SEP SEV DGEST DITD

INSTITUTO TECNOLÓGICO SUPERIOR DE TANTOYUCA

RIESGOS Y AMENAZAS EN UNA RED DE DATOS

MATERIA: ADMINISTRACION DE REDES DE DATOS

DOCENTE: ING. EDGAR GUILLERMO MEDELLIN ORTA

PRESENTA:

HERNANDEZ REYES GUADALUPE

INGENIERIA: SISTEMAS COMPUTACIONALES

SEMESTRE: SC-8A

TANTOYUCA VER. A 24/05/2020

Tabla de contenido

Amenazas y Riesgos en una Red de Datos.

Amenazas y Riesgos en una Red de Datos.

1. Aspectos Generales.

Desde los comienzos de la computación, los sistemas han estado expuestos a una serie de peligros o riesgos que van aumentando conforme se globalizan más las comunicaciones entre estos sistemas.

Casi todas las organizaciones públicas o privadas, al igual que las personas, dependen de alguna manera de la tecnología de la información como una herramienta esencial para lograr sus objetivos de negocio o para poder desarrollar actividades en su vida cotidiana; al mismo tiempo, todos tienen que enfrentarse con una amplia gama de amenazas y vulnerabilidades asociadas a los entornos informáticos de hoy.

Los riesgos de la información están presentes cuando confluyen dos elementos: amenazas y vulnerabilidades. Las amenazas y vulnerabilidades están íntimamente ligadas, y no puede haber ninguna consecuencia sin la presencia conjunta de éstas. Las amenazas deben tomar ventaja de las vulnerabilidades y pueden venir de cualquier parte, interna o externa, relacionada con el entorno de las organizaciones.

2. Objetivos Básicos.

Para soportar estos objetivos se definen las políticas de seguridad que regirán en nuestro dominio de seguridad. Estas políticas deben ser definidas en varias categorías: acceso físico, seguridad en la comunicación, computadoras, sistemas operativos, bases de datos, aplicaciones, personal, ambiente natural, respaldos, planes de contingencias, etc.

2.1. Confidencialidad.

Asegurar que la información no esté expuesta o revelada a personas no autorizadas.

2.2. Integridad.

Asegurar consistencia de los datos, en particular prevenir la creación, alteración o borrado de datos de entidades no autorizadas.

2.3. Disponibilidad.

Asegurar que los usuarios legítimos no obtengan acceso denegado a su información y recursos.

2.4. Uso legítimo.

Asegurar que los recursos no sean usados por personas no autorizadas o en formas no autorizadas.

3. Conceptos Básicos.

3.1.1. Amenaza.

Una amenaza es una persona, entidad, evento o idea que plantea algún daño a un activo.

3.1.2. Ataque.

Un ataque es una realización de una amenaza.

3.1.3. Protección.

Una protección son los controles físicos, mecanismos, políticas y procedimientos que protegen los activos o recursos de las amenazas.

3.1.4. Vulnerabilidad.

Una vulnerabilidad es el debilitamiento o ausencia de una protección en un recurso o activo.

3.1.5. Riesgo.

Un riesgo es una medida del costo de una realización de una vulnerabilidad que incorpora la probabilidad de éxito de un ataque. El riesgo es alto si el valor del activo vulnerable es alto y la probabilidad de éxito de un ataque es alto.

4. Tipos de Riesgos y Amenazas.

4.1. Incremento del Riesgo.

El vandalismo computacional se manifiesta en muchas formas. Las diferentes categorías de este vandalismo se basan en cómo estas se extienden y se activan. Los programas Caballos de Troya, por ejemplo, son programas disfrazados como algo inofensivo pero activados por la propia víctima.

4.1.1. Virus.

Son programas que se autoreplican y afectan principalmente los archivos ejecutables, a veces llegan a afectar a miles de computadoras. Esta es una form molesta de ataque en el sistema por que se comporta como un parásito. Cuando el programa infectado es ejecutado, también se ejecuta el código viral.

Los virus no pueden ejecutarse como un programa independiente; ellos necesitan un programa anfitrión (host program) que los inicialice. Una vez que el virus se ha establecido y atacado a otros programas en el sistema, es difícil eliminarlo.

4.1.2. Bacterias.

Los programa bacteria crean copias de sí mismos en forma geométrica, siendo su modo primario de dañar por medio de consumir recursos computacionales hasta que el sistema llega a una paralización.

La bacteria no altera los datos ni destruye archivos. Su propósito es degradar el servicio del sistema, pues dependiendo de cómo es programada, puede empezar a ocupar todo el espacio en disco o los ciclos de CPU muy rápidamente, llevando al sistema a detenerse. Un programa que es de un solo byte de longitud podría consumir 4GB.

4.1.3. Gusanos.

Son programas únicos que migran de computadora a computadora sobre la red, mientras van dañando al sistema o divulgando información crítica del sistema a sus creadores, con el fin de preparar el camino a ataques más directos.

Un worm no altera o daña otros programas, pero podría ser un vehículo para otros programas como los virus.

4.1.4. Puertas Traseras.

Las puertas traseras son aspectos no documentados construidos dentro de programas y que pueden proveer a usuarios con conocimientos, un acceso no autorizado a los recursos computacionales.

Los back doors permiten al usuario entrar a los programas rápidamente para propósitos de evaluación, depuración, mantenimiento y monitoreo en el proceso de desarrollo de sistemas. Muchas veces los back doors son olvidados y dejados en el código cuando este es liberado.

Uno de los aspectos más significativos de esta amenaza es que se encuentran disponibles para muchos usuarios.

La mejor defensa contra un ataque a través de una puerta trasera es obteniendo el conocimiento de ésta, antes de que llegue a ser ampliamente difundida. Por lo cual, una de las mejores protecciones es la comunicación entre administradores de sistemas.

4.1.5. Bombas Lógicas.

Son programas diseñados para dañar un sistema y se activan por cambios futuros en la configuración del mismo.

Las bombas lógicas ejecutan una función, o un conjunto de funciones, que no fueron características intencionales del programa original, siendo las más comunes la destrucción de aplicaciones o datos. Son frecuentemente colocadas por los programadores encargados de mantenimiento de sistemas.

La mejor protección contra los desastres de las bombas lógicas es tener bien definidos procesos de administración y mantenimiento de cuentas de usuario. Tales

procedimientos serán enfocados para detectar bombas lógicas antes de que éstas tengan la oportunidad de hacer daños.

4.1.6. Trampas.

Las trampas son también aspectos no documentados construidos dentro de los programas, activados por los usuarios involuntarios, que trastornan la computadora. Colectivamente estas amenazas son conocidas como amenazas programadas.

4.1.7. Caballos de Troya.

Son probablemente las amenazas programadas más comunes y fáciles de implantar, son programas que imitan a un programa que el usuario quiere ejecutar, pero son realmente diferentes.

Un caballo de Troya engaña al usuario en la ejecución de un programa dañando al sistema por tomar ventaja de los permisos de acceso del usuario.

4.1.8. Huecos de Seguridad.

Los huecos de seguridad son imperfecciones en el diseño de software, que mal usados, otorgan privilegios a usuarios comunes.

Los huecos de seguridad se manifiestan en cuatro formas:

- Huecos de Seguridad Físicos.

Donde el problema potencial es causado por permitir acceso físico al equipo a personas no autorizadas, donde estas pueden realizar operaciones que no deberían ser capaces de hacer.

- Huecos de Seguridad de Software.

Donde el problema es causado por elementos mal escritos de software privilegiado los cuales pueden ser utilizados para realizar cosas que no deberían poder hacer.

- Huecos de Seguridad por Uso Incompatible.

Donde, por falta de experiencia o por errores propios, el Administrador del Sistema ensambla una combinación de hardware y software el cual cuando se usa como un sistema está seriamente dañado, desde el punto de vista de la seguridad.

- Selección de una filosofía de Seguridad y su Mantenimiento.

El software perfecto, el hardware protegido y los componentes compatibles no trabajarán adecuadamente a menos que se selecciones una política de seguridad apropiada y las partes del sistema se direcciones para reforzarla.

4.2. Amenazas de Seguridad.

4.2.1. Phishing.

Es la capacidad de duplicar una página Web para hacer creer al visitante que se encuentra en la página original en lugar de la copiada.

Se tienen dos variantes de esta amenaza:

Vishing.

Utilización de técnicas de phishing pero para servicios asociados con voz sobre IP (VoIP).

Smishing.

Utilización de técnicas de phishing en los mensajes de texto de teléfonos móviles.

4.2.2. Spam.

Envío de cualquier correo electrónico, masivo o no, a personas a través de este medio que incluyen temas tales como pornografía, bromas, publicidad, venta de productos, entre otros, los cuales no han sido solicitados por el(los) destinatario(s).

4.2.3. Ingeniería social.

Es la manipulación de las personas para convencerlas de que ejecuten acciones, actos o divulguen información que normalmente no realizan, entregando al atacante la información necesario para superar las barreras de seguridad.

4.2.4. Código Malicioso.

Hardware, software o firmware que es intencionalmente introducido en un sistema con un fin malicioso o no autorizado.

Ejemplo: Troyanos, Works, Spyware, Rootkits, Adware, Backdoor, Cookies, Dialers, Exploit, Hijacker, keyloggers, Pornware, etc.

4.2.5. Hoax.

Es un mensaje de correo electrónico con contenido falso o engañoso y normalmente distribuido en cadena, aparte de ser molesto, congestiona las redes y los servidores de correo, pueden ser intencionales para la obtención de direcciones de correo para posteriormente ser utilizadas como spam. Algunos de los Hoax más conocidos son correos con mensajes sobre virus incurables, temática religiosa, cadenas de solidaridad, cadenas de la suerte, Regalos de grandes compañías, entre otros.

4.3. Tipos de Riesgos.

Una vez que alguien está decidido a atacarnos, puede elegir alguna de estas formas.

4.3.1. Interrupción.

El ataque consigue provocar un corte en la prestación de un servicio: el servidor web no está disponible, el disco en red no aparece o solo podemos leer (no escribir), etc.

4.3.2. Intercepción.

El atacante ha logrado acceder a nuestras comunicaciones y ha copiado la información que estábamos transmitiendo.

4.3.3. Modificación.

Ha conseguido acceder, pero, en lugar de copiar la información, la está modificando para que llegue alterada hasta el destino y provoque alguna reacción anormal. Por ejemplo, cambia las cifras de una transacción bancaria.

4.3.4. Fabricación.

El atacante se hace pasar por el destino de la transmisión, por lo que puede tranquilamente conocer el objeto de nuestra comunicación, engañarnos para obtener información valiosa, etc.

4.4. Tipos de atacantes.

Se suele hablar de hacker de manera genérica para referirse a un individuo que se salta las protecciones de un sistema.

A partir de ahí podemos distinguir entre:

4.4.1. Hacker.

Ataca la defensa informática de un sistema solo por el reto que supone hacerlo. Si tiene éxito, moralmente debería avisar a los administradores sobre los agujeros de seguridad que ha utilizado, porque están disponibles para cualquiera.

4.4.2. Cracker.

También ataca la defensa, pero esta vez sí quiere hacer daño: robar datos, desactivar servicios, alterar información, etc.

4.4.3. Script kiddie.

Son aprendices de hacker y cracker que encuentran en Internet cualquier ataque y lo lanzan sin conocer muy bien qué están haciendo y, sobre todo, las consecuencias derivadas de su actuación (esto les hace especialmente peligrosos).

4.4.4. Programadores de malware.

Expertos en programación de sistemas operativos y aplicaciones capaces de aprovechar las vulnerabilidades de alguna versión concreta de un software conocido para generar un programa que les permita atacar.

4.4.5. Sniffers.

Expertos en protocolos de comunicaciones capaces de procesar una captura de tráfico de red para localizar la información interesante.

SNIFFER

4.4.6. Ciberterrorista.

Cracker con intereses políticos y económicos a gran escala.

Conclusión.

Después de realizar una investigación sobre las amenazas y riesgos en una red de datos, se puede concluir que es muy necesario conocerlos y tener los conocimientos para poder llevar una buena administración en la red, tomando en cuentas que las amenazas están al día y si no son atendidas a tiempo podrían provocar alguna afectación a la red, por ello conocerlas es de suma importancia para poder controlarlas antes de que el daño sea introducido a la red.

Bibliografías.

Amenazas a la Seguridad en Redes.

http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/argueta_a_a/capitulo1.pdf

Amenazas de Seguridad.

https://administracion-de-redes-tec-iguala.blogspot.com/2016/05/

Riesgos, Políticas y Herramientas de Seguridad en Redes.

Alonso Cañon. (1997). Riesgos, Políticas y Herramientas de Seguridad en Redes.. Universidad Eafit: s/e.