CAPITULO 8

SEGURIDAD Y CONTROL DE SISTEMAS DE INFORMACIÓN

Vulnerabilidad y abuso de los sistemas

Los sistemas de información concentran los datos en archivos de computadoras a los que podrían tener fácil acceso un gran número de personas y grupos externos a la organización. Por ello, los datos automatizados son más susceptibles a destrucción, fraude, error y abuso. Cuando los sistemas de computación fallan o no funciona como es debido, las compañías que dependen mucho de ellos experimentan una pérdida grave de su capacidad para operar.

Si usted opera un negocio, necesita hacer de la seguridad y el control sus principales prioridades. La seguridad se refiere a las políticas, procedimientos y medidas técnicas utilizadas para impedir el acceso no autorizado, la alteración, el robo o el daño físico a los sistemas de información.

¿Por qué son vulnerables los sistemas?

Cuando se almacenan grandes cantidades de datos en forma electrónica, estos son vulnerables a muchos tipos de amenazas a los que no están expuestos los datos asentados en papel. Los adelantos en telecomunicaciones software de computadora han intensificado esta vulnerabilidad. Gracias a las redes de telecomunicación es posible que haya acceso no autorizado, abuso o fraude, no estando limitado a un solo lugar, sino que puede darse en cualquier punto de acceso a la red. Las redes inalámbricas son aún más vulnerables a la penetración, porque es fácil explorar las bandas de radiofrecuencia.

Las amenazas pueden derivarse de factores técnicos, organizacionales y del entorno combinados con decisiones administrativas deficientes. En el entorno de computación cliente/servidor multicapa existen vulnerabilidades en cada capa y en las comunicaciones que tienen lugar entre las capas. Los usuarios en la capa del cliente pueden causar daño al introducir errores, acceder al sistema sin autorización, o descargar spyware y virus sin darse cuenta.

Los hackers pueden, acceder a los datos valiosos durante su transmisión o alterar mensajes sin autorización. Internet y otras redes son altamente vulnerables a alteraciones por la radiación.

Los sistemas tienen un mal funcionamiento si el hardware de cómputo se descompone, si no está configurado apropiadamente o si está dañado por un uso inadecuado o por actos delictivos. Las fallas de energía, los incendios u otros desastres naturales pueden alterar los sistemas de cómputo.

Sin fuertes medidas de seguridad, los datos valiosos se pueden perder o destruir, o caer en manos equivocadas y revelar secretos comerciales importantes o información que viole la privacidad personal.

Vulnerabilidades de internet

Es más vulnerable que las redes internas porque están abiertas a todo el mundo. Cuando las redes corporativas se enlazan a internet, los sistemas de información son vulnerables a ataques de extraños.

Las computadoras conectadas constantemente a internet están más abiertas a la intrusión de extraños que las que permanecen menos tiempo. En las conecciones de banda ancha están conectadas más tiempo, los ataques se pueden realizar con más rapidez, y en las líneas DSL que ofrecen direcciones IP fijas a los clientes, es más fácil establecer la identidad de una computadora local.

La mayor parte del tráfico de voz sobre IP en internet no está encriptado, por lo que los hackers pueden escuchar potencialmente las conversaciones en un gran número de puntos desde el módem de la red de área local (LAN) hasta los servidores vecinos.

El correo electrónico podrían contener archivos adjuntos que sirven como trampolín para el software malicioso o acceso no autorizado a los sistemas corporativos internos.

Las aplicaciones de mensajería instantánea no utilizan una capa de seguridad para los mensajes de texto, por lo que éstos pueden ser interceptados y leídos por extraños durante la trasmisión sobre Internet. En algunos casos, las actividades de mensajería instantánea sobre internet se puede utilizar como puerta trasera a una red que de otra manera sería segura.

Retos de seguridad de los servicios inalámbricos

No es seguro conectarse a una red de puntos activos Wi-Fi, porque estas redes están abiertas y no aseguradas, lo que significa que cualquiera puede acceder a ellas, y la comunicación entre su computadora portátil y el servidor inalámbrico no está encriptada.

Con frecuencia, las redes inalámbricas de los hogares no están aseguradas mediante encriptación, y los hackers que pasen por su casa pueden utilizar fácilmente su red y escuchar sus comunicaciones con su ruteador inalámbrico. Incluso los dispositivos de comunicaciones Bluetooth tienen evidentes fallas en la seguridad de sus comunicaciones.

Las LANs que emplean el estándar 802.11 pueden ser fácilmente penetradas por extraños equipados con computadoras portátiles, tarjetas inalámbricas, antenas externas y software de piratería informática. Los hackers utilizan estas herramientas para detectar redes desprotegidas, monitorear el tráfico de red y, en algunos casos, obtener acceso a internet o a redes corporativas.

La tecnología de trasmisión Wi-Fi fue diseñada para facilitar que las estaciones se encontraran y escucharan entre sí. ***Los identificadores de conjuntos de servicios*** (SSIDs) que identifican los puntos de acceso en una red Wi-Fi se difunden múltiples veces y pueden ser detectados con mucha facilidad por los programas husmeadores de los intrusos. Guerra móvil es aquello donde los espía conducen cerca de los edificios e intentan interceptar el tráfico de una red inalámbrica.

Un hacker puede emplear una herramienta de análisis 802.11 para identificar el SSID. Un intruso que se ha asociado con un punto de acceso utilizando el SSID correcto puede acceder a otros recursos de la red y emplear el Windows para determinar qué otros usuarios están conectados a la red, acceder a los discos duros de sus Pc y abrir o copiar sus archivos.

Los intrusos pueden utilizar la información para establecer puntos de acceso ilegales en un canal de radio diferente en ubicaciones físicas cercanas a los usuarios para obligar a la NIC de radio de un usuario a asociarse con el punto de acceso ilegal. Una vez que se realice esta asociación, los hackers que utilicen el punto de acceso ilegal pueden captar los nombres y contraseñas de usuarios sin que éstos lo sospechen.

WEP Privacidad Equivalente Alámbrica básica requiere que un punto de acceso y todos sus usuarios compartan la misma contraseña encriptada de 40 bits, la cual puede ser fácilmente descifrada por los hackers a partir de una pequeña cantidad de tráfico.

Software malicioso

Los programas de software malicioso se conocen como ***malware*** e incluyen una diversidad e amenazas como virus de computación, gusanos y troyanos.

♣ ***Virus de computadora*** es un programa de software malintencionado al que se adjunta a sí mismo a otros programas de software o archivos de datos con el propósito de ejecutarse, sin conocimiento o permiso del usuario. La mayoría de los virus trasmiten una carga útil, que podría se benigna o sumamente destructiva. Por lo general, los virus se esparcen de pc a pc cuando los usuarios realizan una acción.

♣ ***Gusanos*** son programas de computadora independientes que se copian a sí mismos de una computadora a otras de una red. Funcionan por sí mismos sin adjuntarse a otros archivos de programas de computadora y dependen menos de los actos humanos para esparcirse. Estos destruyen datos y programas, así como alteran o incluso detienen el funcionamiento de las redes de computadoras.

Ahora los virus y los gusanos se están esparciendo a los dispositivos de computación inalámbricos. El gusano Cabir busca continuamente otros dispositivos de bluetooth y con el tiempo descarga la bateria de un dispositivo. Los virus de dispositivos móviles plantean serias amenazas a la computación empresarial porque en la actualidad hay muchos dispositivos inalámbricos enlazados a sistemas de información corporativos.

♣ ***Caballo de troya*** es un programa de software que aparenta ser benigno pero que hace algo distinto a lo esperado. Constituye una manera para que los virus y otro código malicioso sean introducidos en un sistema de cómputo.

Algunos tipos de ***spyware*** actúan como software malicioso. Estos programas se instalan subrepticiamente a sí mismos en las computadoras para vigilar las actividades de navegación del usuario en la web y presentar publicidad.
El spyware ofrece a los extraños la posibilidad de invadir su privacidad y robar su identidad personal.
Registradores de claves registran cada tecleo ingresado en una computadora para robar números seriales de software, para lanzar ataques por internet. Otros programas de spyware cambian las páginas de inicio del navegador web, redirigen las solicitudes de búsqueda o disminuyen el desempeño de la computadora al apoderarse de mucha memoria.

Hackers y cibervandalismo
Hacker es la persona que accede sin autorización a una red de computadoras, para lucrar, causar daños, o por placer personal.
Cracker es un hacker con intenciones criminales.
Las actividades de un hacker van más allá de una mera intrusión a los sistemas para incluir el robo de bienes e información, así como el daño de los sistemas y el cibervandalismo.
Cibervandalismo es la alteración intencional, destrozo o incluso la destrucción de un sitio Web o un sistema de información corporativo.
Spoofing puede involucrar la redirección de un enlace web a una dirección diferente de la que se pretende, con el sitio camuflado como la dirección pretendida y así poder recopilar y procesar pedidos, robando información empresarial así como información delicada de los clientes del sitio verdadero.
Sniffing es un tipo de programa que vigila la información que viaja a través de una red. Cuando se utilizan de manera legal, los sniffer ayudan a identificar puntos potencialmente problemáticos en la red o actividades delictivas en las redes, pero cuando se emplean con propósitos criminales, pueden ser perjudiciales y muy difíciles de detectar.
Ataques de negación de servicios (Denial of Service)los hacker inundan un servidor de red o de Web con muchos miles de comunicaciones o solicitudes de servicios falsas para que la red deje de funcionar. La red recibe tantas consultas que no pueden atenderlas todas y en consecuencia queda fuera de servicio para atender las solicitudes legítimas. Ocasionan que sobresature un sitio web imposibilitando a los usuarios legítimos el acceso.
Ataque distribuido de negación del servicio (Distributed Denial of Service)se utilizan cientos o incluso miles de Pcs para inundar o agobiar la red desde numerosos puntos de lanzamiento. Se utilizan Pcs zombies infectadas con software malicioso y organizadas en una ***botnet***. Al infectarlas abre un acceso trasero a través del cual un atacante puede dictar instrucciones, que la pc infectada obedecerá. Una vez que se infectan suficientes Pcs, pueden utilizar los recursos acumulados de la botnet para iniciar ataques distribuidos de negación del servicio, campañas de correo electrónico no solicitado.

Delito informático y ciberterrorismo
La mayor parte de las actividades de un hacker son delitos penales, y las vulnerabilidades de los sistemas los convierten en objetivos de otros tipos de delitos informáticos. Un delito informático es cualquier violación al código penal que involucre un conocimiento de tecnología de cómputo para su perpetración, investigación o prosecución.
Los tipos de delitos más perjudiciales desde el punto de vista económico son los ataque Dos, la introducción de virus, el robo de servicios y la alteración de los sistemas de cómputo.

♣ ***Robo de identidad:*** es un delito en el cual el impostor obtiene fracciones de información personal clave, como nº de tarjetas de crédito, con el propósito de hacerse pasar por alguien más.

Los comercios electrónicos son fuentes estupendas de información personal de los clientes. Provistos de esta información, los delincuentes pueden asumir nuevas identidades y obtener nuevos créditos para sus propios fines.

Phishing implica el establecimiento de sitios web falso o el envío de mensajes de correo electrónico semejantes a los de las empresas auténticas para solicitar a los usuarios datos personales confidenciales. El mensaje de correo electrónico da instrucciones a los receptores para que actualicen o confirmen registros suministrando nº "claves", ya sea respondiendo al mensaje de correo electrónico , ingresando la información en un sitio web falso o llamando a un nº telefónico. Existen nuevas técnicas de phishing difíciles de detectar como:

● ***Evil twins*** son redes inalámbricas que fingen ofrecer conexiones Wi-Fi confiables a internet. Los defraudadores tratan de capturar contraseñas o nº de tarjetas de crédito de los usuarios involuntarios que entran a la red.

●***Pharming*** redirige a los usuarios a una página web falsa, aún cuando estos ingresen la dirección correcta de la página web en su navegador. Esto es posible si los autores del pharming obtienen acceso a la información de las direcciones de internet almacenadas por los proveedores de servicios de internet con el fin de acelerar la navegación y si los prestadores cuentan con software deficiente en sus servidores que permiten a los defraudadores realizar actividades de piratería y cambiar las direcciones.

♣ ***Fraude del clic*** ocurre cuando un individuo o un programa de computadora hace clic de manera fraudulenta en un anuncio en línea sin la intención de conocer más sobre el anunciante o de realizar una compra.

Algunas empresas contratan a terceros para hacer clic de manera fraudulenta en los anuncios de un competidor con el propósito de debilitarlo al provocar que se incrementen sus costos de Marketing. El fraude del clic también se puede realizar con programas de software que hacen el clic, y con frecuencia se utilizan las redes de robots con este propósito.

♣ ***Ciberterrorismo y ciberarmamento*** Las vulnerabilidades de internet y de otras redes pueden ser aprovechadas por terroristas, servicios de inteligencia extranjeros u otros grupos para crear disturbios y daños generalizados. Se cree que algunos países están desarrollando capacidades de ciberarmamento ofensivo y defensivo.

Amenazas internas

Los empleados de una empresa plantean serios problemas de seguridad, dado que tienen acceso a información privilegiada, y si existen procedimientos de seguridad ineficientes, pueden tener la oportunidad de escudriñar en todos los sistemas de la organización sin dejar huellas

La falta de conocimiento de los usuarios es la principal causa individual de las brechas de seguridad en las redes. Muchos olvidan las contraseñas para acceder a los sistemas de cómputo o permiten a sus colegas que las utilicen, lo cual pone en riesgo al sistema. Los intrusos que buscan acceso al sistema en ocasiones engañan a los empleados para que les proporcionen sus contraseñas fingiendo que son miembros legítimos de la organización y requieren información. Esta práctica se conoce como ingeniería social.

Los usuarios finales introducen errores al ingresar datos erróneos o al no seguir las instrucciones apropiadas para el procesamiento de datos y el uso del equipo de cómputo. Los especialistas en sistemas de información podrían crear errores de software a medida que diseñan y desarrollan nuevo software o cuando dan mantenimiento a los programas existentes.

Por lo general, el software comercial contiene defectos que no sólo producen vulnerabilidades de desempeño sino de seguridad que dan acceso a las redes para los intrusos. Estas vulnerabilidades dan al malware la oportunidad de superar las defensas de los antivirus.

Para corregir los defectos del software una vez que se han identificados, el fabricante del software crea pequeñas piezas de software conocidas como parches para reparar los defectos sin alterar el funcionamiento adecuado del software.

A los usuarios les toca detectar estas vulnerabilidades, probarlas y aplicar todos los parches. Este proceso se conoce como administración de parches.
El malware es creado con tanta rapidez que las empresas tienen muy poco tiempo para responder entre el momento en que se anuncia la existencia de una vulnerabilidad y de su parche correspondiente, y el momento en que aparece software malicioso para explotar esa vulnerabilidad.

Valor del negocio en relación con la seguridad y el control

Las empresas tienen activos de información muy valiosos que deben proteger. Si estos se perdieran, destruyeran o cayeran en manos equivocadas podrían tener repercusiones devastadoras.
La seguridad y control inadecuados también pueden dar lugar a serios problemas de responsabilidad legal. Las empresas deben proteger no sólo sus propios activos de información, sino también los de sus clientes, empleados, socios de negocios. En caso contrario, la empresa podría verse involucrada en costosos litigios por exposición o robo de datos. En consecuencia, una sólida estructura de seguridad y control que proteja los activos de información del negocio pueden generar un alto rendimiento de la inversión.

Requerimientos legales y regulatorios para la administración de registros electrónicos

La administración de registros electrónicos consta de políticas, procedimientos y herramientas para manejar la conservación, destrucción y almacenamiento de registros electrónicos.
Puesto que los sistemas de información se utilizan para generar, almacenar y transportar este tipo de datos, la legislación obliga a las empresas a que consideren la seguridad de los sistemas de información y otros controles necesarios para garantizar la integridad, confidencialidad y exactitud de sus datos. Cada una de las aplicaciones de sistemas que maneje datos críticos para la elaboración de informes financieros requiere controles para proteger la red corporativa, prevenir el acceso no autorizado a los sistemas y los datos, y garantizar la integridad y disponibilidad de los datos en el caso de un desastre o de otra interrupción del servicio.
Si trabaja en una empresa que cotiza en bolsa, deberá apegarse a la ley Sarbanes-Oxley que impone la responsabilidad a las empresas y sus administraciones de salvaguardar la exactitud e integridad y disponibilidad de los datos en el caso de un desastre o de otra interrupción del servicio.

Evidencia electrónica y cómputo forense

La seguridad, el control y la administración de registros electrónicos se han vuelto esenciales para responder en situaciones legales. En la actualidad, los juicios se apoyan cada vez más, en información de páginas impresas o escritas a máquina, en pruebas en forma de datos digitales almacenados en discos flexibles, CDs y discos duros de computadoras, así como en correo electrónico, mensajes instantáneos y transacciones de comercio electrónico a través de Internet. El correo electrónico es el tipo más común de evidencia electrónica.
En una situación legal la empresa está obligada a responder una solicitud de revelación para acceder la información que pudiera ser utilizada como prueba, y por ley debe producir esos datos.
Los cortes imponen ahora multas financieras severas e incluso penas judiciales por la destrucción inapropiada de documentos electrónicos, anomalías en la generación de registros y fallas en el almacenamiento adecuado de registros.
Una política efectiva de conservación de documentos electrónicos garantiza que los documentos electrónicos, el correo electrónico y otros registros estén bien organizados, sean accesibles y nunca se conserven demasiado tiempo ni se eliminen tan pronto.
El cómputo forense consiste en la recopilación, examen, autenticación, preservación y análisis de los datos contenidos o recuperados de los medios de almacenamiento de una computadora en forma tal que la información se pueda utilizar como prueba en un tribunal de justicia, como:

● Recuperación de datos de las computadoras, conservando la integridad de la prueba.
● Almacenar y manejar de manera segura los datos electrónicos recuperados.
● Encontrar información significativa en grandes volúmenes de datos electrónicos
● Presentar la información a un tribunal de justicia

La evidencia electrónica podría residir en el medio de almacenamiento de una computadora en forma de archivos de computadora y como datos del ambiente, que no son visibles para el usuario promedio.

Es necesario incluir una previsión sobre le cómputo forense en el proceso de planeación de contingencias de una empresa.

Establecimiento de una estructura para la seguridad y el control

La protección de los recursos de información requiere una sólida política de seguridad y un conjunto de controles. ISO 17799 proporciona lineamientos útiles. Especifica mejores prácticas en seguridad y control de sistemas de información, incluyendo política de seguridad, planeación de continuidad del negocio, seguridad física, control de acceso, conformidad y creación de una función de seguridad dentro de la organización.

Evaluación del riesgo

Determina el nivel de peligro para la empresa si una actividad o un proceso no están debidamente controlados. Se pueden determinar el valor de los activos de información, los puntos de vulnerabilidad, la frecuencia probable de un problema y los daños potenciales.

Una vez que se han evaluado los riesgos, los desarrolladores de sistemas se concentrarán en los puntos de control que tengan la mayor vulnerabilidad y potencial de pérdidas. En este caso, los controles deben enfocarse en buscar normas de minimizar el riesgo de fallas de energía y errores del usuario (ej del libro tabla 8.3).

Política de seguridad

Consta de enunciados que clasifican los riesgos de seguridad, identifican los objetivos de seguridad aceptables y determinan los mecanismos para alcanzar estos objetivos. La administración debe calcular cuánto costará alcanzar este nivel de riesgo aceptable.

En empresas grandes el grupo de seguridad instruye y capacita a los usuarios, mantiene la administración al tanto de las amenazas y fallas de seguridad, y da mantenimiento a las herramientas elegidas para implementar la seguridad. El director de seguridad es el responsable de aplicar la política de seguridad.

Una política de uso aceptable define los usos aceptables de los recursos de la información y el equipo de cómputo de la empresa, incluyendo las computadoras de escritorio y las portátiles, los dispositivos inalámbricos, los teléfonos e internet. La política debe dejar en claro la postura de la empresa respecto de la privacidad, la responsabilidad del usuario y el uso personal del equipo y las redes de la empresa. Una buena política de uso aceptable define los actos aceptables e inaceptables para cada usuario y especifica las consecuencias del incumplimiento.

Las políticas de autorización determinan diferentes niveles de acceso a los activos de información para los distintos niveles de usuarios.

Los sistemas de administración de autorizaciones establecen dónde y cuando se le permite a un usuario acceder a ciertas partes de un sitio Web o de una base de datos corporativa. Estos sistemas permiten a cada usuario acceder solamente a aquellas partes de un sistema para las cuales tiene autorización, con base en la información establecida por un conjunto de reglas de acceso. El sistema de administración de autorizaciones sabe exactamente a cuál información tiene permitido acceder cada usuario.

Aseguramiento de la continuidad del negocio

Las empresas necesitan emprender pasos adicionales para asegurar que sus sistemas estén siempre disponibles.

En el proceso de transacciones en línea, la computadora procesa inmediatamente las transacciones que se ingresen en línea. A cada instante se realizan enormes cantidades de cambios a bases de datos, elaboración de informes y solicitudes de información.

Los sistemas de cómputo tolerantes a fallas contienen hardware, software y componentes de suministro de energía redundantes que forman un entorno de servicio continuo e ininterrumpido. Las computadoras tolerantes a fallas utilizan rutinas de software especiales o lógica de autoverificación integrada en su sistema de circuitos para detectar fallas de hardware y cambiar automáticamente a un dispositivo de respaldo. Algunas partes de esas computadoras se pueden quitar y reparar sin interrumpir el funcionamiento del sistema de cómputo.
Tanto la tolerancia a fallas como el cómputo de alta disponibilidad procuran reducir el tiempo de caída, que es el período durante el cual el sistema no funciona. Sin embargo, el **cómputo de alta disponibilidad** ayuda a las empresas a recuperarse rápidamente de una caída del sistema, en tanto que la tolerancia a fallas promete una disponibilidad ininterrumpida junto con la eliminación del tiempo de recuperación.
La computación de alta disponibilidad requiere servidores de respaldo, distribución del procesamiento entre múltiples servidores, almacenamiento de alta capacidad y buenos planes para la recuperación de desastres y para la continuidad del negocio. La plataforma de cómputo de la empresa debe ser sumamente robusta, con potencia de procesamiento, almacenamiento y ancho de banda escalables.

La computación orientada a la recuperación incluye el diseño de sistemas que se recuperen con rapidez, así como capacidades de implementación y herramientas que ayuden a los operadores a identificar las fuentes de fallas en los sistemas conformados por múltiples componentes y a corregir fácilmente sus errores.

Planeación para la recuperación de desastres y la continuidad del negocio
Concibe planes para la restauración de los servicios de cómputo y comunicaciones después de que han sido interrumpidos por algún suceso. Estos planes se enfocan en los aspectos técnicos involucrados en mantener los sistemas en funcionamiento, cómo cuáles archivos se deben respaldar, y en el mantenimiento de los sistemas de cómputo de respaldo o los servicios de recuperación de desastres.
La planeación para la continuidad del negocio se enfoca en establecer formas en que la empresa puede restaurar las operaciones de negocios después de que ocurre un desastre. El plan identifica los procesos de negocios críticos y determina los planes de acción para manejar las funciones de misión crítica si se caen los sistemas.
Subcontratación de seguridad muchas empresas pueden subcontratar una variedad de funciones de seguridad a proveedores de servicios de seguridad administrados que vigilan la actividad de la red y realizan pruebas de vulnerabilidad y detección de intrusiones.

El rol de la auditoría

Una auditoría de MIS examina el entorno de seguridad general de la empresa así como los controles que rigen los sistemas de información individuales. El auditor debe rastrear el flujo de transacciones de muestra a través del sistema y realizar pruebas, utilizando, si es necesario, software de auditoría automatizado.
Las auditorias de seguridad revisan tecnologías, procedimientos, documentación, capacitación y personal. Una auditoría completa simulará incluso un ataque o un desastre para probar la respuesta de la tecnología, el personal de sistemas de información y los empleados de la empresa.
La auditoría enlista y clasifica todas las debilidades de control y calcula la probabilidad de que sucedan, luego evalúa el impacto financiero y organizacional de cada amenaza. Para finalizar, notificando tales debilidades a la administración para que esta dé una respuesta, a través de un plan para contrarrestar las debilidades significativas de los controles.

Tecnologías y herramientas para la seguridad

Control de acceso consiste en todas las políticas y procedimientos de que se vale una empresa para prevenir el acceso inapropiado a los sistemas por parte de los usuarios internos y externos no autorizados. Para tener acceso un usuario debe estar autorizado y autenticado. La autenticación se refiere a la capacidad de saber que una persona es quien afirma ser.
Con frecuencia la autenticación se establece por medio de contraseñas que sólo los usuarios conocen. Tenemos nuevas tecnologías de autenticación como:
● ***Token*** es un dispositivo físico, semejante a una tarjeta de identificación, diseñado para comprobar la identidad de un solo usuario
● ***Tarjeta inteligente*** es un dispositivo del tamaño de una tarjeta de crédito que contiene un chip programado con permisos de acceso y otros datos. Un dispositivo lector interpreta los datos de la tarjeta y permite o niega el acceso.
● ***Autenticación biométrica*** utiliza sistemas que leen e interpretan rasgos humanos individuales, como las huellas digitales, la voz, para otorgar o denegar el acceso. Esta técnica compara las características únicas de una persona contra un perfil almacenado de estas características para determinar si existen diferencias entre estas y el perfil almacenado. Si coinciden se le otorga el acceso.

Firewalls, sistemas de detección de intrusiones y software antivirus

Un firewalls es una combinación de hardware y software que controla el flujo del tráfico que entra y sale de una red. Por lo general, se coloca entre las redes internas privadas de una organización y las redes externas poco confiables, como internet, aunque los firewalls se pueden utilizar para proteger una parte de la red de una empresa del resto de la red
El firewalls identifica nombres, direcciones IP, aplicaciones y otras características del tráfico que entra. Comprueba esta información contra las reglas de acceso que el administrador de la red ha programado en el sistema. El firewall evita las comunicaciones no autorizadas, tanto al interior como al exterior de la red.
Filtrado de paquetes examina campos seleccionados en los encabezados de los paquetes de datos que fluyen entre la red confiable e internet, y analiza los paquetes individuales de manera aislada. La inspección complete del estado proporciona seguridad adicional al determinar si los paquetes son parte de un diálogo continuo entre el emisor y un receptor. Establece tablas de estado para rastrear la información a través de múltiples paquetes. Éstos son aceptados o rechazados al evaluar si son parte de una conversación aprobada o si están tratando de establecer una conexión legítima.
Traducción de direcciones de red (NAT): NAT oculta las direcciones IP de las computadoras de host internas de la organización para evitar que los programas sniffers que se encuentran fuera del firewall las detecten y las utilicen para penetrar en los sistemas internos.
Filtrado proxy de aplicación examina el contenido de aplicación de los paquetes. Un servidor proxy detiene los paquetes de datos que se originan fuera de la organización, los inspecciona y los pasa a un proxy al otro lado del firewall.
Para crear un buen firewall, un administrador debe mantener reglas internas detalladas que identifiquen a los usuarios, las aplicaciones o direcciones que tienen permiso o que se rechazan. Los firewalls no impiden completamente la penetración de la red por parte de los usuarios externos y se deben considerar como un elemento de un plan de seguridad global.
Sistema de detección de intrusiones contienen herramientas de vigilancia de tiempo completo que se colocan en los puntos más vulnerables de las redes corporativas para detectar y disuadir a los intrusos. El sistema genera una alarma si encuentra un suceso sospechoso o anómalo. También se puede personalizar para que apague una parte delicada de una red si recibe tráfico no autorizado.
El software antivirus está especialmente diseñado para revisar los sistemas de computación y discos en búsqueda de diversos virus de computadora. Este tipo de software sólo es eficaz contra virus que ya se conocían cuando se escribió el programa. Para proteger sus sistemas, la gerencia debe actualizar continuamente su software antivirus.

Potección de redes inalámbricas

WEP proporciona un pequeño margen de seguridad si los usuarios de Wi-Fi recuerdan activarlo. Las corporaciones pueden mejorar aún más la seguridad de Wi-Fi utilizándola en conjunto con tecnología de red privada virtual (VNP) cuando accedan a los datos internos de la corporación.
El estándar 802.11i emplea autenticación mutua para evitar que un usuario del servicio inalámbrico sea atraído a una red falsa que podría robar las credenciales de red del usuario. Se revisan los paquetes de datos para asegurar que forman parte de una sesión actual de la red y que los hackers no los repitan para engañar a los usuarios.
Para ser efectiva, la tecnología de seguridad inalámbrica debe ir acompañada de políticas y procedimientos apropiados para el uso seguro de los dispositivos inalámbricos.

Infraestructura de encriptación y clave pública

La encriptación es el proceso de transformar textos o datos comunes en texto cifrado que no puede ser leído por nadie más que por el emisor y el receptor al que va destinado.
El Protocolo de Capa de Conexión Segura (SSL) y Seguridad de la Capa de Transporte (TLS) permiten a las computadoras cliente y servidor manejar las actividades de encriptación y desencriptación a medida que se comunican entre sí durante una sesión segura en la Web.
El Protocolo de Transferencia de Hipertexto (S-HTTP) es un protocolo que se utiliza para encriptar los datos que fluyen a través de internet, pero está limitado a mensajes individuales, en tanto que SSL y TLS están diseñados para establecer una conexión segura entre dos computadoras.
Existen dos modos de encriptación alternativos: la ***encriptación de clave simétrica***, donde el emisor y el receptor establecen una sesión segura en internet por medio de la creación de una sola clave de encriptación, que se envía al receptor de tal manera que tanto el emisor como el receptor compartan la misma clave. El problema es que la clave misma debe ser compartida de alguna manera entre los emisores y los receptores, lo cual la expone a extraños que podrían interceptarla y desencriptarla.
La ***encriptación de clave pública*** utiliza dos claves: una compartida y otra privada. Las claves están matemáticamente relacionadas, de tal forma que los datos encriptados con una clave sólo se pueden desencriptar con la otra clave. Para enviar y recibir mensajes, los comunicadores primero crean pares separados de claves privadas y públicas. La clave pública se conserva en un directorio y la clave privada debe mantenerse en secreto. El emisor encripta un mensaje con la clave pública del receptor. Al recibir el mensaje, el receptor utiliza su clave privada para desncriptarlo.

Las firmas digitales y los certificados apoyan la autenticación. Una firma digital es un mensaje encriptado que sólo el emisor puede crear con su clave privada. Se emplea para verificar el origen y el contenido de un mensaje.
Los certificados digitales son archivos de datos utilizados para establecer la identidad de los usuarios y archivos electrónicos para la protección de las transacciones en línea. Un sistema de certificados digitales recurre a un tercero confiable, conocido como autoridad de certificación, para validar la identidad de un usuario.
El sistema de certificación digital podría permitir, que un usuario de tarjeta de crédito y un comerciante validaran que sus respectivos certificados digitales fueran emitidos por un tercero autorizado y confiable antes de intercambiar datos.
La infraestructura de clave pública, el uso de la criptografía de clave pública que funciona con una autoridad de certificación, se utiliza de manera generalizada en el comercio electrónico.