Universidad Corporativa Coppel | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad | #1 | Análisis de Vulnerabilidades y Amenazas

Seguridad Informática 1

Ingeniería en Desarrollo de Software

academia global

TUTOR: Jessica Hernández Romero

ALUMNO: Pilar Barajas Cervantes

FECHA: 04/09/2024

índice

Introducción 3
Descripción 4
Justificación 5
Tabla de análisis 6
Conclusión 8
Referencia 9

Introducción

El análisis de vulnerabilidades y amenazas es una metodología que permite identificar los puntos débiles de una empresa y protegerse de posibles riesgos, este es también llamado evaluación de vulnerabilidades, es un proceso que evalúa las redes o activos de Tl para encontrar debilidades o fallas de seguridad. Por otro lado, el análisis de amenazas ayuda a identificar los riesgos de seguridad que pueden afectar a un producto, aplicación red o entorno. Algunas cosas a tener en cuenta sobre los análisis de vulnerabilidades y amenazas son:

- **La vulnerabilidad se produce cuando los sistemas, equipos o redes tienen deficiencia o carencias que pueden permitir un ataque.**
- **La amenaza es un peligro que existe independientemente de si es vulnerable o no.**
- **La vulnerabilidad y la amenaza, por separado, son peligrosas pero juntas se convierten en un riesgo.**
- **El riesgo es la probabilidad de que una empresa se convierta en un desastre.**
- **La decisión de hacer pública una vulnerabilidad es polémica.**

Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura.

Descripción

Para una empresa lo más importante es tener protegida toda información de cada uno de sus clientes para evitar las amenazas y las vulnerabilidades, un antivirus siempre tiene que estar constante mente actualizado es muy esencial para la protección de un equipo. Contar con un firewall confiable y actualizado que ayude a identificar amenazas y conductas sospechosas también ayudara a estar protegido contra cualquier amenaza, tener una copia de seguridad y actualizada constantemente es una de las mejores medidas contra la perdida de información, habilitar las actualizaciones automáticas para el sistema operativo es otra practica sustancial para evitar ciberataques, desconfiar de ventanas exageradas, estas son practicas sencillas que puede realizar cualquier empresa.

El análisis de vulnerabilidades es un proceso que permite identificar los puntos débiles de una empresa y establecer medidas para protegerse de posibles riesgos. Consiste en evaluar los sistemas TI o redes para identificar debilidades, fallas, o vulnerabilidades de seguridad. Estas vulnerabilidades pueden ser aprovechadas por actores de amenazas internos o externos. Estas amenazas también pueden surgir por varias razones, como configuraciones incorrectas, versiones de software obsoletas, fallas de diseño. Las amenazas son peligros que existen independientemente de que se sea vulnerable o no. las amenazas informáticas pueden provenir de ataques externos o de amenazas internas, como el robo de información o el uso inadecuado de los sistemas.

Justificación

La evaluación de riesgos permite a las empresas adoptar medidas y tomar decisiones enfocadas en cumplir los objetivos establecidos. Ya que este es un proceso interno fundamental porque permite detectar los riesgos que se podrían materializar y de qué manera estos afectarían el normal desarrollo de las actividades. El objetivo de esta evaluación es conocer las características de la amenaza y su origen, teniendo en cuenta la probabilidad de ocurrencia, el nivel de impacto y escenarios en los que se pueda presentar. Existen cuatro pasos básicos que se deben seguir para realizar una evaluación de riesgos:

1. **Identificación de riesgos, como su nombre lo indica, en esta etapa se deben identificar los posibles riesgos, tanto internos como externos, a los que esta enfrentada la empresa.**
2. **Análisis de riesgos, después de identificar los riegos el siguiente paso en la evaluación es analizarlos. Este análisis puede realizarse teniendo en cuenta diferentes grados de detalle y complejidad, esto depende de que es lo que se quiere lograr con el análisis.**
3. **Valoración de riesgos, este paso es fundamental poque contribuye directamente a la toma de decisiones. Cuando hablamos de valoración nos referimos a la comparación que se hace con los resultados obtenidos en los análisis y criterios que se establecieron para cada riesgo.**
4. **Tratamiento de riesgo, elegir las mejores opciones para el tratamiento de los riesgos depende del balance que se haga entre los beneficios que se generan por el logro de objetivos frente a costos.**

Tabla de análisis

Amenazas humanas	Amenazas Lógicas	Amenazas Físicas	Vulnerabilidades de Almacenamiento	Vulnerabilidades de Comunicación
1._Servidor descargado de internet.	1._Desconocimiento de la fuente del software.	1._Equipos lentos.	1._Contraceñas básicas.	1._No se tiene denegado el uso de equipo de actividades
2._Docentes.	2._Contar con un servidor diferente.	2._Firewall inhabilitado.	2._Usuarios de registros básicos.	2._Desconocimiento del Software.
3._No contar con alarmas de seguridad.	3._Contar con un solo servidor a la base de datos central.	3._Antivirus gratuito para todo el equipo	3._Servidor principal diferente al centro de cómputo.	3._Equipos conectados de manera directa al modem
4._No contar con el acceso denegado al uso del equipo para las actividades.		4._No contar con dispositivos de detención de sismos.		4._Equipos portátiles que se conectan vía Wi_Fi.

- **Amenazas humanas: su finalidad es obtener información, pero sin modificarla, lo que implica que sean muy difíciles de detectar ya que no realizan ningún cambio de la información que consiguen.**
- **Amenazas lógicas: son aquellas que dañan los sistemas de software datos o red de una computadora, sin afectar el software.**
- **Amenazas físicas: algunos ejemplos son, los daños en los discos duros, un corto circuito, un incendio, un robo, una inundación, un terremoto o un escape de agua.**
- **Amenazas de almacenamiento: existen varias amenazas que pueden afectar el almacenamiento de datos o de materiales.**
- **1._amenazas a la seguridad de los datos.**
- **2._almacenamiento incorrecto**
- **3._ubicaciones inadecuadas, entre otras.**
- **Amenazas de comunicación: pueden surgir debido a configuraciones inadecuadas, fallas de actualizaciones, debilidades en contraseñas entre otros factores.**

Conclusión

Hoy en día, la ciberseguridad incluye productos centrados en evitar que las empresas, cada vez más sofisticadas, pongan en peligro la red, ingenieros que establecen y llevan a cabo la detección y procesos de respuesta para cuando se encuentran amenazas potenciales, sin embargo, la ciberseguridad debe comenzar mucho antes de encontrar las amenazas, para eso están los análisis de vulnerabilidades. Todas las empresas deben evaluar periódicamente sus defensas de seguridad en busca de grietas en su caparazón si quieren mantener una postura de seguridad sólida. Especialmente ahora, que hay una creciente ola de ciberdelincuencia en México, por ejemplo, los ataques de Ransomware, bombas lógicas, Malware, adware, caballos de troya, Spam entre muchos otros.

En materia de seguridad informática, los puntos débiles de los sistemas son comúnmente aprovechados por personas que buscan la manera de acceder a realizar alguna acción maliciosa. Desafortunadamente todos los sistemas tecnológicos presentan alguna debilidad, por ello es la importancia de la seguridad informática ya que se está invirtiendo para el objetivo más valioso de cualquier empresa: la seguridad. En un primer momento es muy importante conocer esos puntos débiles, posteriormente una vez identificados, las empresas deben definir las medidas de seguridad adecuadas con la finalidad de reducir los riesgos, y así evitar una amenaza. Finalmente se puede decir que la detección de una vulnerabilidad es el paso previo de que se efectúe una amenaza, ya que esta se encuentra presente en todo momento.

Referencia

Pirani: We make risk management simple. (s. f.). Pirani. https://www.piranirisk.com/

Thomson Reuters Mexico. (2022, 18 febrero). Thomson Reuters México - Respuestas confiables. https://www.thomsonreutersmexico.com/