Capítulo 5

POLÍTICAS DE SEGURIDAD INFORMÁTICA

En este capítulo se describen las políticas de seguridad para optimizar el control del ISP

POLÍTICAS DE SEGURIDAD INFORMÁTICA

La Seguridad informática dentro de cualquier empresa es uno de los de las tareas mas importantes que deben realizarse en la implementación de sistemas computacionales. La seguridad no es un producto, al contrario es un proceso constante, siempre esta cambiando, reaccionando a los nuevas maneras de interceptar, alterar o introducir datos. Esta constante actualización es con el objetivo de prevenir daños irreparables a los datos o los equipos de las empresas.

La implementación adecuada de seguridades nos permitirá proteger tanto la información importante de nuestros sistemas, como nuestros equipos y aplicaciones. Para que estas seguridades sean correctamente aplicadas se deberían crear políticas de seguridad que deberán ser seguidas por aplicaciones, servidores y usuarios, así como definir una arquitectura de red para evitar las posibles intrusiones.

Adicionalmente y aunque no forma parte de este documento se deberán crear planes de contingencia.

5.1. Políticas de Seguridad

Estas políticas se definirán a dos niveles:

Arquitectura:

Instalación de equipos como firewall, IDS. Cuya principal función es separar redes internos de las redes externas.

Sistema Operativo:

Actualización del sistema operativo (parches y actualizaciones de seguridad). Se deben cerrar los puertos y servicios que no sean los necesarios, para así no permitir ingresos no deseados por canales de comunicación que no controlemos o monitoreemos.

5.1.1. Definición de Políticas de Seguridad Informática

Una política de seguridad informática es una forma de comunicarse con los usuarios. La cual les informa que deseamos proteger y él por qué de ello.

La política de seguridad debe ayudar a que los miembros de las empresas reconozcan a la información y los equipos computacionales como uno de sus principales activos. Y de esta manera concientizarlos por el uso y limitaciones de los recursos y servicios informáticos.

5.1.2. Elementos de una Política de Seguridad Informática

Las Políticas de Seguridad Informática deben considerar lo siguiente:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definición de violaciones y sanciones por no cumplir con las políticas.
- Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

Las políticas de seguridad informática, también deben ofrecer explicaciones sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. Especificar la autoridad responsable de aplicar los correctivos o sanciones.

Deben ser redactadas en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, claro está sin sacrificar su precisión.

Deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales, tales como: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, cambios en la empresa o negocio.

5.1.3. Razones que Impiden la Aplicación de las Políticas de Seguridad Informática

El principal obstáculo que se presenta es el de convencer a la administración de la empresa la necesidad y beneficios de la implementación de estas políticas. No realizan una comparación costo/beneficio, ya que no están concientes de la importancia de la información y cuanto dinero y tiempo cuesta no tenerla.

5.2. Privacidad en la Red

5.2.1. Características para considerar una red segura

Para considerar una red como segura deben cumplirse las siguientes características:

Disponibilidad: Los datos siempre deben estar accesibles. Sin importar si ha ocurrido algún problema interno o externo como por Ej. Corte de energía eléctrica, fallas de hardware, etc.

Autenticación: El usuario es quien dice ser. Estos se encuentran en muchos servicios y aplicaciones.

Integridad: Los datos que han sido enviados, recibidos o almacenados son completos y no han sido modificados.

Confidencialidad: Los datos enviados o almacenados no hayan sido interceptados o leídos por parte de personas no autorizadas.

5.2.2. Riesgos o Amenazas a la Privacidad de las Redes

Las principales amenazas o riesgos que enfrentan las empresas que utilizan las redes son:

Interceptación de las Comunicaciones: la comunicación puede ser interceptada y los datos copiados o modificados. La interceptación puede realizarse mediante el acceso físico a las líneas de las redes.

Acceso no Autorizado a Ordenadores y Redes de Ordenadores: el acceso no autorizado a ordenadores o redes de ordenadores se realiza habitualmente de forma mal intencionada para copiar, modificar o destruir datos. Técnicamente, se conoce como intrusión y adopta varias modalidades: explotación de información interna, ataques aprovechando la tendencia de la gente a utilizar contraseñas previsibles, aprovechar la tendencia de la gente a desvelar información a personas en apariencias fiables e interceptación de contraseñas.

Ejecución de Programas no autorizados: Generalmente estos programas borrar o destruyen datos. Son los clásicos ejemplos de virus. Otros tipos de programas rastrean lo que hacen los usuarios (troyanos)**.**

Saturación de los equipos: consiste en el envió de requerimientos a un equipo hasta agotarle sus recursos, o el enviar muchos mensajes a través de una red, de tal manera que existan gran cantidad de colisiones y la red se vuelva lenta e inestable.

Accidentes no Provocados: numerosos problemas de seguridad se deben a accidentes imprevistos o no provocados como: son tormentas, inundaciones, incendios, terremotos, interrupción del servicio por obras de construcción, defectos de programas y errores humanos o deficiencias de la gestión del operador, el proveedor de servicio o el usuario.

5.3. Políticas Generales

Como objetivo adicional del proyecto se decidió la creación de una política de seguridad en la que enmarcar el sistema.

Implementación

Los procesos de logging de las aplicaciones y los sistemas operativos deben estar activados en todos los hosts y servidores.

Las funciones de alarma y alerta de los firewalls y otros dispositivos de control de acceso al perímetro deben estar activados.

Todos los servicios críticos deben tener además herramientas redundantes de detección de intrusos instaladas, la cuales operen con principios diferentes a los de las herramientas primarias ya instaladas.

Administración

Se deben revisar diariamente los logs en los sistemas de control de acceso al perímetro (firewall, IDS).

Se deben revisar semanalmente los logs de los hosts y servidores que se encuentran en la red interna.

Se debe entrenar a los usuarios para que avisen de cualquier anomalía en el rendimiento del sistema a los administradores.

Todos los problemas que reciban los administradores serán revisados en busca de síntomas que indiquen actividad intrusa.

Los síntomas sospechosos deberán ser comunicados al personal de seguridad.

Cuando se produzca una intrusión, a menos que los sistemas críticos hayan sido comprometidos, la organización intentará primero recavar pruebas sobre los intrusos antes de reparar los sistemas, buscando más información de quién y cómo se produjo la intrusión. Esta persona debe ser entrenada en las vías legales para reportar una intrusión.

Se permitirá que determinados agujeros de seguridad queden sin corregir controladamente para el estudio de los atacantes y sus técnicas ('honeypots').

5.4. Antivirus

La protección contra virus debe realizarse en dos frentes:

- Correo electrónico de los clientes del ISP
- Usuarios internos de un ISP (Personal administrativo)

5.4.1. Correo electrónico de clientes

Uno de los servicios mas usados por los clientes de un ISP es el correo electrónico. El intercambio de archivo de correo es elevado y constante, siendo este es uno de los principales medios para infectar el equipo del cliente.

Una de medidas de seguridad que se debe implementar en un ISP es la revisión de todos los correos que ingresen para sus clientes para comprobar que estén libres de virus.

Para la revisión de los virus en los archivo de correo se debe de instalar un software antivirus y mantenerlo constante actualizado.

Alcance

Se debe revisar todos los correos que ingresen a los clientes del ISP en busca de virus. Esta revisión la realizara de manera automática el software antivirus.

Objetivos

Filtrar los correos que contengan virus y que puedan infectar los equipos de los clientes. Este puede ser considerado un servicio más del ISP.

Elementos

El principal elemento es el software antivirus que debe estar constantemente actualizado.

Responsabilidades

El administrador de sistemas es la persona encargada de la actualización del software antivirus cada 15 días para que este pueda detectar hasta las últimas modificaciones de los virus.

5.4.2. Usuarios Internos

Alcance

Proteger a cada uno de los equipos de la red interna del ataque de virus informáticos.

Objetivos

Prevenir de infecciones de virus informáticos en la red interna.

Elementos/Recursos

El principal elemento es el software antivirus que debe estar constantemente actualizado y el personal que labora en la empresa.

Responsabilidades

El administrador de sistemas es la persona encargada de la actualización del software antivirus cada 15 días para que este pueda detectar las más recientes modificaciones de los virus.

Chequear los CD-ROM's ingresados en nuestra PC sólo una vez, esto no aplica si son regrabables.

Formatear todo disquete nuevo, sin importar si son formateados de fábrica, ya que pueden infectarse aún desde el proceso del fabricante.

Revisar todo disquete que provenga del exterior, es decir que no haya estado bajo nuestro control. Aún cuando nos indiquen que está revisado. Nunca sabemos si esa persona sabe operar correctamente su antivirus.

Al bajar páginas de Internet, archivos ejecutables, etc. Estos siempre deben ser revisados antes de ejecutarlos. Y la descarga debería ser realizada a un directorio específico, para luego de revisarlos pasarlos a las carpetas de trabajo.

Revisar todos los e-mailes antes de abrirlos. Si llegan con un remitente desconocido, o archivos adjuntos que no conocemos de que se trata, eliminarlos inmediatamente.

Antes de actualizar el antivirus, verificar nuestra PC completamente.

5.4.3. Medidas de Protección Efectivas

La mejor medida de protección es adquirir un antivirus y mantenerlo siempre actualizado. Adicionalmente mantenerse informado sobre las nuevas técnicas de ataques y como evitarlas. Actualmente existes muchos sitios de información sobre nuevos ataques y herramientas que nos protegen en línea.

5.4.4. Referencia para Software de Antivirus

Tener varios programas antivirus, preferentemente con diferentes enfoques.

- Utilizar o activar las diversas opciones de protección. Estas podrían ser : equipos personales, para servidores de Correo
- Comprar las versiones actualizadas de las vacunas.
- Leer la documentación y manuales de los antivirus.

5.5. Correo Electrónico

El correo electrónico se ha convertido en una herramienta fundamental dentro de las empresas, y uno de los principales servicios que ofrece un ISP por lo que se hace indispensable que se cuente con medidas de seguridad adecuadas.

A continuación detallamos las políticas que deben ser aplicadas a un servidor de correo electrónico en un ISP

Alcance:

Asegurar que los correos electrónicos que ingresan y salen como servicio de un ISP. Para obtener esto se deben definir medidas antivirus que fueron mencionadas en el punto anterior pero que aquí detallamos.

Elementos/Recursos:

El personal que administra el centro de computo son los encargados de definir los parámetros que sirven para filtrar los correos, y las direcciones IP validas como remitentes o destinatarios de los correos.

Responsabilidades:

El administrador de sistemas es la persona encargada de definir:

- Que considera correos SPAM, definir que entradas son consideradas de este tipo.
- Las direcciones IP validas que pueden accesar a nuestra red, estas pueden ser remitentes como destinatarios
- Los tipos de archivos adjuntos deben ser bloqueados por Ej. EXE, COM

5.6. Seguridad de Sistema de Detección de Intrusos - IDS

La definición de las políticas para este tema están separadas en los puntos los cuales son Implementación y Administración, esto ayudará a que se definan correctamente las funciones del personal.

Las políticas aplicadas a IDS deben contener como mínimo los siguientes puntos:

Implementación

- Los procesos de logging de las aplicaciones y los sistemas operativos deben estar activados en todos los hosts y servidores.
- Las funciones de alarma y alerta de los firewalls y otros dispositivos de control de acceso al perímetro deben estar activados.

- Procesos de auditorias periódicas para la revisión de los procesos, control y revisión de los IDS.

Administración

- Se debe instalar el IDS para el chequeo de la integridad de los sistemas de ficheros en los firewalls y otros sistemas de control de acceso al perímetro.

- Se deben revisar diariamente los logs en los sistemas de control de acceso al perímetro y periódicamente los logs de los hosts y servidores que se encuentran en la red interna.

- Todos los problemas que reciban los administradores serán revisados en busca de síntomas que indiquen actividad intrusa.

Estas políticas son las mínimas que debe tener una empresa como seguridad básica. Estos procedimientos son usados normalmente en empresas que tienen Riesgos Bajos.

5.6.1. Políticas para Riesgos Medios

Implementación

- Todos los servicios críticos deben ser monitorizados por herramientas adicionales como Tripwire o *tcpwrappers* instaladas apropiadamente, como suplemento de la actividad de logging que incorpora el sistema operativo.

Administración

- Las herramientas HIDS como Tripwire deben ser revisadas periódicamente.

- Si se produce una intrusión, lo primero que debe revisar los sistemas que fueron afectados buscando información de quien y como se produjo la intrusión, para luego por vías legales reportar la intrusión.

- Se permitirá que determinados agujeros de seguridad queden sin corregir controladamente para el estudio de los atacantes y sus técnicas (’honeypots’).

5.6.2. Políticas para Riesgos Altos

Implementación

- Los servicios críticos deben ser monitorizados por herramientas adicionales como Tripwire o *tcpwrappers* instaladas apropiadamente, como suplemento de la actividad de logging que incorpora el sistema operativo.

- Los servicios críticos deben tener además herramientas redundantes de detección de intrusos instaladas, la cuales operen con principios diferentes a los de las herramientas primarias ya instaladas.

- En los puntos de concentración de la red se instalaran NIDSs que monitoricen el tráfico en busca de patrones conocidos de ataques.

Administración

- Siempre deben estar ejecutándose, sin necesidad que ninguna supervisión exclusiva.

- La organización intentará perseguir a los intrusos pero no permitirá que no se corrijan agujeros de seguridad para el estudio de los atacantes.

En las políticas para Riesgos Medios están incluidas las políticas básicas, en las Políticas de Riesgos Altos deben estar incluidas las políticas básicas más las de Riesgos Medios y las propias para los de Riesgo Alto.

5.7. Seguridad para el Servidor de Servicio de Nombres de Dominio - DNS

El servicio DNS es una parte esencial del funcionamiento de una red ya sea de tipo Internet o red administrativa empresarial como una Lan; existen por tanto dos estrategias básicas para el aseguramiento de un servicio de este tipo: evitar la interrupción del servicio y evitar el compromiso de los datos.

5.7.1. Métodos para Asegurar el Servidor

Las políticas que deben aplicarse para darle seguridad al servidor de DNS son:

5.7.1.1 Servicio de DNS redundante

Este servicio consiste en asignar más de un servidor de DNS dentro de la empresa, esto puede hacer uso de una gran cantidad de recursos al inicio pero después esto se será en una política de solución más efectiva, ya que cuando el servidor principal tenga problemas el segundo debe subir o ponerse al aire automáticamente.

Adicionalmente se debe respaldar la información para mantener información actualizada y segura.

5.7.1.2 Servidor en su Red Perimetral

De esta forma se partirán las redes en internas, solo de la empresa, y externas, fuera de la empresa, dejando de esta manera una zona la cual es conocida como **Zona Desmilitarizada (DMZ)**, de esta manera los requerimientos serán atendidos en sus respectivas lugares de solicitud.

5.7.1.3 Control de interfaces

Otra política que debe aplicarse para la seguridad del servidor de DNS es la de el Control de Interfases, la cual consiste en limitar las consultas a través del control de interface de la red, esto hará que solo haya resolución de DNS por una sola interface del servidor y para la parte interna de la red y la externa no dejar realizar la resolución de DNS.

5.7.1.4 Limitar tráfico por IP

Especificando las direcciones IP de los Servidores de DNS se podrán proteger las zonas de transferencias, aunque esto solo hará que el intruso tenga un mayor trabajo para poder ingresar.

5.7.1.5 Encriptación

Esta política consiste en habilitar la encriptación de los paquetes que se envían a través del Internet, ya sea utilizando protocolos de IPSec o usando una Red Publica Virtual (VPN) en su Sistema Operativo.

5.7.1.6 Proteger el Cache

Hay que proteger la corrupción del cache, ya que los intrusos hacen uso de esta información para beneficio personal, esta información deben ser restringida ya que almacenan datos importantes.

5.7.1.7 Autorizar las actualizaciones dinámicas de DHCP

Al activar esta política usada para la seguridad del Servidor de DNS, hay que dar las direcciones de la configuración a los clientes, y de esta manera tendremos un control de las actualizaciones en el servidor DCHP.

5.8. Seguridad para Firewall

Los firewalls conectan las redes externas con nuestra red interna, y es en este punto donde podemos monitorear y rechazar paquetes de datos.

Todos los datos entrantes o salientes que viajan por la red son inspeccionados por el firewall ya que pasan a través de él. El firewall examina cada trama de datos y bloquea los que no cumplen las reglas de seguridad.

Alcance

Revisión de todos los paquetes de datos que entren o salgan de nuestra red

Objetivo

Prevenir que paquetes de datos no autorizados o sospechosos

Responsabilidades

Que ningún equipo de la red interna este conectado a la red externa sin que haya un firewall de por medio

El administrador de sistema debe definir las reglas de seguridad que manejara el firewall:

- Bloqueo de puertos
- Direcciones IP validas en la red
- Recursos que se pueden accesar desde la red externa
- Definir que sitios no pueden ser visitados por los usuarios internos
- Definir que usuarios pueden ingresar a la red interna

Revisión periódica de los registros de log, para análisis de ataques sistemáticos. Debido a que muchos intrusos realizan pruebas de seguridad antes de realizar un ataque directo.

El complemento ideal para que el Firewall tenga mejor funcionamiento es la instalación de un Sistema de Detección de Intrusos (IDS).

5.9. Consideraciones finales de la seguridad

El propósito de usar o definir políticas de seguridad es para que la empresa este protegida para cualquier eventualidad. Las políticas de seguridad generalmente presentan tres aspectos:

Una política general que establece el enfoque a la seguridad

Las reglas específicas son el equivalente de una política específica, estas reglas definen lo que está y ó no esta permitido. Las reglas pueden ser apoyadas por procedimientos y otros métodos o guías.

El enfoque técnico ó análisis que soporta la política general y las reglas específicas.

Las políticas diseñadas o establecidas deben ser efectivas, y para esto los o el diseñador tiene que tener el compromiso y concesión de ejecutarlas.

Ejecución de las políticas

Las políticas deben sincronizarse con otros procesos para que de esta manera estas sean ejecutadas correctamente, para esto debe implicarse o incluir a la alta gerencia en la ejecución de la misma.

Las políticas de seguridad pueden estructurarse según su destino, para lo cual debemos tomar en cuenta lo siguiente:

- Para los usuarios.
- Para los administradores/gestores.
- Requisitos técnicos
- Bajo riego.

- Riesgo medio.
- Alto riesgo, etc.

5.10. Conclusión

Una solución de seguridad no es algo que se pueda definir como un producto que se instala o se aplica y está terminado, la seguridad es un proceso constante de estudio de nuevos métodos de ataque, servicios, parches y productos que están disponibles en Internet para atacar redes, sistemas, y aplicaciones. Es un proceso de auditorias constantes, de actualización de políticas y procedimientos preventivos ante posibles ataques.