Seguridad Informática

La **seguridad informática** es la disciplina que se Ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos.
consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Principios de Seguridad Informática:
Para lograr sus objetivos la seguridad informática se fundamenta en tres principios, que debe cumplir todo sistema informático:

Confidencialidad: Se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático, Basándose en este principio, las herramientas de seguridad informática deben proteger el sistema de invasiones y accesos por parte de personas o programas no autorizados. Este principio es particularmente importante en sistemas distribuidos, es decir, aquellos en los que los usuarios , computadores y datos residen en localidades diferentes , pero están física y lógicamente interconectados.

Integridad: Se refiere a la validez y consistencia de los elementos de información almacenados y procesador en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben asegurar que los procesos de actualización estén bien sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos. Este principio es importante en sistemas descentralizados, es decir, aquellos en los que diferentes usuarios , computadores y procesos comparten la misma información.

Disponibilidad: Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deber reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran, este principio es importante en sistemas informáticos cuyos compromiso con el usuario, es prestar servicio permanente.

Factores de Riesgo:

Ambientales/Físicos : factores externos , lluvias, inundaciones , terremotos, tormentas, rayos, humedad, calor entre otros.

Tecnológicos: Fallas de hardware y/o software, fallas en el aire acondicionado, falla en el servicio eléctrico, ataque por virus informático, etc.

Humanos: hurto, adulteración, fraude, modificación, revelación, pérdida, sabotaje, vandalismo, crackers, hackers, falsificación, robo de contraseñas, alteraciones etc.

Mecanismos de seguridad

Un mecanismo de seguridad informática es una técnica o herramienta que se utiliza para fortalecer la confidencialidad , la integridad y/o la disponibilidad de un sistema informático.

Existen muchos y variados mecanismos de seguridad informática. Su selección depende del tipo de sistema, de su función y de los factores de riesgo que lo amenazan.

Clasificación según su función:

Preventivos: Actúan antes de que un hecho ocurra y su función es detener agentes no deseados.

Detectivos: Actúan antes de que un hecho ocurra y su función es revelar la presencia de agentes no deseados en algún componente del sistema. Se caracterizan por enviar un aviso y registrar la incidencia.

Correctivos: Actúan luego de ocurrido el hecho y su función es corregir la consecuencias.

Según un informe del año 1991 del Congressional Research Service, las computadoras tienen dos características inherentes que las dejan abiertas a ataques o errores operativos

1.-Una computadora hace exactamente lo que está programada para hacer, incluyendo la revelación de información importante. Un sistema puede ser reprogramado por cualquier persona que tenga los conocimientos adecuados.

2.-Cualquier computadora puede hacer sólo aquello para lo que está programada , no puede protegerse a sí misma contra un mal funcionamiento o un ataque deliberado a menos que este tipo de eventos haya sido previsto de antemano y se hayan puesto medidas necesarias para evitarlos.

Los propietarios de computadoras y los administradores utilizan una gran variedad de técnicas de seguridad para protegerse:

1. Restricciones al acceso Físico: Esta consiste en la aplicación de barreras y procedimientos de control , como medidas de prevención y contramedidas ante amenazas a los recursos de información confidencial.

Se refiere a los controles y mecanismos de seguridad dentro y alrededor del dentro de computo así como los medios de accesos remoto al y desde el mismo, implementados para proteger el

hardware y medios de almacenamiento de datos. Una forma de reducir las brechas de seguridad es asegurarse de que sólo las personas autorizadas pueden acceder a una determinada máquina. Las organizaciones utilizan una gran variedad de herramientas técnicas para identificar a su personal autorizado. Las computadoras pueden llevar a cabo ciertas comprobaciones de seguridad, los guardias de seguridad humanos otras. En función del sistema de seguridad implementado, podrá acceder a un sistema en función a:

- ✓ **Algo que tenga:** Una llave, una tarjeta de identificación con una fotografía o una tarjeta inteligente que contenga una identificación digital codificada almacenada en un chip de memoria.
- ✓ **Algo que conozca:** una contraseña, un número de identificación, una combinación de bloqueo o algo de su historial personal.
- ✓ **Algo que haga:** Su firma o su velocidad de escritura y los patrones de error.
- ✓ **Verificación Automática de Firmas (VAF)**

  En este caso lo que se considera es lo que el usuario es capaz de hacer, aunque también podría encuadrarse dentro de las verificaciones biométricas.

  Mientras es posible para un falsificador producir una buena copia visual o facsímil, es extremadamente difícil reproducir las dinámicas de una persona: por ejemplo la firma genuina con exactitud.

  La VAF, usando emisiones acústicas toma datos del proceso dinámico de firmar o de escribir. La secuencia sonora de emisión acústica generada por el proceso de escribir constituye un patrón que es único en cada individuo. El patrón contiene información extensa sobre la manera en que la escritura es ejecutada.

  El equipamiento de colección de firmas es inherentemente de bajo costo y robusto. Esencialmente, consta de un bloque de metal (o algún otro material con propiedades acústicas similares) y una computadora barata.

Sistema Biométrico: La Biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas., La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Los lectores biométricos identifican a la persona **por lo que es** (manos, ojos, huellas digitales y voz).

Los Beneficios de una Tecnología Biométrica Pueden eliminar la necesidad de poseer una tarjeta para acceder. Aunque las reducciones de precios han disminuido el costo inicial de las tarjetas en los últimos años, el verdadero beneficio de eliminarlas consiste en la reducción del trabajo concerniente a su administración.

Utilizando un dispositivo biométrico los costos de administración son más pequeños, se realiza el mantenimiento del lector, y una persona se encarga de mantener la base de

datos actualizada. Sumado a esto, las características biométricas de una persona son intransferibles

Huella Digital Basado en el principio de que no existen dos huellas dactilares iguales, este sistema viene siendo utilizado desde el siglo pasado con excelentes resultados. Cada huella digital posee pequeños arcos, ángulos, bucles, remolinos, etc. (llamados minucias) características y la posición relativa de cada una de ellas es lo analizado para establecer la identificación de una persona. Esta aceptado que dos personas no tienen más de ocho minucias iguales y cada una posee más de 30, lo que hace al método sumamente confiable.

Verificación de Voz: La dicción de una (o más) frase es grabada y en el acceso se compara la vos (entonación, diptongos, agudeza, etc.). Este sistema es muy sensible a factores externos como el ruido, el estado de animo y enfermedades de la persona, el envejecimiento, etc.

Verificación de Patrones Oculares: Estos modelos pueden estar basados en los patrones del iris o de la retina y hasta el momento son los considerados más efectivos (en 200 millones de personas la probabilidad de coincidencia es casi 0).

Contraseñas

Las contraseñas son las herramientas más utilizadas para restringir el acceso a los sistemas informáticos. Sin embargo, sólo son efectivas si se escogen con cuidado, la mayor parte de los usuarios de computadoras escogen contraseñas que son fáciles de adivinar: El nombre de la pareja, el de un hijo o el de una mascota, palabras relacionadas con trabajos o aficiones o caracteres consecutivos del teclado. Un estudio descubrió que las contraseñas favoritas en el Reino Unido son Fred-God, mientras que en América eran, Love- sexy, . Los hackers conocen y explotan estos clichés, por lo que un usuario precavido no debe.

Normas de Elección de Claves

Se debe tener en cuenta los siguientes consejos:

1. No utilizar contraseñas que sean palabras (aunque sean extranjeras), o nombres (el del usuario, personajes de ficción, miembros de la familia, mascotas, marcas, ciudades, lugares, u otro relacionado).
2. No usar contraseñas completamente numéricas con algún significado (teléfono, D.N.I., fecha de nacimiento, patente del automóvil, etc.).
3. No utilizar terminología técnica conocida.

4. Elegir una contraseña que mezcle caracteres alfabéticos (mayúsculas y minúsculas) y numéricos.
5. Deben ser largas, de 8 caracteres o más.
6. Tener contraseñas diferentes en máquinas diferentes y sistemas diferentes. Es posible usar una contraseña base y ciertas variaciones lógicas de la misma para distintas máquinas. Esto permite que si una password de un sistema cae no caigan todos los demás sistemas por utilizar la misma password.
7. Deben ser fáciles de recordar para no verse obligado a escribirlas. Algunos ejemplos son:
    - Combinar palabras cortas con algún número o carácter de puntuación
    - Usar un acrónimo de alguna frase fácil de recordar
    - Añadir un número al acrónimo para mayor seguridad
    - Mejor incluso si la frase no es conocida elegir una palabra sin sentido, aunque pronunciable
    - Realizar reemplazos de letras por signos o números.

Firewalls

Quizás uno de los elementos más publicitados a la hora de establecer seguridad, sean estos elementos. Aunque deben ser uno de los sistemas a los que más se debe prestar atención, distan mucho de ser la solución final a los problemas de seguridad.

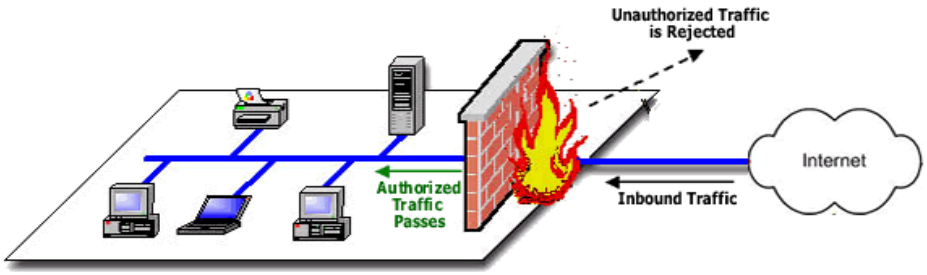
Los Firewalls están diseñados para proteger una red interna contra los accesos no autorizados. En efecto , un firewall es un ***Gatewa****y* con un bloqueo (la puerta bloqueada solo se abre para los paquetes de información que pasan una o varias inspecciones de seguridad), estos aparatos solo lo utilizan las grandes corporaciones

Un *gateway* (puerta de enlace) es un dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino. **Es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior**

Un Firewall es un sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce la una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet).

Puede consistir en distintos dispositivos, tendientes a los siguientes objetivos:

1. Todo el tráfico desde dentro hacia fuera, y viceversa, debe pasar a través de él.
2. Sólo el tráfico autorizado, definido por la política local de seguridad, es permitido.



El Firewall, sólo sirve de defensa perimetral de las redes, no defienden de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa.

Algunos Firewalls aprovechan esta capacidad de que toda la información entrante y saliente debe pasar a través de ellos para proveer servicios de seguridad adicionales como la encriptación del tráfico de la red. Se entiende que si dos Firewalls están conectados, ambos deben "hablar" el mismo método de encriptación-desencriptación para entablar la comunicación

Tipos de Firewall

1. Filtrado de Paquetes
2. Proxy-Gateways de Aplicaciones
3. Dual-Homed Host
4. Screened Host
5. Screened Subnet
6. Inspección de Paquetes

   Este tipo de Firewalls se basa en el principio de que cada paquete que circula por la red es inspeccionado, así como también su procedencia y destino. Se aplican desde la capa de Red hasta la de Aplicaciones. Generalmente son instalados cuando se requiere seguridad sensible al contexto y en aplicaciones muy complejas.
7. Firewalls Personales :Estos Firewalls son aplicaciones disponibles para usuarios finales que desean conectarse a una red externa insegura y mantener su

computadora a salvo de ataques que puedan ocasionarle desde un simple "cuelgue" o infección de virus hasta la pérdida de toda su información almacenada.

8.

- ✓ **Filtrado de paquetes:** El filtrado de paquetes mediante puertos y protocolos permite establecer que servicios estarán disponibles al usuario y por cuales puertos. Se puede permitir navegar en la WWW (puerto 80 abierto) pero no acceder a la transferencia de archivos vía FTP (puerto 21 cerrado).

  Debido a su funcionamiento y estructura basada en el filtrado de direcciones y puertos este tipo de Firewalls trabajan en los niveles de Transporte y de Red del Modelo OSI y están conectados a ambos perímetros (interior y exterior) de la red.

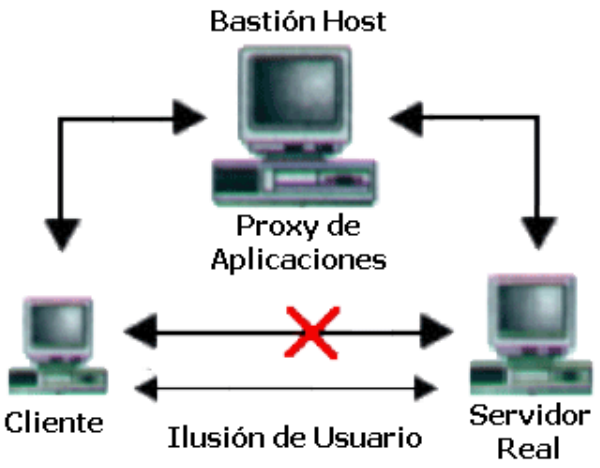
  Tienen la ventaja de ser económicos, tienen un alto nivel de desempeño y son transparentes para los usuarios conectados a la red. Sin embargo presenta debilidades como:

  1. No protege las capas superiores a nivel OSI.
  2. Las necesidades aplicativas son difíciles de traducir como filtros de protocolos y puertos.
  3. No son capaces de esconder la topología de redes privadas, por lo que exponen la red al mundo exterior.
  4. Sus capacidades de auditoría suelen ser limitadas, al igual que su capacidad de registro de actividades.
  5. No soportan políticas de seguridad complejas como autentificación de usuarios y control de accesos con horarios prefijados.

- ✓ **Proxy-Gateways de Aplicaciones:** Para evitar las debilidades asociadas al filtrado de paquetes, los desarrolladores crearon software de aplicación encargados de filtrar las conexiones. Estas aplicaciones son conocidas como Servidores Proxy y la máquina donde se ejecuta recibe el nombre de Gateway de Aplicación o Bastion Host.

  El Proxy, instalado sobre el Nodo Bastión, actúa de intermediario entre el cliente y el servidor real de la aplicación, siendo transparente a ambas partes.

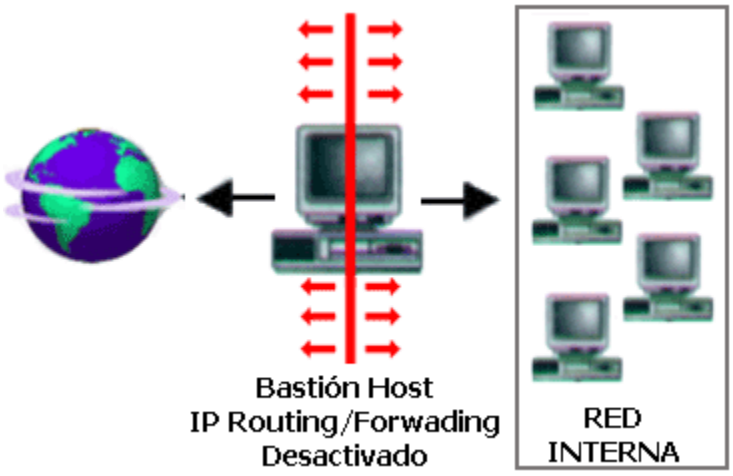
  Cuando un usuario desea un servicio, lo hace a través del Proxy. Este, realiza el pedido al servidor real devuelve los resultados al cliente. Su función fue la de analizar el tráfico de red en busca de contenido que viole la seguridad de la misma.



- ✓ **Dual-Homed Host** : Son dispositivos que están conectados a ambos perímetros (interior y exterior) y no dejan pasar paquetes IP (como sucede en el caso del Filtrado de Paquetes), por lo que se dice que actúan con el "IP-Forwarding desactivado".

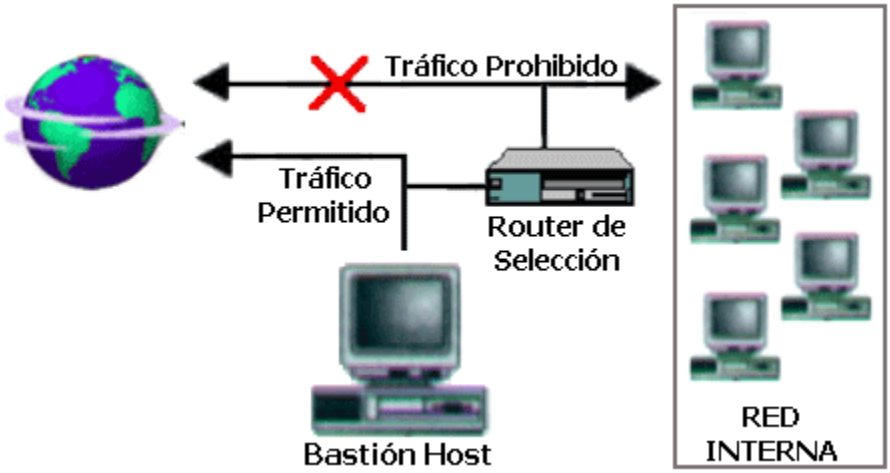
  Un usuario interior que desee hacer uso de un servicio exterior, deberá conectarse primero al Firewall, donde el Proxy atenderá su petición, y en función de la configuración impuesta en dicho Firewall, se conectará al servicio exterior solicitado y hará de puente entre este y el usuario interior.

  Es decir que se utilizan dos conexiones. Uno desde la máquina interior hasta el Firewall y el otro desde este hasta la máquina que albergue el servicio exterior.



- ✓ **Screened Host** : En este caso se combina un Router con un host bastión y el principal nivel de seguridad proviene del filtrado de paquetes. En el bastión, el

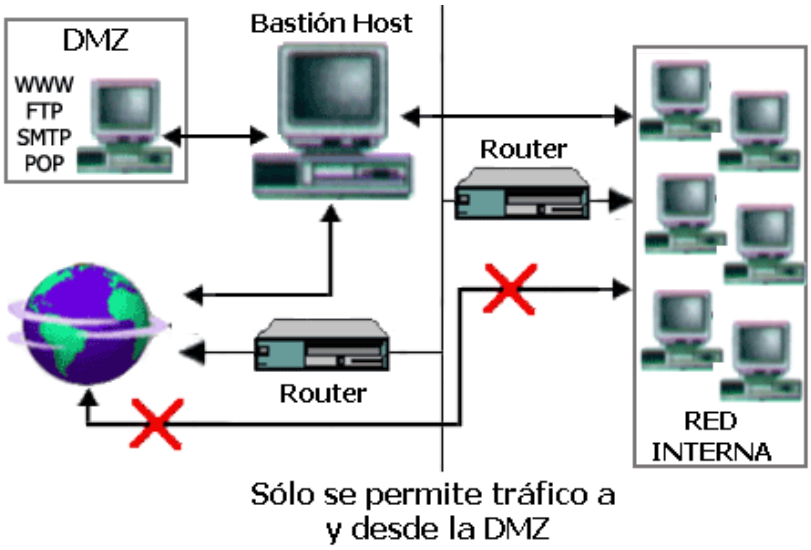
único sistema accesible desde el exterior, se ejecuta el Proxy de aplicaciones y en el Choke se filtran los paquetes considerados peligrosos y sólo se permiten un número reducido de servicios.



- ✓ **Screened Subnet:** En este diseño se intenta aislar la máquina más atacada y vulnerable del Firewall, el Nodo Bastión. Para ello se establece una Zona Desmilitarizada (DMZ) de forma tal que sin un intruso accede a esta máquina no consiga el acceso total a la subred protegida.

En este esquema se utilizan dos Routers: uno exterior y otro interior. El Router exterior tiene la misión de bloquear el tráfico no deseado en ambos sentidos: hacia la red interna y hacia la red externa. El Router interior hace lo mismo con la red interna y la DMZ (zona entre el Router externo y el interno).

Es posible definir varias niveles de DMZ agregando más Routers, pero destacando que las reglas aplicadas a cada uno deben ser distintas ya que en caso contrario los niveles se simplificarían a uno solo.



Como puede apreciarse la Zona Desmilitarizada aísla físicamente los servicios internos, separándolos de los servicios públicos. Además, n o existe una conexión directa entre la red interna y la externa. Los sistemas Dual-Homed Host y Screnned pueden ser complicados de configurar y comprobar, lo que puede dar lugar, paradójicamente, a importantes agujeros de seguridad en toda la red. En cambio, si se encuentran bien configurados y administrados pueden brindar un alto grado de protección y ciertas ventajas:

1. Ocultamiento de la información: los sistemas externos no deben conocer el nombre de los sistemas internos. El Gateway de aplicaciones es el único autorizado a conectarse con el exterior y el encargado de bloquear la información no solicitada o sospechosa.
2. Registro de actividades y autenticación robusta: El Gateway requiere de autenticación cuando se realiza un pedido de datos externos. El registro de actividades se realiza en base a estas solicitudes.
3. Reglas de filtrado menos complejas: Las reglas del filtrado de los paquetes por parte del Router serán menos compleja dado a que él sólo debe atender las solicitudes del Gateway.

Así mismo tiene la desventaja de ser intrusivos y no transparentes para el usuario ya que generalmente este debe instalar algún tipo de aplicación especializada para lograr la comunicación. Se suma a esto que generalmente son más lentos porque deben revisar todo el tráfico de la red.

Restricciones en el Firewall

La parte más importante de las tareas que realizan los Firewalls, la de permitir o denegar determinados servicios, se hacen en función de los distintos usuarios y su ubicación:

1. Usuarios internos con permiso de salida para servicios restringidos: permite especificar una serie de redes y direcciones a los que denomina **Trusted (validados)** . Estos usuarios, cuando provengan del interior, van a poder acceder a determinados servicios externos que se han definido.
2. Usuarios externos con permiso de entrada desde el exterior: este es el caso más sensible a la hora de vigilarse. Suele tratarse de usuarios externos que por algún motivo deben acceder para consultar servicios de la red interna.

También es habitual utilizar estos accesos por parte de terceros para prestar servicios al perímetro interior de la red. Sería conveniente que estas cuentas sean activadas y desactivadas bajo demanda y únicamente el tiempo que sean necesarias.

Beneficios de un Firewall

Los Firewalls manejan el acceso entre dos redes, y si no existiera, todos las computadoras de la red estarían expuestos a ataques desde el exterior. Esto significa que la seguridad de toda la red, estaría dependiendo de que tan fácil fuera violar la seguridad local de cada maquina interna.

El Firewall es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, el administrador será el responsable de la revisión de estos monitoreos.

Otra causa que ha hecho que el uso de Firewalls se haya convertido en uso casi imperativo es el hecho que en los últimos años en Internet han entrado en crisis el número disponible de direcciones IP, esto ha hecho que las intranets adopten direcciones sin clase, las cuales salen a Internet por medio de un "traductor de direcciones", el cual puede alojarse en el Firewall.

Los Firewalls también son importantes desde el punto de vista de llevar las estadísticas del ancho de banda "consumido" por el trafico de la red, y que procesos han influido más en ese trafico, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor el ancho de banda disponible.

Los Firewalls también tienen otros usos. Por ejemplo, se pueden usar para dividir partes de un sitio que tienen distintas necesidades de seguridad o para albergar los servicios WWW y FTP brindados.

Limitaciones de un Firewall

La limitación más grande que tiene un Firewall sencillamente es el hueco que no se tapa y que coincidentemente o no, es descubierto por un intruso. Los Firewalls no son sistemas inteligentes, ellos actúan de acuerdo a parámetros introducidos por su diseñador, por ende si un paquete de información no se encuentra dentro de estos parámetros como una amenaza de peligro simplemente lo deja pasar. Más peligroso aún es que ese intruso deje Back Doors, abriendo un hueco diferente y borre las pruebas o indicios del ataque original.

Otra limitación es que el Firewall "NO es contra humanos", es decir que si un intruso logra entrar a la organización y descubrir passwords o los huecos del Firewall y difunde esta información, el Firewall no se dará cuenta.

El Firewall tampoco provee de herramientas contra la filtración de software o archivos infectados con virus, aunque es posible dotar a la máquina, donde se aloja el Firewall, de antivirus apropiados.

Finalmente, un Firewall es vulnerable, él NO protege de la gente que está dentro de la red interna. El Firewall trabaja mejor si se complementa con una defensa interna. Como moraleja: "cuanto mayor sea el tráfico de entrada y salida permitido por el Firewall, menor será la resistencia contra los paquetes externos. El único Firewall seguro (100%) es aquel que se mantiene apagado".

Encriptación

Encriptación es el proceso mediante el cual cierta información o texto sin formato es cifrado de forma que el resultado sea ilegible a menos que se conozca los datos necesarios para su interpretación. Es una medida de seguridad utilizada para que al momento de almacenar o transmitir información sensible ésta no pueda ser obtenida con facilidad por terceros.

Opcionalmente puede existir además un proceso de desencriptación a través del cuál la información puede ser interpretada de nuevo a su estado original. Aunque existen métodos de encriptación que no pueden ser revertidos.

El termino encriptación es traducción literal del inglés y no existe en el idioma español, la forma mas correcta de utilizar este término sería Cifrado.

4.1 Criptología

La encriptación como proceso forma parte de la criptología, ciencia que estudia los sistemas utilizados para ocultar información, La criptología es la ciencia que estudia la transformación de un determinado mensaje en un código de forma tal que a partir de dicho código solo algunas personas sean capaces de recuperar el mensaje original.

4.2 Usos de las Encriptación

Algunos de los usos mas comunes de la encriptación son el almacenamiento y transmisión de información sensible como contraseñas, números de identificación legal, números de tarjetas crédito, reportes administrativos contables y conversaciones privadas, entre otros.

4.3 Métodos de Encriptación

Para poder encriptar un dato, se pueden utilizar tres procesos matemáticos diferentes. Los algoritmos HASH, los simétricos y los asimétricos.

4.3.1. Algoritmo HASH:

Este algoritmo efectúa un cálculo matemático sobre los datos que constituyen el documento y da como resultado un número único llamado MAC. Un mismo documento dará siempre un mismo MAC.

4.3.2. Criptografía de Clave Secreta o Simétrica

Utilizan una clave con la cual se encripta y desencripta el documento. Todo documento encriptado con una clave, deberá desencriptarse, en el proceso inverso, con la misma clave, es importante destacar que la clave debería viajar con los datos, lo que hace arriesgada la operación, imposible de utilizar en ambientes donde interactúan varios interlocutores.

Los Criptosistemas de clave secreta se caracterizan porque la clave de cifrado y de la descifrado es la misma, por tanto la robustez del algoritmo recae en mantener el secreto de la misma.

Sus principales características son:

-Rápidos y fáciles de implementar

-clave de cifrado y descifrado son la misma

-cada par de usuarios tiene que tener una clave secreta compartida

-una comunicación en la que intervengan múltiples usuarios requiere de muchas claves secretas distintas.

4.3.3. Algoritmos Asimétricos (RSA)

Requieren dos claves, una privada (única y personal, solo conocida por su dueño) y la otra llamada pública, ambas relacionadas por una fórmula matemática compleja imposible de reproducir. El concepto de criptografía de clave pública fue introducido por Whitfield Diffie y Martin Hellman a fin de solucionar la distribución de claves secretas de los sistemas tradicionales, mediante un canal inseguro. El usuario, ingresando su PIN genera clave Publicas y Privadas necesarias. La clave publica podrá ser distribuida sin ningún inconveniente entre todos los

4.5 Firma Digital:

La firma digital permite garantiza algunos conceptos de seguridad y son importantes al utilizar documentos en formato digital, tales como identidad o autenticidad, integridad y no repudio. El modo de funcionamiento es similar a lo explicado para los algoritmos de encriptación , se utilizan también algoritmos de clave pública, aplicados en dos etapas.

Ventajas ofrecidas por la firma Digital

- ✓ Integridad de la información: la integridad del documento es una protección contra la modificación de los datos en forma intencional o accidental. El emisor protege el documento, incorporándole a ese un valor control de integridad, el receptor deberá efectuar el mismo cálculo sobre el documento recibido y comparar el valor calculado con el enviado por el emisor.
- ✓ Autenticidad del origen del mensaje: este aspecto de seguridad protege al receptor del documento, garantizándole que dicho mensaje ha sido generado por la parte identificada en el documento como emisor del mismo, no pudiendo alguna otra entidad suplantar a un usuario del sistema.
- ✓ No repudio del origen: el no repudio del origen protege al receptor del documento de la negación del emisor de haberlo enviado. Este aspecto de seguridad es más fuerte que los anteriores ya que el emisor no puede negar bajo ninguna circunstancia que ha generado dicho mensaje , transformándose en un medio de prueba inequívoco respecto de la responsabilidad del usuario del sistema.

4.6.Encriptar datos en un PDA.

La importancia de tener nuestros datos a salvo de miradas extrañas o tener un mínimo de privacidad se ha convertido en un tema muy importante. Los PDAs son muchas veces usados como pequeñas oficinas portátiles donde se guardan datos de gran valor y donde es de gran importancia tener estos datos protegidos. Muchos usuarios PDA por comodidad no protegen el acceso de inicio con una clave, imagínense en caso de pérdida del aparato o descuido poder dejar estos datos confidenciales en manos ajenas a las nuestras. Para solucionar este problema o tener cierto grado de seguridad, es muy importante poder encriptar nuestros datos.

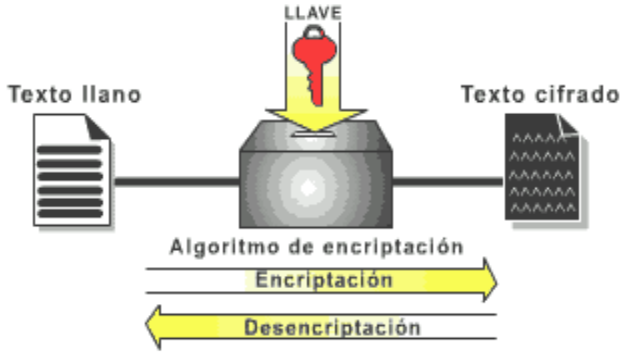
4.7 Encriptación de Ficheros:

Windows nos da una alternativa para poder proteger estos datos y prevenir su pérdida. El Encripting File System (EFS) en el encargado de codificar los ficheros. Estod Ficheros

solo se pueden leer cuando el usuario que los ha creado hace “logon” en su maquina (con lo cual, presumiblemente, nuestra password será una pasword robusta). De hecho, cualquiera que acceda a nuestra máquina, no tendrá nunca acceso a nuestros ficheros encriptados aunque sea un administrador del equipo.

4.8 Tipos de Cifrados

Cifrado en otros nombre que se le da al proceso de encriptación. El propósito de un cifrado es tomar datos sin encriptar, llamado texto claro, y producir una versión encriptada de los mismo. Existen dos clases de cifrad: Cifrado de Flujo de datos y Cifrado de bloques.



Cifrado de flujo de datos: En el cifrado por flujo de datos encriptan un bit de texto en claro por vez. El ejemplo más simple de cifrado por flujo de datos es el que consiste en combinar los datos, un bit a la vez, con otro bloque de datos llamado pad. Los cifrados por flujo de datos funcionan realmente bien con datos en tiempo real como voz y video.

Cifrado por bloques: operan sobre bloques de tamaño mayor que un bit del texto en claro y producen un bloque de texto cifrado, generalmente los bloques de salida son del mismo tamaño que los de la entrada. El tamaño del bloque debe ser lo suficientemente grande.

4.9 Autenticación

Este proceso, es otro método para mantener una comunicación seguro entre ordenadores. La autenticación es usada para verificar que la información viene de una fuente de confianza. Básicamente, si la información es autentica, sabes quién la ha creado y que no ha sido alterada. La encriptación y la autenticación, trabajan mano a mano para desarrollar un entorno seguro.

Hay varias maneras para autenticar a una persona o información en un ordenador:

Contraseñas – El uso de un nombre de usuario y una contraseña provee el modo más común de autenticación. Esta información se introduce al arrancar el ordenador o acceder a una aplicación. Se hace una comprobación contra un fichero seguro para confirmar que coinciden, y si es así, se permite el acceso.

Tarjetas de acceso – Estas tarjetas pueden ser sencillas como si de una tarjeta de crédito se tratara, poseyendo una banda magnética con la información de

autenticación. Las hay más sofisticadas en las que se incluye un chip digital con esta información.

Firma digital – Básicamente, es una manera de asegurar que un elemento electrónico (email, archivo de texto, etc.) es autentico. Una de las formas más conocidas es DSS (*Digital Signature Standard*) la cual está basada en un tipo de encriptación de clave pública la cual usa DSA (*Digital Signature Algorithm*). El algoritmo DSA consiste en una clave privada, solo conocida por el que envía el documento (el firmante), y una clave pública. Si algo es cambiado en el documento después de haber puesto la firma digital, cambia el valor contra lo que la firma digital hace la comparación, invalidando la firma.

Recientemente, otros métodos de autenticación se están haciendo populares en varios medios que deben mantenerse seguros, como son el escaneo por huellas, de retina, autenticación facial o identificación de voz.

Antivirus

Los ***antivirus*** son herramientas simples; cuyo objetivo es detectar y eliminar virus informáticos. Nacieron durante la década de 1980.

• Un virus informático ocupa una cantidad mínima de espacio en disco (el tamaño es vital para poder pasar desapercibido), se ejecuta sin conocimiento del usuario y se dedica a auto-replicarse, es decir, hace copias de sí mismo e infecta archivos, tablas de partición o sectores de arranque de los discos duros y disquetes para poder expandirse lo más rápidamente posible.

• Básicamente, el propósito de un virus es provocar daño en el equipo infectado.

• Normalmente un antivirus tiene un componente que se carga en memoria y permanece en ella para verificar todos los archivos abiertos, creados, modificados y ejecutados, en tiempo real. Es muy común que tengan componentes que revisen los adjuntos de los correos electrónicos salientes y entrantes, así como los scripts y programas que pueden ejecutarse en un navegador web (ActiveX, Java, JavaScript).

Básicamente, un antivirus compara el código de cada archivo con una base de datos de los códigos de los virus conocidos, por lo que es importante actualizarla periódicamente a fin de evitar que un virus nuevo no sea detectado. También se les ha agregado funciones avanzadas, como la búsqueda de comportamientos típicos de virus (técnica conocida como heurística) o la verificación contra virus en redes de computadoras. Actualmente

existe una nueva tecnología basada en Inteligencia artificial llamada TruPrevent que cuenta con la capacidad de detección de virus desconocidos e intrusos.

• Los antivirus son esenciales en sistemas operativos cuya seguridad es baja, como Microsoft Windows, pero existen situaciones en las que es necesario instalarlos en sistemas más seguros, como Unix y similares.

Con tantos software malignos dando vuelta por internet, se hace necesario disponer de un buen antivirus que nos proteja continuamente.

A continuación presentamos las características básicas de los mejores antivirus del mercado.

¿Qué se debe tener en cuenta para calificar un antivirus?

Un antivirus debe ser evaluado por distintas características como son, capacidad de detección de software maligno conocidos y desconocidos, actualización constante y efectiva, velocidad de escaneo y monitorización, dar grandes posibilidades a los expertos y sencillez a los inexpertos, efectiva documentación de ayuda.

Simbología de las principales características de cada uno:

E - Rápido en escaneo/monitor

A - Buena capacidad de actualización

D - Buena capacidad de detectar virus

R - Buena capacidad para remover

S - Mínimo consumo de recursos al sistema

H - Muchas herramientas y facilidades disponibles

G - Versión gratuita personal (no para uso comercial)

Los mejores antivirus de la actualidad

Antivirus	Protección	Carga del sistema	Utilidad
AhnLab V3 Internet Security 9,0	6	4.5	5.5
Avast Free AntiVirus 17,2 & 17,3	6	4.5	5.5
AVG Internet Security 17,2 & 17,3	6	5	5.5
Avira Antivirus Pro 15,0	6	6	6
Bitdefender Internet Security 21,0	6	6	5.5
BullGuard Internet Security 17,0	4.5	6	5.5
Comodo Internet Security Premium 10,0	5.5	4.5	5
ESET Internet Security 10,0	5.5	4	6
F-Secure Safe 14	6	5.5	5
G Data InternetSecurity 25,3	6	5	5.5
K7 Computing Total Security 15,1	5.5	4	5.5
Kaspersky Lab Internet Security 17,0	6	6	6
McAfee Internet Security 19,0	4.5	5.5	6
Microsoft Windows Defender 4,10	4.5	4.5	6
MicroWorld eScan Internet Security Suite 14,0	4.5	6	5.5
Norton Norton Security 22,9	6	6	5.5
ThreatTrack VIPRE Internet Security Pro 9,3	5.5	4.5	5.5
Trend Micro Internet Security 11,0 & 11,1	6	6	5.5

Las medidas de seguridad (niveles Básico y Medio) contemplan las siguientes acciones a adoptar:

- 1. Descripción de las rutinas de control de datos de los programas que se utilicen para ingresarlos en las bases, inclusión de acciones a tomar en caso de errores detectados, rutinas de control a fin de evitar incorporar a la base datos ilógicos, incorrectos o faltantes;
- 2. Copias de respaldo de la información contenida en las bases;
- 3. Designación de un responsable de adopción y control de cumplimiento de medidas;
- 4. Identificación del personal que accede a las bases;
- 5. Procedimiento de autenticación de usuario y control de acceso, tanto para la visualización como para el tratamiento de los datos;
- 6. Adoptar medidas de prevención a efectos de impedir amenazas por la intromisión de software malicioso que pudiere afectar archivos con datos personales;
- 7. Adoptar procedimientos que garanticen una adecuada gestión de los soportes que contengan datos personales;
- 8. Realización de auditorías que tengan como objeto el control del cumplimiento de las medidas y de los principios de finalidad, integridad, etc., de los datos personales contenidos en las bases.

En conclusión estas medidas se basan en: **protección, control y aseguramiento** de la integridad de la información.

CONCLUSION

Adoptar medidas de seguridad no sólo es válido para cumplir con las formalidades de la ley, sino que pueden constituirse en un primer mecanismo para la protección de la demás información confidencial de las empresas.

Entendemos que un primer paso podría darse extendiendo las medidas a todos los archivos, soportes o registros que contengan información valiosa para la empresa. Es importante resaltar que el enunciado de esta premisa es sólo un primer paso para comenzar a establecer mecanismos de protección y cuidado que deben ir fortaleciéndose con acciones concretas y adaptadas a la necesidad de cada negocio.