramienta de Detección de Virus)
Software que detecta y posiblemente remueve virus de computadoras, alertando apropiadamente al usuario.

Vulnerability (Vulnerabilidad)
Una vulnerabilidad es la existencia de una debilidad, error de diseño o de implementación que puede conducir a un evento inesperado e indeseable, comprometiendo la seguridad del sistema, red, aplicación o protocolo.

Web Browser Cache
Esta es la parte del sistema de ficheros que es usada para guardar las páginas Web y los ficheros relacionados. Puede ser utilizada para recuperar ficheros recientemente accesados en lugar de descargarlos en cada caso desde la red.

Web Browser Capabilities
El conjunto de funcionabilidades en un navegador Web para el uso del usuario final.

Web Server (Servidor Web)
Un programa servidor que proporciona acceso a páginas Web. Algunos servidores Web proporcionan acceso a otros servicios, tales como bases de datos y directorios.

Worm (Gusano)
Un programa de computadora que se reproduce así mismo y se autopropaga. En oposición a los virus, los gusanos se generan en ambiente de redes.