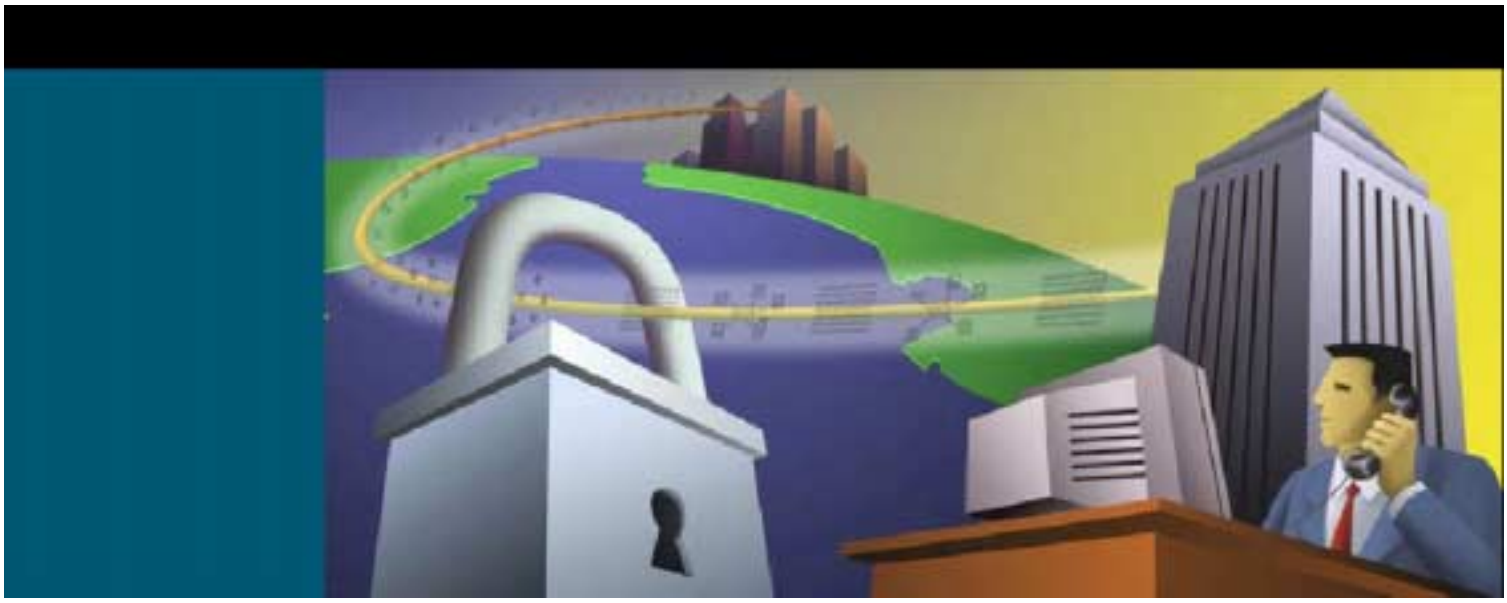
Guía de seguridad de redes
para principiantes



Una introducción a los problemas clave de seguridad para la Economía del comercio electrónico (E-Business)

Con el auge de Internet pública y el comercio electrónico (e-commerce), las computadoras personales y los equipos en red que no tienen la protección y la seguridad adecuadas, están siendo cada vez más vulnerables a ataques nocivos. Hackers, virus, empleados vengativos e incluso errores humanos representan amenazas y peligros para las redes. Y todos los usuarios de computadoras, desde los que navegan en Internet ocasionalmente hasta las grandes empresas, podrían verse afectados por violaciones a la seguridad. Sin embargo, estas violaciones a la seguridad pueden evitarse fácilmente. ¿Cómo? Esta guía le brinda un panorama general de las amenazas más comunes a la seguridad de la red como también los pasos que tanto usted como su organización deben seguir para protegerse de tales amenazas y asegurarse de que la transmisión de datos a través de las redes sea segura.

Importancia de la seguridad

Sin duda alguna, Internet se ha convertido en la red de datos pública más importante, permitiendo y facilitando las comunicaciones personales y comerciales en todo el mundo. El volumen de tráfico por Internet y por las redes corporativas se está multiplicando exponencialmente cada día. Se están realizando cada vez más comunicaciones por correo electrónico; los empleados móviles, los trabajadores a distancia y las sucursales usan Internet para conectarse en forma remota con las redes corporativas; y las transacciones comerciales formalizadas en Internet, a través de World Wide Web (www), actualmente dan cuenta de gran parte de los ingresos de las empresas.

Si bien Internet ha transformado y mejorado significativamente la forma de concretar negocios, esta extensa red y las tecnologías asociadas han abierto las puertas a una cantidad de amenazas de seguridad de las cuales las corporaciones deben protegerse. A pesar de que se supone que los ataques más graves a las redes suceden cuando afectan a negocios que manejan datos confidenciales, como historiales financieros o antecedentes médicos personales, las consecuencias de los ataques a cualquier entidad oscilan entre los que ocasionan un inconveniente leve y los completamente devastadores: esto puede implicar pérdida de datos importantes, violación de la privacidad y hasta varias horas o incluso días de inactividad de la red.

Pese a los riesgos costosos de las potenciales violaciones a la seguridad, Internet puede ser uno de los medios más seguros para realizar negocios. Por ejemplo, suministrar información de la tarjeta de crédito a un vendedor telefónico o a un mozo de un restaurante puede ser más arriesgado que enviar la información por un sitio Web, ya que las transacciones de comercio electrónico están generalmente protegidas con una tecnología de seguridad.
Los mozos y los vendedores telefónicos no siempre son supervisados ni son siempre personas confiables. Sin embargo, el temor a los problemas de seguridad puede ser tan perjudicial para los negocios como los son las violaciones reales a la seguridad.
El temor y el recelo general frente a las computadoras está latente y por consiguiente genera una desconfianza de Internet. Esta desconfianza puede limitar las oportunidades comerciales para las empresas, especialmente las que se basan completamente en la Web. De este modo, las empresas deben promulgar políticas de seguridad y estipular resguardos que no sólo sean efectivos sino que también se perciban como tales.
Las organizaciones deben estar en condiciones de comunicar en la forma adecuada cómo planean proteger a sus clientes.

Aparte de brindar protección a los clientes, las empresas deben proteger a sus empleados y socios ante las violaciones a la seguridad. Internet, intranet y extranet permiten una comunicación rápida y efectiva entre empleados y socios. No obstante, tanto la comunicación como la eficiencia pueden verse impedidas por los efectos de un ataque a las redes. Un ataque puede directamente generar varias horas de inactividad para los empleados y las redes se deben desconfigurar para reparar el daño o restaurar la información. Es evidente que la pérdida de datos importantes y de un tiempo valioso pueden ocasionar un gran impacto en la moral y la eficiencia de los empleados.

La legislación es otra fuerza que impulsa la necesidad de la seguridad de las redes. Los gobiernos reconocen la importancia de Internet y el hecho de que una considerable parte de la producción económica mundial depende de ella. Sin embargo, también reconocen que abrir la infraestructura económica mundial para que esté a merced de los abusos de delincuentes podría ocasionar un perjuicio económico considerable. Por lo tanto, los gobiernos nacionales están desarrollando leyes que tienen la finalidad de regular el gran flujo de información económica. Asimismo, a fin de cumplir con las reglamentaciones promulgadas por los gobiernos, el sector informático ha desarrollado una serie de normas de seguridad para proteger los datos y probar que están seguros. Las empresas que no cuenten con políticas de seguridad demostrables para proteger los datos estarán violando estas normas y recibirán la sanción correspondiente.

“Me he dado cuenta de que los problemas en la seguridad de la red generalmente se deben a una falla en la implementación de las políticas de seguridad y en el uso de las herramientas de seguridad a las que se puede acceder fácilmente. Es de vital importancia que las empresas cumplan con las evaluaciones de riesgo profesional y desarrollen infraestructuras y planes globales de seguridad públicamente avalados por la más alta gerencia.”
—Mark Carter, COO, CoreFacts, LLC, Empresa de análisis y recuperación de información.

Amenazas a los datos

Tal como sucede con cualquier tipo de delito, las amenazas a la privacidad e integridad de los datos proviene de una pequeña minoría de vándalos. Sin embargo, mientras que un ladrón de automóviles puede robar solamente un vehículo por vez, un único hacker que trabaja desde una computadora básica puede ocasionar daño en una gran cantidad de redes y desatar un caos en todo el mundo.

Quizás más preocupante aún es el hecho de que las amenazas pueden proceder de personas conocidas. En realidad, muchos de los expertos en seguridad de redes aducen que la mayoría de los ataques a las redes son iniciados por empleados que trabajan en las empresas donde han ocurrido violaciones a la seguridad. Ya sea por travesura, rencor o equivocación, generalmente los empleados se las ingenian para atacar las redes de las empresas donde trabajan y destruir la información.

Además, con la reciente incorporación de las tecnologías de conectividad remota, los negocios se están expandiendo para incluir gran cantidad de trabajadores a distancia, sucursales y socios de negocios. Si los activos de los sistemas de redes remotos no tienen el control ni la seguridad correspondiente, estos socios y empleados remotos plantean las mismas amenazas que los empleados internos y también presentan el riesgo de violaciones a la seguridad.

Ya sea que le interese asegurar un vehículo, una propiedad, una nación o una red, es esencial contar con un conocimiento general de quiénes son sus potenciales enemigos y cómo actúan.

¿Quiénes son los enemigos?

Hackers

Este término genérico y a menudo idealizado se aplica a los entusiastas de la computación a quienes les encanta acceder a las redes o computadoras de otras personas. A muchos hackers les agrada simplemente acceder sin autorización a las computadoras de escritorio y dejar sus “huellas” mediante mensajes o aplicaciones ocurrentes para probar su hazaña. Otros hackers, generalmente conocidos como “crackers”, son más perniciosos, producen la paralización de sistemas informáticos íntegros, hurtan o estropean información confidencial, descompaginan páginas Web y en última instancia desestabilizan los negocios. Algunos hackers aficionados simplemente posicionan las herramientas de pirateo en línea y las implementan sin comprender demasiado cómo funcionan y cuáles son los efectos que producen.

Personal desprevenido

Debido a que los empleados se concentran en sus obligaciones laborales específicas, generalmente suelen descuidar reglas estándar relacionadas con la seguridad de la red. Por ejemplo, pueden elegir contraseñas que son fáciles de recordar para poder conectarse a las redes fácilmente. No obstante, los hackers pueden adivinar o craquear fácilmente estas contraseñas usando el sentido común o con un programa de craqueo de contraseñas. Los empleados pueden inconscientemente ocasionar otras violaciones a la seguridad, incluyendo la exposición y difusión accidental de virus informáticos. Una de las formas más comunes de contraer un virus es a través de un disco flexible o de la descarga de archivos de Internet. Los empleados que usan discos flexibles para transferir información pueden involuntariamente infectar las redes de la empresa con virus contraídos de computadoras de bibliotecas o centros de copiado. Es probable que ni siquiera ellos mismos sepan que los virus se encuentran en sus PC. Las empresas también se enfrentan al riesgo de infección cuando los empleados descargan archivos de Internet, como presentaciones de PowerPoint.

Sorprendentemente, las empresas también deben estar alertas ante errores humanos. Los empleados, ya sean principiantes o expertos en computación, pueden cometer errores tales como instalar equivocadamente un software de protección antivirus o accidentalmente pasar por alto advertencias relacionadas con las amenazas a la seguridad.

“El noventa y nueve por ciento de los encuestados descubrieron abuso de los privilegios de acceso a Internet por parte de los empleados.”
—Encuesta anual realizada por el Computer Security Institute y el FBI, 2001

Personal descontento

Mucho más perturbadora que la probabilidad de un error por parte de un empleado que pudiera afectar la red, es la posibilidad de que un miembro del personal esté enojado o quiera vengarse e inflija un daño. Los empleados disgustados, generalmente porque fueron reprendidos, suspendidos o despedidos del trabajo, pueden vengarse infectando las redes de la empresa con virus o intencionalmente eliminar archivos importantes. Este grupo es especialmente peligroso porque en general tiene más conocimiento de la red, de la importancia

del contenido de la información, de la ubicación estratégica de la información considerada de alta prioridad y los resguardos establecidos para protegerla.

Curiosos

Algunos empleados, tanto conformes como descontentos, también pueden ser curiosos o traviesos. Los empleados identificados como "curiosos" participan en espionajes de la empresa, accediendo sin autorización a datos confidenciales a fin de facilitar a la competencia información que de otra forma sería inaccesible. Otros empleados simplemente satisfacen su curiosidad personal accediendo a información personal y privada, como datos financieros, mensajes amorosos de correo electrónico entre compañeros de trabajo o el sueldo de un compañero de trabajo. Algunas de estas actividades puede resultar relativamente inofensivas pero otras, como revisar datos financieros, el historial de un paciente o información de recursos humanos, son mucho más graves, pueden ser perjudiciales para las reputaciones y generar una responsabilidad económica por parte de la empresa.

¿Qué pueden hacer estos enemigos?

Virus

Los virus son las amenazas a la seguridad más conocidas porque generalmente cuentan con amplia cobertura de prensa.
Los virus son programas informáticos generados por programadores malintencionados y están diseñados para que se reproduzcan solos e infecten a las computadoras cuando un evento específico los active. Por ejemplo, los virus denominados virus de macro atacan a los archivos con instrucciones de macro (rutinas que se pueden repetir automáticamente, como ser combinaciones de correspondencia) y se activan cada vez que la macro se ejecuta.
Los efectos de algunos virus son relativamente benignos y provocan interrupciones molestas, tal como la presentación de un mensaje gracioso cada vez que se pulsa una determinada letra del teclado.
Otros virus son más destructivos y ocasionan problemas tales como la eliminación de archivos de un disco duro o la desaceleración de un sistema.

Una red puede verse infectada por un virus sólo si el mismo ingresa a la red por una fuente externa: muchos virus suelen proceder de un disco flexible infectado o de un archivo descargado de Internet. Cuando una computadora de la red está infectada, las demás computadoras son más propensas a contraer el virus.

"El 85 por ciento de los encuestados descubrió violaciones a la seguridad de las computadoras ocurridas durante el último año, lo que redunda en un incremento del 42 por ciento en comparación con el año 1996."
—Encuesta anual realizada por el Computer Security Institute y el FBI, 2001

Programas troyanos

Los programas troyanos, o caballos de troya, son instrumentos de distribución para código destructivo. Los troyanos parecen programas útiles o inofensivos, por ejemplo juegos de computadora, pero en realidad son enemigos encubiertos. Estos programas pueden eliminar datos, enviar copias de sí mismos a listas de direcciones de correo electrónico y acceder a computadoras para realizar otros ataques. Los troyanos sólo pueden contraerse al copiar el programa a un sistema mediante un disco, al realizar descargas de Internet o al abrir un archivo adjunto de correo electrónico. Ni los troyanos ni los virus pueden difundirse por un mensaje de correo electrónico: sólo se propagan por los archivos adjuntos de correo electrónico.

Vándalos

Los sitios Web se han vuelto más animados a partir del desarrollo de aplicaciones de software tales como Active X y applets (subprogramas) de Java. Estos dispositivos habilitan la animación y la ejecución de otros efectos especiales, logrando que los sitios Web sean más atractivos e interactivos. Sin embargo, la facilidad de descarga y ejecución de estas aplicaciones ha proporcionado un nuevo medio para producir daños. Un vándalo consiste en un subprograma o una aplicación de software que causa destrozos de diversas magnitudes. Un vándalo puede destruir un único archivo o una gran parte de un sistema informático.

Ataques

Se ha documentado una gran cantidad de ataques a redes que normalmente se clasifican en tres categorías generales: ataques de reconocimiento, ataques de acceso y ataques de denegación de servicio (DoS).

- Los ataques de reconocimiento consisten básicamente en actividades para reunir información que permiten a los hackers recopilar datos que se usan para luego poner en peligro las redes. Generalmente, las herramientas de software, como los husmeadores y buscadores, se emplean para

delimitar los recursos de red y explotar las potenciales debilidades de las redes, los hosts y las aplicaciones objetivo. Por ejemplo, existe software específicamente diseñado para craquear contraseñas. Dicho software se creó para que los administradores de red puedan brindar asistencia a los empleados que hayan olvidado las contraseñas o para descubrir las contraseñas de los empleados que dejaron la empresa sin informar a nadie cuáles eran sus contraseñas. No obstante, si cae en manos equivocadas, este software puede llegar a ser un arma peligrosa.

- Los ataques de acceso se realizan para explotar vulnerabilidades en las áreas de red, tales como los servicios de autenticación y la funcionalidad del Protocolo de transferencia de archivos (FTP), a fin de poder acceder a las cuentas de correo electrónico, las bases de datos y otras clases de información confidencial.
- Los ataques DoS impiden el acceso a todo el sistema informático o a una parte del mismo. Generalmente se logran mediante el envío de una gran cantidad de datos mezclados o incontrolables a una máquina que está conectada a una red de la empresa o a Internet, bloqueando el acceso del tráfico legítimo. Aún más perjudicial es el ataque de denegación de servicio distribuido (DDoS), mediante el cual el agresor compromete varias máquinas o hosts.

Intercepción de datos

Los datos transmitidos a través de cualquier tipo de red pueden ser interceptados por personas no autorizadas. Los perpetradores pueden realizar escuchas de las comunicaciones o incluso alterar los paquetes de datos que se transmiten. Los perpetradores pueden emplear diversos métodos para interceptar la información. Por ejemplo, el falseo de la dirección IP de origen (IP spoofing) consiste en hacerse pasar por persona autorizada en la transmisión de datos por medio del uso de la dirección IP (Protocolo de Internet) de uno de los receptores de la información.

Ingeniería social

La ingeniería social es el acto con cada vez mayor prevalencia para obtener información confidencial de seguridad de la red por medios no técnicos. Por ejemplo, un ingeniero social podría darse a conocer como un representante de soporte técnico y llamar a los empleados para que reúnan la información de las contraseñas. Otros ejemplos de ingeniería social incluyen sobornar a un compañero de trabajo para acceder a un servidor o revisar la oficina de un compañero para encontrar una contraseña anotada en un sitio oculto.

Correo no solicitado (Spam)

El término *spam* es comúnmente utilizado para referirse al correo electrónico no solicitado o a la acción de difundir mensajes publicitarios no solicitados a través del correo electrónico. El *spam* generalmente es inofensivo pero puede ser una molestia porque ocupa el espacio de almacenamiento y el tiempo del receptor.

Herramientas de seguridad

Una vez identificadas las potenciales fuentes de amenazas y los tipos de peligros que pueden ocurrir, resulta mucho más fácil ordenar las políticas de seguridad y los resguardos apropiados. Las organizaciones cuentan con una gran variedad de tecnologías, desde paquetes de software antivirus hasta hardware dedicado a la seguridad de red, como los sistemas de detección de intrusiones y los servidores de seguridad o *firewalls*, a fin de brindar protección a todas las áreas de la red.

Al igual que un edificio, una red requiere varios niveles de protección para ser completamente segura.

Una vez establecidas estas soluciones, se pueden implementar herramientas que periódicamente detecten las vulnerabilidades en la seguridad de la red garantizando seguridad proactiva y continua. Además, se pueden contratar consultores profesionales de seguridad de redes para que brinden asesoramiento en el diseño de la solución de seguridad conveniente para la red o para garantizar que la solución de seguridad existente esté actualizada y sea segura. Con todas estas opciones disponibles, es posible implementar una infraestructura de seguridad que permita la protección suficiente sin sacrificar demasiado la necesidad de acceder a la información en forma ágil y sencilla.

Los diez mejores consejos de seguridad

1. Sugerir o exigir a los empleados que elijan contraseñas que no sean evidentes.
2. Obligar a los empleados a cambiar las contraseñas cada 90 días.
3. Asegurarse de que la suscripción del antivirus esté vigente.
4. Instruir a los empleados sobre los riesgos de seguridad de los archivos adjuntos de correo electrónico.
5. Implementar una solución de seguridad de la red que sea completa y global.
6. Evaluar periódicamente la postura de seguridad.
7. Bloquear el acceso a la red a los empleados que dejan de pertenecer a la empresa en forma inmediata.
8. Si hay personas que están autorizadas a trabajar desde sus casas, proveer un servidor seguro y con administración centralizada para el tráfico remoto.
9. Actualizar regularmente el software del servidor Web.
10. No ejecutar ningún servicio de red innecesario.

Paquetes de antivirus

El software de protección contra virus viene con muchas computadoras y puede detener muchas amenazas de virus si se realiza una actualización periódica del mismo y su mantenimiento es óptimo.
La industria de los antivirus se basa en una amplia red de usuarios que le suministra advertencias oportunas ante la presencia de nuevos virus, de manera tal que se puedan desarrollar y distribuir los antídotos rápidamente. Debido a que todos los meses se generan miles de virus nuevos, es de vital importancia que la base de datos de virus se mantenga actualizada. El paquete de antivirus contiene una base de datos de virus que poder identificar los virus conocidos cuando intentan atacar. Los proveedores de software antivirus más conocidos publican en sus sitios Web las últimas novedades en antídotos y el software puede indicarles a los usuarios que periódicamente recopilen nuevos datos.
La política de seguridad de la red debería estipular que todas las computadoras de la red estén actualizadas y preferentemente que todas tengan instalado el mismo paquete de antivirus, aunque sea para que los costos de mantenimiento y actualización sean mínimos.
Es también fundamental actualizar periódicamente el software. Generalmente, para los autores de los virus la prioridad fundamental es no ser detectados por el antivirus.

Políticas de seguridad

Al configurar una red, ya sea una red de área local (LAN), una LAN virtual (VLAN) o una red de área extensa (WAN), es importante establecer desde el principio las políticas de seguridad. Las políticas de seguridad son reglas electrónicamente programadas y almacenadas en equipos de seguridad para controlar áreas tales como los privilegios de acceso. Obviamente, las políticas de seguridad también consisten en reglamentaciones escritas o verbales que delimitan el funcionamiento de una organización. Además, las empresas deben asignar a la persona responsable de implementar y administrar estas políticas, determinar el modo en que se informará a los empleados acerca de las reglas y realizar los controles necesarios.

La administración de la política de seguridad, del dispositivo y de los dispositivos múltiples funciona como una sala de control de seguridad central donde el personal custodia la seguridad del edificio o campus, inicia patrullas y activa alarmas.

¿En qué consisten las políticas?

Las políticas implementadas deben controlar quién accede a determinadas áreas de la red y cómo impedir que usuarios no autorizados ingresen a zonas restringidas. Por ejemplo, es común que sólo los integrantes del departamento de recursos humanos puedan acceder a los historiales de sueldo de los empleados. Las contraseñas generalmente impiden que los empleados accedan a zonas restringidas, pero solamente si tales contraseñas

se mantienen en confidencialidad. Las políticas escritas tan básicas como advertir a los empleados que no dejen por escrito sus contraseñas en áreas de trabajo, pueden prevenir las violaciones a la seguridad. Los clientes o proveedores con acceso a determinadas partes de la red también deben regirse por las políticas de reglamentación.

¿Quién implementará y administrará las políticas?

Los individuos o grupos de personas que custodian y mantienen la red y la seguridad de la misma deben tener acceso a todas las áreas de la red. Por lo tanto, la función de administración de la política de seguridad debe asignarse a personas de confianza y con el conocimiento técnico necesario. Tal como se mencionó anteriormente, la mayoría de las violaciones a la seguridad se realizan internamente, por lo tanto este individuo o equipo no debe ser una amenaza en potencia. Una vez asignados, los administradores de red deben aprovechar las herramientas de software sofisticado que pueden servir para definir, distribuir, implementar y auditar las políticas de seguridad a través de interfaces basadas en explorador.

¿Cómo se comunicarán las políticas?

Las políticas carecen de sentido si no las conocen y comprenden todas las partes involucradas. Es fundamental que existan mecanismos eficientes para comunicar las políticas existentes, los cambios de políticas, las nuevas políticas y las alertas de seguridad con relación a ataques o virus inminentes.

Identidad

Une vez establecidas las políticas, se deben emplear las tecnologías y los métodos de identificación que contribuyan a la autenticación positiva y a la verificación de los usuarios y sus privilegios de acceso.

Los servidores de control de acceso funcionan como las tarjetas de acceso de las puertas y el personal de vigilancia que supervisa la seguridad del sitio, suministrando autorización centralizada, autenticación y contabilidad para tráfico y usuarios (AAA).

Contraseñas

La forma más simple y común de asegurarse de que sólo los individuos con la autorización pertinente accedan a una zona determinada de la red, es mediante la “protección con contraseña” de dichas áreas, lo que significa que sólo podrán acceder las personas que tengan contraseñas específicas para tal fin. En la analogía de seguridad física anterior, las contraseñas son comparables a las tarjetas de identificación para el acceso. No obstante, las infraestructuras más poderosas de seguridad de redes son prácticamente ineficaces si las personas no protegen sus contraseñas. Muchos usuarios eligen como contraseñas palabras o números fáciles de recordar, como fechas de cumpleaños, números de teléfono o nombres de mascotas y otros no cambian las contraseñas ni tienen la precaución de mantenerlas en reserva. Las políticas o reglas de oro para las contraseñas son:

- Cambiar las contraseñas en forma periódica
- Elegir contraseñas con poco sentido
- Nunca dar a conocer las contraseñas a nadie hasta no pertenecer más a la empresa

En el futuro algunas contraseñas podrán reemplazarse por biométrica, que es la tecnología que identifica a los usuarios en base a características físicas, como huellas digitales, impresiones oculares o de voz.

Certificados digitales

Los certificados digitales o los certificados de claves públicas son los equivalentes electrónicos de los pasaportes o las licencias de conductor y se emiten por Autoridades certificadoras (CA) específicas.
Los certificados digitales comúnmente se usan para identificación al establecer túneles seguros por Internet, tal como sucede en la red privada virtual (VPN).

Control de acceso

Antes de que un usuario pueda acceder a la red con su contraseña, la red debe evaluar si la contraseña es válida. Los servidores de control de acceso validan la identidad del usuario y determinan cuáles son las áreas o la información a la que el usuario puede acceder en base a los perfiles almacenados de usuarios. En la analogía de seguridad física, los servidores de control de acceso son equivalentes al personal de vigilancia que supervisa el uso de la tarjeta de acceso.

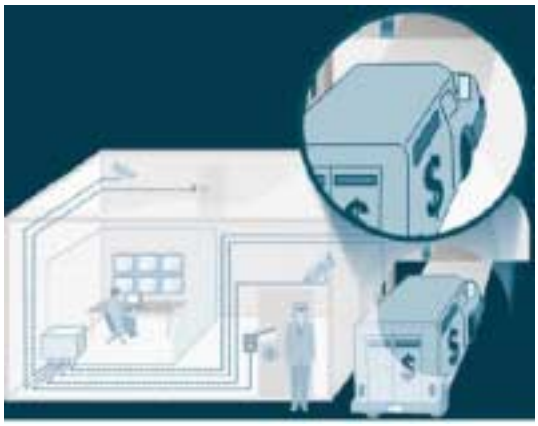
Los servidores de seguridad o firewalls y las listas de control de acceso se asemejan a cerraduras de las puertas en el perímetro de los edificios que permiten solamente el acceso a los usuarios autorizados (los que tengan claves o identificaciones).

Servidores de seguridad o firewalls

Un *firewall* es una solución de software o hardware implementada en la infraestructura de red para imponer las políticas de seguridad de una organización mediante el acceso restringido a recursos de red específicos. En la analogía de seguridad física, un *firewall* es el equivalente a la cerradura en la puerta exterior del edificio o en la puerta de una sala dentro del edificio, ya que sólo los usuarios autorizados, es decir, los que tienen una tarjeta de acceso o llave, puedan ingresar. La tecnología del *firewall* también está disponible en versiones adecuadas al uso doméstico. El *firewall* crea una capa protectora entre la red y el mundo exterior. De hecho, el *firewall* copia la red en el punto de entrada para que pueda recibir y transmitir datos autorizados sin una demora prolongada.
No obstante, contiene filtros integrados que pueden impedir el acceso al sistema real de material potencialmente peligroso o no autorizado. También registra una intrusión frustrada y la reporta a los administradores de red.

Cifrado

La tecnología de cifrado garantiza que sólo el receptor autorizado pueda leer o interceptar los mensajes. Generalmente, el cifrado se utiliza para proteger los datos que se transmiten por una red pública y emplea algoritmos matemáticos avanzados para “codificar” los mensajes y los archivos adjuntos. Existen diversos tipos de algoritmos de cifrado pero algunos son más seguros que otros. El cifrado ofrece la seguridad necesaria para sustentar la tecnología VPN cada vez más popular. Las VPN son conexiones privadas o túneles de las redes públicas, como Internet. Se utilizan para que trabajadores a distancia, empleados móviles, sucursales y socios de negocios puedan conectarse entre sí o a las redes corporativas. Todos los dispositivos de hardware y software VPN admiten tecnología de cifrado avanzada para ofrecer la mayor protección para los datos que transfieren.



Las redes privadas virtuales (VPN) se asemejan a los vehículos blindados que trasladan cargamento valioso a un punto de descarga asignado para garantizar el traslado seguro y confidencial.

Detección de intrusiones

Las organizaciones siguen empleando *firewalls* como los dispositivos de control y administración central para impedir que usuarios no autorizados accedan a las redes. No obstante, la seguridad de la red es en cierto modo similar a la seguridad física en el hecho de que ninguna tecnología cubre las necesidades; en cambio, una defensa en capas proporciona los mejores resultados. Las organizaciones están considerando cada vez más tecnologías adicionales de seguridad para contrarrestar el riesgo y la vulnerabilidad que los servidores de seguridad no pueden resolver por sí solos. Un sistema de detección de intrusiones (IDS) basado en la red mantiene la red vigilada las veinticuatro horas del día. El IDS analiza las secuencias de datos de paquetes en una red, busca actividad no autorizada, como ataques de hackers, y permite que los usuarios reaccionen frente a las violaciones de seguridad antes de que los sistemas se expongan al peligro. Cuando se detecta actividad no autorizada, el IDS puede enviar alarmas a una consola de administración con detalles de la actividad y es posible que ordene a otros sistemas, como los enrutadores, la interrupción de las sesiones no autorizadas. En la analogía física, un IDS equivale a una cámara de video y a un sensor de movimiento que detecta la actividad sospechosa o no autorizada y funciona con sistemas de respuesta automatizada que, como los guardias de seguridad, detienen la actividad.

La detección de intrusiones es similar a un sensor de movimiento o a una cámara de vigilancia que detecta actividad, activa alertas y genera una respuesta armada. El análisis es como un guardia de seguridad que controla y cierra las puertas o ventanas abiertas antes de que sean violadas.

Análisis de redes

Los escáneres de redes realizan análisis detallados de los sistemas de redes para recopilar un inventario electrónico de los activos y detectar vulnerabilidades que podrían llegar a poner en riesgo la seguridad. Esta tecnología permite que los administradores de redes identifiquen y solucionen debilidades en la seguridad antes de que los intrusos puedan aprovecharlas. En la analogía de seguridad física, el análisis es similar a la inspección periódica de un edificio para confirmar que las puertas estén trabadas y las ventanas cerradas. Sirve para evaluar y comprender el riesgo, permitiendo por consiguiente que se tomen las medidas correctivas.

Experiencia

Si bien las herramientas de análisis electrónico pueden ser muy exhaustivas para detectar las vulnerabilidades de seguridad de la red, se pueden complementar con una evaluación de seguridad a cargo de consultores profesionales en seguridad. Una evaluación de seguridad consiste en un análisis concentrado de la postura de seguridad de una red, que destaca las vulnerabilidades o las debilidades en la seguridad en las que se debe trabajar. Las evaluaciones periódicas sirven para asegurar que la postura de seguridad de la red no se debilite en medio de los cambios que resultan tan frecuentes. En la analogía de seguridad física, una evaluación periódica de seguridad, tal como el análisis, es como un guardia que patrulla regularmente toda la zona asegurada, controlando que puertas y ventanas estén cerradas, informando todas las irregularidades que encuentra y ofreciendo orientación para la corrección.

El resultado

A medida que el tiempo transcurra, se desarrollarán cada vez más tecnologías nuevas para mejorar la eficiencia de los negocios y de las comunicaciones. Al mismo tiempo, las innovaciones tecnológicas ofrecerán aún más seguridad a la red, y consecuentemente, más tranquilidad para operar en entornos comerciales de vanguardia. Siempre que las empresas permanezcan a la vanguardia en esta tecnología emergente y se mantengan siempre alertas frente a las amenazas a la seguridad y los peligros, los beneficios de las redes superarán sin duda alguna los riesgos.

¿Desea obtener más información?

Para obtener más información acerca de seguridad de redes y del modo en que las tecnologías y los productos de Cisco Systems ayudan a solucionar problemas de seguridad y para aprovechar la cantidad de beneficios que las redes ofrecen, visite el sitio Web de Cisco Systems en http://www.cisco.com/go/security

Oficina Central Corporativa
Cisco Systems, Inc.
170 West Tasman Drive
San José, CA 95134-1706
EE.UU.
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Oficina Central para Europa
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
Países bajos
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Oficina Central para América
Cisco Systems, Inc.
170 West Tasman Drive
San José, CA 95134-1706
EE.UU.
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Oficina Central para Asia y el Pacífico
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 a #29-01
Singapur 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems tiene más de 200 oficinas en los siguientes países y regiones. Las direcciones, números de teléfono y fax se pueden encontrar en el Sitio

Web de Cisco en www.cisco.com/go/offices

Argentina • Australia • Austria • Bélgica • Brasil • Bulgaria • Canadá • Chile • República Popular China • Colombia • Costa Rica • Croacia • República Checa • Dinamarca • Dubai, Emiratos Árabes Unidos • Finlandia • Francia • Alemania • Grecia • Hong Kong RAE • Hungría • India • Indonesia • Irlanda • Israel • Italia • Japón • Corea • Luxemburgo • Malasia • México • Países Bajos • Nueva Zelanda • Noruega • Perú • Filipinas • Polonia • Portugal • Puerto Rico • Rumania • Rusia • Arabia Saudita • Escocia • Singapur • Eslovaquia • Eslovenia • Sudáfrica • España • Suecia • Suiza • Taiwán • Tailandia • Turquía • Ucrania • Reino Unido • Estados Unidos • Venezuela • Vietnam • Zimbabwe