Fundamentos de Seguridad

DESARROLLO Y GESTIÓN DE SEGURIDAD DE REDES

Introducción

Debido a que el uso de Internet se encuentra en aumento, cada vez más compañías permiten a sus socios y proveedores acceder a sus sistemas de información.

Por lo tanto, es fundamental saber qué recursos de la compañía necesitan protección para así controlar el acceso al sistema y los derechos de los usuarios del sistema de información. Los mismos procedimientos se aplican cuando se permite el acceso a la compañía a través de Internet.

Introducción

Además, debido a la tendencia creciente hacia un estilo de vida nómada de hoy en día, el cual permite a los empleados conectarse a los sistemas de información casi desde cualquier lugar, se pide a los empleados que lleven consigo parte del sistema de información fuera de la infraestructura segura de la compañía.

1.1 Introducción a la Seguridad Informática

Los riesgos, en términos de seguridad, se caracterizan por lo general mediante la siguiente ecuación.

$$\text{Riesgos} = \frac{\text{Amenaza x Vulnerabilidad}}{\text{Contramedida}}$$

1.1 Introducción a la Seguridad Informática

La amenaza representa el tipo de acción que tiende a ser dañina, mientras que la vulnerabilidad *(conocida a veces como falencias (flaws) o brechas (breaches))* representa el grado de exposición a las amenazas en un contexto particular.

Finalmente, la contramedida representa todas las acciones que se implementan para prevenir la amenaza

1.1 Introducción a la Seguridad Informática

Las contramedidas que deben implementarse no sólo son soluciones técnicas, sino también reflejan la capacitación y la toma de conciencia por parte del usuario, además de reglas claramente definidas.

1.1 Introducción a la Seguridad Informática

Para que un sistema sea seguro, deben identificarse las posibles amenazas y por lo tanto, conocer y prever el curso de acción del enemigo.

Por tanto, el objetivo de este informe es brindar una perspectiva general de las posibles motivaciones de los hackers, categorizarlas, y dar una idea de cómo funcionan para conocer la mejor forma de reducir el riesgo de intrusiones.

Objetivos de la Seguridad Informática

La seguridad informática se resume, por lo general, en cinco objetivos principales:

1. Integridad: garantizar que los datos sean los que se supone que son.
2. Confidencialidad: asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian
3. Disponibilidad: garantizar el correcto funcionamiento de los sistemas de información

Objetivos de la Seguridad Informática

4. Evitar el rechazo: garantizar de que no pueda negar una operación realizada.
5. Autenticación: asegurar que sólo los individuos autorizados tengan acceso a los recursos

1.2 Confidencialidad, integridad y disponibilidad de la información

Confidencialidad

La confidencialidad consiste en hacer que la información sea ininteligible para aquellos individuos que no estén involucrados en la operación.

Integridad

La verificación de la integridad de los datos consiste en determinar si se han alterado los datos durante la transmisión (accidental o intencionalmente).

1.2 Confidencialidad, integridad y disponibilidad de la información

Disponibilidad

El objetivo de la disponibilidad es garantizar el acceso a un servicio o a los recursos.

No repudio

Evitar el repudio de información constituye la garantía de que ninguna de las partes involucradas pueda negar en el futuro una operación realizada.

1.2 Confidencialidad, integridad y disponibilidad de la información

Autenticación

La autenticación consiste en la confirmación de la identidad de un usuario; es decir, la garantía para cada una de las partes de que su interlocutor es realmente quien dice ser.

Un control de acceso permite (por ejemplo gracias a una contraseña codificada) garantizar el acceso a recursos únicamente a las personas autorizadas.

Necesidad de un enfoque global

- Seguridad en las telecomunicaciones: tecnologías de red, servidores de compañías, redes de acceso, etc.
- Seguridad física, o la seguridad de infraestructuras materiales: asegurar las habitaciones, los lugares abiertos al público, las áreas comunes de la compañía, las estaciones de trabajo de los empleados, etc.

1.3 El Proceso de la Seguridad

Generalmente, la seguridad de los sistemas informáticos se concentra en garantizar el derecho a acceder a datos y recursos del sistema configurando los mecanismos de autentificación y control que aseguran que los usuarios de estos recursos sólo posean los derechos que se les han otorgado.

Cómo implementar una política de seguridad

Por esta razón, uno de los primeros pasos que debe dar una compañía es definir una política de seguridad que pueda implementar en función a las siguientes cuatro etapas:

- Identificar las necesidades de seguridad y los riesgos informáticos que enfrenta la compañía así como sus posibles consecuencias.

Cómo implementar una política de seguridad

- Proporcionar una perspectiva general de las reglas y los procedimientos que deben implementarse para afrontar los riesgos identificados en los diferentes departamentos de la organización.
- Controlar y detectar las vulnerabilidades del sistema de información, y mantenerse informado acerca de las falencias en las aplicaciones y en los materiales que se usan.
- Definir las acciones a realizar y las personas a contactar en caso de detectar una amenaza.

Cómo implementar una política de seguridad

La política de seguridad comprende todas las reglas de seguridad que sigue una organización (en el sentido general de la palabra).

Por lo tanto, la administración de la organización en cuestión debe encargarse de definirla, ya que afecta a todos los usuarios del sistema.

Cómo implementar una política de seguridad

En este sentido, no son sólo los administradores de informática los encargados de definir los derechos de acceso sino sus superiores.

El rol de un administrador de informática es el de asegurar que los recursos de informática y los derechos de acceso a estos recursos coincidan con la política de seguridad definida por la organización.

Cómo implementar una política de seguridad

La seguridad informática de una compañía depende de que los empleados (usuarios) aprendan las reglas a través de sesiones de capacitación y de concientización.

Cómo implementar una política de seguridad

Sin embargo, la seguridad debe ir más allá del conocimiento de los empleados y cubrir las siguientes áreas:

- Un mecanismo de seguridad física y lógica que se adapte a las necesidades de la compañía y al uso de los empleados
- Un procedimiento para administrar las actualizaciones
- Una estrategia de realización de copias de seguridad (backup) planificada adecuadamente
- Un plan de recuperación luego de un incidente
- Un sistema documentado actualizado

Las causas de inseguridad

Un estado de inseguridad activo; es decir, la falta de conocimiento del usuario acerca de las funciones del sistema, algunas de las cuales pueden ser dañinas para el sistema (por ejemplo, no desactivar los servicios de red que el usuario no necesita)

Un estado de inseguridad pasivo; es decir, la falta de conocimiento de las medidas de seguridad disponibles (por ejemplo, cuando el administrador o usuario de un sistema no conocen los dispositivos de seguridad con los que cuentan)

1.4 La Naturaleza de un ataque

Tarea....

Bibliografía

http://es.ccm.net/contents/622-introduccion-a-la-seguridad-informatica