Introducción a la Ciberseguridad

Ciberseguridad – FPUNA

Amenazas

Amenazas

- Las amenazas de seguridad de la información o **ciberamenazas** son definidas por el Instituto Nacional de Estándares y Tecnologías (NIST) norteamericano. Este entiende la amenaza como un **evento con potencial de afectar negativamente a las operaciones de una organización o a sus activos**, ***"a través del acceso no autorizado a un sistema de información, la destrucción, divulgación o modificación de información y/o la denegación de servicio"*.**
- De esta forma, analizar las amenazas consiste en examinar fuentes de amenazas de seguridad de la información que pueden explotar las **vulnerabilidades** de un sistema. De esta forma, se podrán determinar los **riesgos** digitales o amenazas de ese sistema de información particular.

Vulnerabilidades

Vulnerabilidades

El concepto de amenaza también cuenta con una noción de vulnerabilidad. Esta puede considerarse como la debilidad en los procedimientos de seguridad de un sistema de información. Esta debilidad podría explotarse accidental o intencionadamente para violar los controles o la política de seguridad de dicho sistema. Se trata, por tanto, de un concepto diferente al de amenaza en Ciberseguridad. Las amenazas representan un potencial de daño mientras que las **vulnerabilidades** representan una condición para que se materialice ese daño.

Ejemplo

Teniendo en cuenta los **conceptos de amenaza y vulnerabilidad**, es posible poner como ejemplo una página web que procesa datos de tarjetas de crédito. Para esta página, Internet supone un entorno de amenazas, porque en él hay piratas informáticos y ciberdelitos, entre otros.

Más allá de ello, las vulnerabilidades de esta página web podrían ser que no se establezcan controles de autentificación para acceder a información relevante o que la arquitectura de red interna se exponga a redes no confiables como Internet.

Ataques

Ataques

Los ataques no deben confundirse con las amenazas. Los ataques o ciberataques son un mecanismo por el que un agente de amenazas explota una vulnerabilidad para causar un impacto de seguridad informática que afecte a la confidencialidad, integridad o disponibilidad de un sistema de información.

Gestión de Riesgo

Gestión de Riesgo

La gestión de riesgos de ciberseguridad es el **proceso** que tiene por objetivo la **identificación**, **análisis**, **medición** y **gestión de los riesgos asociados a la seguridad de la información** en lo relativo a la conexión al ciberespacio.

Consecuencias de la falta de gestión de riesgos de ciberseguridad

- Pérdidas de información.
- Incumplimientos y consecuencias legales.
- Accesos no autorizados a información confidencial o a las instalaciones.
- Robo de datos, información o incluso equipos.
- Daños en la reputación de la organización y la marca.
- Pérdidas económicas causadas por paralizaciones de la actividad, reclamaciones legales o reparación de daños.

Ataques comunes

Ciberataque

- Un ciberataque es un intento malicioso y deliberado por parte de un individuo o una organización para irrumpir en el sistema de información de otro individuo u otra organización. Usualmente, el atacante busca algún tipo de beneficio con la interrupción de la red de la víctima.

Malware

Malware es un término que se usa para describir el software malicioso, que incluye spyware, ransomware, virus y gusanos. El malware infringe las redes mediante una vulnerabilidad, usualmente cuando un usuario hace clic en un enlace peligroso o en un archivo adjunto de correo electrónico que, luego, instala un software riesgoso. Una vez dentro del sistema, el malware puede hacer lo siguiente:

- Bloquear el acceso a los componentes clave de la red (ransomware).
- Instalar malware o software dañino adicional.
- Obtener información furtivamente mediante la transmisión de datos del disco duro (spyware).
- Alterar ciertos componentes y hacer que el equipo sea inoperable.

Suplantación de identidad (phishing)

La suplantación de identidad (phishing) es la práctica de enviar comunicaciones fraudulentas que parecen provenir de fuentes confiables, habitualmente a través del correo electrónico. El objetivo es robar datos sensibles, como información de inicio de sesión y tarjetas de crédito, o instalar malware en la máquina de la víctima. La suplantación de identidad (phishing) es una ciberamenaza cada vez más común.

Ataque de intermediario

Los ataques de intermediarios (MitM – Man-in-the-Middle), también conocidos como ataques de escucha secreta, ocurren cuando los ataques se insertan en transacciones entre dos partes. Una vez que los atacantes interrumpen el tráfico, pueden filtrar y robar datos.

Hay dos puntos en común en las entradas de ataques de MitM:

1. En Wi-Fi público inseguro, los atacantes pueden insertarse entre el dispositivo del visitante y la red. Sin saberlo, el visitante pasa toda la información al atacante.
2. Una vez que el malware vulnera un dispositivo, el atacante puede instalar software para procesar toda la información de la víctima.

Ataque de denegación de servicio

Un ataque de denegación de servicio satura los sistemas, los servidores o las redes con tráfico para agotar los recursos y el ancho de banda. Como resultado, el sistema no puede completar las solicitudes legítimas. Los atacantes además pueden usar múltiples dispositivos comprometidos para lanzar un ataque. Esto se conoce como ataque por denegación de servicio distribuido (DDoS).

Inyección de SQL

Una inyección de lenguaje de consulta estructurado (SQL) ocurre cuando un atacante inserta un código malicioso en un servidor que usa el SQL y fuerza al servidor para que revele información que normalmente no revelaría. El atacante puede efectuar la inyección de SQL simplemente enviando un código malicioso a un cuadro de búsqueda de un sitio web vulnerable.

Ataques de día cero

Un ataque de día cero puede impactar después del anuncio de una vulnerabilidad en la red, pero antes de que se implemente un parche o solución. Los atacantes apuntan a la vulnerabilidad divulgada durante esta ventana de tiempo. La detección de amenazas a la vulnerabilidad de día cero requiere de atención constante.

Tunelización de DNS

La tunelización de DNS usa el protocolo DNS para comunicar tráfico que no pertenece al DNS por el puerto 53. Envía HTTP y otro tráfico del protocolo por el DNS. Hay varias razones legítimas para usar la tunelización de DNS. Sin embargo, también existen motivos maliciosos para usar los servicios de VPN de tunelización de DNS. Pueden usarse para encubrir tráfico saliente del DNS y ocultar datos que típicamente se comparten mediante una conexión a Internet. Para el uso malicioso, se manipulan las solicitudes del DNS a fin de exfiltrar los datos de un sistema comprometido a la infraestructura del atacante. También puede usarse para las retrollamadas de comando y control de la infraestructura del atacante al sistema comprometido.

Ciclo de vida de la seguridad

Ciclo PDCA

El ciclo PDCA obtiene este nombre debido a las siglas: **Plan-Do-Check-Act**. Su metodología se basa en la mejora continua, ya que un proceso no podrá ser nunca implantado al 100% de efectividad y precisión. Las palabras que dan nombre a este ciclo comprenden las 4 fases que se distinguen en ella.

Plan (Planificar)

El objetivo principal de esta fase es establecer el Sistema de Gestión de Seguridad de la Información (SGSI). Concretamente, se establecerán en este paso los objetivos, procedimientos y políticas relacionadas con la Seguridad de la Información, y con la visión puesta en mejorar esta última.

Asimismo, se deberán definir también aspectos tales como el alcance del Sistema de Gestión, los roles y sus funciones y responsabilidades en el proyecto.

Do (Hacer)

Se implementará en este punto el SGSI establecido. Se llevarán a cabo los procedimientos establecidos en la anterior fase y se implantarán los controles y operaciones necesarios con el fin de gestionar la información de la organización de una manera segura y eficaz.

Check (Verificar)

En esta fase se evaluará y revisará la efectividad del SGSI planificado e implantado en anteriores fases. Para ello, se comprobará que se cumplen aspectos tales como la **política de seguridad**, los objetivos o los diferentes procedimientos implementados.

Cabe destacar que estas evaluaciones y revisiones conviene que se lleven a cabo de manera periódica con el fin de asegurar la correcta implantación y funcionamiento de los procedimientos y acciones realizados para establecer e implementar el SGSI.

Act (Actuar)

En esta última fase del ciclo se mantendrá y mejorará el SGSI. Es decir, se llevarán a cabo **acciones y planes tanto correctivos como preventivos** para mejorar los resultados obtenidos e implementar y conseguir así una mejora continua del Sistema de Gestión de la Seguridad de la Información.