Universidad Autónoma de Chiapas

Facultad: Contaduría y Administración

Licenciatura: Ingeniería en Desarrollo y Tecnologías de Software

Análisis de Vulnerabilidades

"1.3 Investigación de Conceptos"

Alumno: Nango Ponce Manuel de Jesus

Grupo: 7M

Matrícula: A200338

Docente: Luis Gutiérrez Alfaro

Tuxtla Gutiérrez, Chiapas
28/08/2023

¿Qué es la vulnerabilidad?

La **vulnerabilidad** en informática se refiere a una debilidad o fallo en un sistema de seguridad que puede ser explotado por un atacante para obtener acceso no autorizado a un sistema o red. En otras palabras, una vulnerabilidad es una brecha en la seguridad que puede ser explotada por un atacante para comprometer la integridad, confidencialidad o disponibilidad de los datos.

En el contexto de análisis de vulnerabilidades, se trata de identificar y evaluar las vulnerabilidades en los sistemas informáticos y redes para determinar su nivel de riesgo y tomar medidas preventivas para mitigarlos. Una evaluación de vulnerabilidad analiza y estima los riesgos de las debilidades en seguridad de los sistemas de información e informática de una organización. Se conocen más de 180.000 vulnerabilidades de seguridad y cada año se descubren nuevas.

¿Qué es seguridad?

La **seguridad** es un concepto amplio que se refiere a la protección de algo valioso contra posibles daños, peligros o amenazas. En el contexto de la informática, la **seguridad informática** o **ciberseguridad** se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la información contenida en una computadora o circulante a través de las redes de computadoras.

La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware, redes de computadoras y todo lo que la organización entienda y valore como un riesgo si la información confidencial involucrada pudiera llegar a manos de otras personas.

Existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura y/o a la propia información. La seguridad informática también se refiere a la práctica de prevenir los ataques maliciosos a las computadoras y los servidores, a los dispositivos móviles, a los sistemas electrónicos, a las redes y los datos.

Escribe los pilares de la seguridad

Los pilares de la seguridad son un conjunto de principios que se utilizan para garantizar la protección de los sistemas informáticos y la información que contienen. Los cuatro pilares principales son:

1. **Confidencialidad:** se refiere a la protección de la información contra el acceso no autorizado. La confidencialidad se logra mediante el uso de técnicas como el cifrado, la autenticación y el control de acceso.
2. **Integridad:** se refiere a la protección de la información contra la modificación no autorizada. La integridad se logra mediante el uso de técnicas como el control de versiones, las firmas digitales y los hash.
3. **Disponibilidad:** se refiere a la protección de la información contra la pérdida o el daño. La disponibilidad se logra mediante el uso de técnicas como la redundancia, los backups y los planes de contingencia.
4. **Autenticidad:** se refiere a la protección de la información contra la falsificación o el engaño. La autenticidad se logra mediante el uso de técnicas como las firmas digitales, los certificados digitales y los sistemas de autenticación.

Es importante tener en cuenta que estos pilares no son independientes entre sí, sino que están interrelacionados y se complementan mutuamente para garantizar una seguridad informática completa.

¿Cuáles son los cuatro elementos que la seguridad en informática intenta proteger?

La seguridad informática se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la información contenida en una computadora o circulante a través de las redes de computadoras.

Los cuatro elementos que se intentan proteger son:

1. **Información:** como activo intangible, representa quizá el elemento más sensible y vulnerable.
2. **Software:** cuya pérdida o modificación mal intencionada puede representar severos quebrantos económicos u operativos no solo hacia el usuario sino a toda una institución.
3. **Hardware:** que al fallar provoca retrasos en la operación diaria y la consecuente pérdida de tiempo y costos elevados.
4. **Redes de computadoras:** que permiten la comunicación entre dispositivos y sistemas, y que son esenciales para el funcionamiento de muchas organizaciones.

Escribe algunos ataques sobre los datos

Los ataques informáticos son una amenaza constante para la seguridad de los datos. Algunos de los ataques más comunes incluyen:

1. **Ataque de denegación de servicio (DoS):** Este ataque tiene como objetivo abrumar un servidor o red con tráfico falso para que no pueda responder a solicitudes legítimas.
2. **Ataque de denegación de servicio distribuido (DDoS):** Este ataque es similar al DoS, pero utiliza múltiples dispositivos para enviar tráfico falso a la red o servidor.
3. **Malware:** El malware es un software malicioso que se utiliza para dañar o tomar el control de un sistema. Los tipos comunes de malware incluyen virus, gusanos, troyanos y ransomware.
4. **Phishing:** El phishing es un ataque que utiliza correos electrónicos fraudulentos o sitios web falsos para engañar a las personas y obtener información confidencial, como contraseñas y números de tarjetas de crédito.
5. **Inyección SQL:** Este ataque se aprovecha de las vulnerabilidades en las aplicaciones web para insertar código malicioso en una base de datos.
6. **Ataque de hombre en el medio (MitM):** Este ataque intercepta la comunicación entre dos sistemas para robar información o modificarla.
7. **Ataque de día cero:** Este ataque aprovecha una vulnerabilidad desconocida en un sistema o aplicación antes de que se descubra y se corrija.

¿De que nos protegemos?

La seguridad informática se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la información contenida en una computadora o circulante a través de las redes de computadoras.

La seguridad informática nos protege de una amplia variedad de amenazas, incluyendo el robo de información personal, la divulgación no autorizada o accidental de información confidencial, el acceso no autorizado a sistemas y redes, el daño o la pérdida de datos, y el uso malintencionado de software y hardware.

En resumen, la seguridad informática nos protege contra cualquier amenaza que pueda comprometer la integridad, confidencialidad o disponibilidad de los datos y sistemas informáticos.

Menciona algunas amenazas que se concrete por medio de una vulnerabilidad?

Las amenazas que se pueden concretar por medio de una vulnerabilidad son variadas y pueden incluir el robo de información confidencial, la modificación o eliminación de datos, la interrupción del servicio, el secuestro de cuentas, la instalación de software malicioso, entre otros.

Menciona los tipos de vulnerabilidades

Existen varios tipos de vulnerabilidades en informática, entre las cuales se encuentran:

Vulnerabilidades de software: son debilidades en el código o diseño del software que pueden ser explotadas por un atacante para comprometer la seguridad del sistema.

Vulnerabilidades de hardware: son debilidades en los componentes físicos del sistema que pueden ser explotadas por un atacante para comprometer la seguridad del sistema.

Vulnerabilidades de red: son debilidades en la configuración o diseño de la red que pueden ser explotadas por un atacante para comprometer la seguridad del sistema.

Vulnerabilidades humanas: son debilidades en el comportamiento humano que pueden ser explotadas por un atacante para comprometer la seguridad del sistema.

¿Por qué aumentan las amenazas ?

Las amenazas informáticas aumentan debido a varios factores, como el aumento en el uso de tecnologías digitales, la creciente sofisticación de los ataques informáticos, la falta de conciencia sobre los riesgos de seguridad informática y la falta de inversión en medidas preventivas.

Menciona tres protecciones más usadas

Algunas protecciones más usadas para garantizar la seguridad informática son:

Firewalls: son sistemas diseñados para bloquear el tráfico no autorizado a una red o sistema.

Antivirus: es un software diseñado para detectar y eliminar software malicioso.

Autenticación multifactor: es un método de autenticación que requiere más de una forma de identificación para acceder a un sistema o red.

¿Qué es amenaza?

Una amenaza es cualquier acción o evento que pueda comprometer la integridad, confidencialidad o disponibilidad de los datos y sistemas informáticos.

¿Factores del riesgo de desastres desde el enfoque holístico ?

Desde el enfoque holístico, los factores de riesgo de desastres se dividen en tres categorías: factores físicos, factores sociales y factores económicos. Los factores físicos incluyen la ubicación geográfica, la topografía, el clima y la geología. Los factores sociales incluyen la densidad de población, la estructura social y la cultura. Los factores económicos incluyen el nivel de desarrollo económico, la distribución de la riqueza y los sistemas de producción.

¿Qué es la ingeniería social?

La ingeniería social es una técnica utilizada por los atacantes informáticos para engañar a las personas y obtener información confidencial. Los ataques de ingeniería social pueden tomar muchas formas, como correos electrónicos fraudulentos, llamadas telefónicas falsas o sitios web falsos. El objetivo de estos ataques es persuadir a las personas para que revelen información confidencial, como contraseñas o números de tarjetas de crédito.

¿Qué son los virus informáticos?

Los virus informáticos son programas maliciosos diseñados para dañar o tomar el control de un sistema informático. Los virus informáticos se propagan mediante la inserción de copias de sí mismos en otros programas o documentos. Cuando se ejecuta el programa o documento infectado, el virus se activa y puede causar daños al sistema, como la eliminación o modificación de archivos.

Define el concepto de autenticación

La autenticación es el proceso de verificar la identidad de un usuario o dispositivo que intenta acceder a un sistema o red. La autenticación se realiza mediante el uso de credenciales, como contraseñas o certificados digitales, que deben ser proporcionados por el usuario o dispositivo antes de que se les permita acceder al sistema o red.

Mecanismos preventivos en seguridad informática

Los **mecanismos preventivos** en seguridad informática son aquellos que se utilizan para evitar que se produzcan incidentes de seguridad. Algunos ejemplos de mecanismos preventivos incluyen:

Firewalls: son sistemas diseñados para bloquear el tráfico no autorizado a una red o sistema.

Antivirus: es un software diseñado para detectar y eliminar software malicioso.

Autenticación multifactor: es un método de autenticación que requiere más de una forma de identificación para acceder a un sistema o red.

Mecanismos correctivos en seguridad informática

Los **mecanismos correctivos** en seguridad informática son aquellos que se utilizan para solucionar los incidentes de seguridad después de que se han producido. Algunos ejemplos de mecanismos correctivos incluyen:

Análisis forense: es el proceso de recopilar y analizar evidencia digital para determinar la causa y el alcance de un incidente de seguridad.

Restauración de datos: es el proceso de recuperar datos perdidos o dañados debido a un incidente de seguridad.

Parches y actualizaciones: son correcciones de software diseñadas para solucionar vulnerabilidades conocidas en sistemas y aplicaciones.

¿Qué es el aumento de privilegios

El **aumento de privilegios** es una técnica utilizada por los atacantes informáticos para obtener acceso no autorizado a sistemas o redes. El aumento de privilegios implica obtener permisos o privilegios adicionales en un sistema o red que permiten al atacante realizar acciones que normalmente no estarían permitidas.

Técnicas de aumento de privilegios en windows y/o Linux

Algunas técnicas comunes de aumento de privilegios en Windows y Linux incluyen:

Explotación de vulnerabilidades: los atacantes pueden aprovechar las vulnerabilidades en sistemas y aplicaciones para obtener acceso no autorizado.

Ataques de fuerza bruta: los atacantes pueden intentar adivinar contraseñas mediante la fuerza bruta, es decir, probando todas las combinaciones posibles hasta encontrar la correcta.

Ataques de diccionario: los atacantes pueden utilizar diccionarios predefinidos o personalizados para adivinar contraseñas comunes o predecibles.

Protección frente al aumento de privilegios

Para protegerse contra el aumento de privilegios, es importante seguir buenas prácticas de seguridad informática, como mantener el software actualizado, utilizar contraseñas seguras y complejas, limitar los permisos y privilegios del usuario y utilizar herramientas como firewalls y antivirus.

CONCLUSIÓN:

La seguridad informática es un tema de gran importancia en la actualidad, ya que la información es uno de los activos más valiosos de cualquier organización. La protección de los sistemas informáticos y la información que contienen es fundamental para garantizar la integridad, confidencialidad y disponibilidad de los datos.

El análisis de vulnerabilidades es una técnica utilizada para identificar y evaluar las vulnerabilidades en los sistemas informáticos y redes. Al evaluar las vulnerabilidades, se pueden determinar los riesgos y tomar medidas preventivas para mitigarlos.

Es importante tener en cuenta que existen muchos tipos diferentes de amenazas informáticas, y que estas amenazas están en constante evolución. Por lo tanto, es fundamental mantenerse actualizado sobre las últimas tendencias y mejores prácticas en seguridad informática.

Algunas medidas preventivas comunes incluyen el uso de firewalls, antivirus y autenticación multifactor. En caso de que se produzca un incidente de seguridad, es importante contar con mecanismos correctivos como el análisis forense, la restauración de datos y los parches y actualizaciones.

En resumen, la seguridad informática es un tema complejo pero fundamental en el mundo digital actual. Al seguir buenas prácticas de seguridad informática y estar preparado para enfrentar las amenazas, se puede garantizar la protección de los sistemas informáticos y la información que contienen.

FUENTES DE INFORMACIÓN

1. Wikipedia. (2022). Vulnerabilidad (seguridad informática). Recuperado de https://es.wikipedia.org/wiki/Vulnerabilidad_(seguridad_inform%C3%A1tica)

2. Sánchez, J. (2019). Análisis de vulnerabilidades: qué es, tipos y herramientas. Recuperado de URL

3. NortonLifeLock. (2022). Common types of cyberattacks. Recuperado de https://www.nortonlifelock.com/cybersecurity/what-is-cybersecurity/common-types-of-cyberattacks

4. Kaspersky. (2022). What is cybersecurity? Recuperado de https://www.kaspersky.com/resource-center/definitions/what-is-cybersecurity

5. Palo Alto Networks. (2022). What is cybersecurity? Recuperado de https://www.paloaltonetworks.com/cyberpedia/what-is-cybersecurity

6. Sánchez, J. (2019). Análisis de vulnerabilidades: qué es, tipos y herramientas.

7. Kaspersky. (2022). What is social engineering? Recuperado de https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering