Capitulo 2:

Amenaza, Vulnerabilidad y Riesgo

Diferencias entre amenaza, vulnerabilidad y riesgo

“ La amenaza siempre está presente…
La vulnerabilidad la propicia el propio usuario.”

¿Qué es una vulnerabilidad?

Una vulnerabilidad pone en riesgo los datos y sistemas de una empresa comprometiendo su integridad, privacidad y disponibilidad.

- **Una debilidad propia de un sistema**
  - permite que un sistema sea atacado
  - Llamadas agujeros de seguridad
  - pueden ser solucionadas una vez sean descubiertas.

Se producen por:

- baja protección contra ataques externos
- falta de actualizaciones
- fallos de programación

Importante:

- Identificar las vulnerabilidades
- Aplicar las medidas correctoras que las eliminen.

Sistema Vulnerable:

“Sistema susceptible de recibir un determinado grado de daño»

(Ejemplo de Causas: falta de actualizaciones, baja protección contra virus, etc.)

¿Qué es una amenaza?

La **amenaza** consiste en aprovechar esa acción vulnerable para atacar el sistema.

Puede proceder de:

- ataques (virus)
- sucesos físicos (incendios)
- negligencias (contraseñas débiles).

Una Amenaza:

- Es la posibilidad de que un sistema vulnerable sea atacado y sufra daños.
- Las amenazas de un sistema informático provienen principalmente de ataques externos:

  - **malware**
  - **denegación de servicio**
  - **inyecciones SQL**
  - **etc**

Pueden llegar por:

1) no cumplir las políticas de seguridad
(conectar dispositivos no autorizados a la red o utilizar contraseñas débiles)

2) sucesos inesperados
(como incendios o robos físicos, por ejemplo).

¿Qué es un riesgo?

Es la posibilidad de que un sistema sufra un incidente de seguridad y que una amenaza se materialice causando una serie de daños.

«Se mide asumiendo que existe una cierta vulnerabilidad frente a una determinada amenaza»

Ej: puede ser un hacker, un ataque de denegación de servicios, un virus, etc

¿Cómo reducir el riesgo en un sistema?

La ciberseguridad de una organización consiste en reducir el riesgo de su infraestructura IT.

Se puede reducir el riesgo:

1- Al detectar e identificar las distintas vulnerabilidades existentes.
2- Aplicando las acciones necesarias para corregirlas
3- Evitar que las amenazas que representan puedan llegar a materializarse.

Medidas para Reducir Riesgos:

1- Realizar una **auditoría de seguridad**

- para identificar las vulnerabilidades

«Para establecer las amenazas que representan para los sistemas y la información»

2- Aplicar las medidas para **eliminar las vulnerabilidades**

- actualización de sistemas operativos
- actualizar programas informáticos
- aplicación de parches de seguridad).

3- Invertir en formación del personal

- eliminar los errores humanos relacionados con la seguridad
- fomentando las mejores prácticas.

4- Establecer protocolos de actuación

- en el caso de que una amenaza finalmente se materialice.

5- Definir una política de seguridad clara y concisa

- hacerla pública para que todo el personal

6- Integrar el **concepto de seguridad en todos los procesos y tareas** **de la empresa.**

- Cada acción o actividad que se realice en el negocio debe:
  - evaluar sus vulnerabilidades
  - establecer a qué amenazadas se expone
  - y así reducir el riesgo de que se produzcan.

7- Utilizar **herramientas de protección:**

- como firewalls
- programas antimalware
- sistemas de doble autenticación
- consolas de seguridad cloud, entre otros.

8- Utilizar **herramientas de monitorización** de seguridad para:

- detectar amenazas
- poder reaccionar de forma inmediata para evitarlas o reducir su impacto.

9- Llevar un **sistema de registro y documentación de toda la actividad relacionada con la seguridad, como:**

- incidencias de seguridad
- intervenciones realizadas
- protocolos de actuación, etc.

Ejemplo: uso de contraseñas débiles

→Mala politica de Seguridad

Vulnerabilidad: es esta falta de un procedimiento para el uso de contraseñas difíciles de descifrar.

Amenaza: posibilidad de sufrir un ataque donde la contraseña sea descubierta por un tercero con fines maliciosos.

Riesgo: que se consuma la amenaza y que la vulnerabilidad sea explotada.

10- Apostar por **proveedores de servicios cloud con un alto nivel de seguridad**

- que cuenten con las certificaciones y credenciales de seguridad aceptadas como estándares a nivel mundial.

Amenazas más importantes a las que se enfrenta una infraestructura IT son:

Software incorrecto

Virus

SQL Injection

Gusanos

Keylogger

Personas-ex-activistas

Spyware

Ingeniería Social

Amenazas Lógicas

Fuerza bruta

Ataque de día cero.

Spam

Malware

Man in the middle

DDOS

Puertas traseras

troyanos

Cross site Scripting

Phishing

Ransomware

Robo de identidad.

El phishing o robo de identidad.

La amenaza consiste en:

«Engañar al usuario»

Ej: para que facilite de forma involuntaria sus credenciales de acceso a un tercero que las utilizará de forma fraudulenta

TEST

https://phishingquiz.withgoogle.com/?hl=es

Código malicioso. Estos ataques malware atacan dispositivos y servidores con el fin de robar información sensible, como datos bancarios o credenciales de acceso.

Ej: Los ataques ransomware son una de las mayores amenazas hoy en día para los sistemas informáticos de las empresas.

Ejemplo: una web debe estar actualizada con las herramientas de seguridad adecuadas para evitar ser vulnerables a amenazas, aunque siempre existirá el riesgo de sufrir un ataque.

Origen de las Amenazas

Personas

Atacantes

Personas

Con frecuencia el punto más débil de cualquier sistema informático son las personas relacionadas en mayor o menor medida con él.

Ej:

1) Un administrador sin conocimientos adecuados o experiencia.

2) Un guardia de seguridad que deja acceder a cualquier usuario a la sala de operaciones.

Atacantes:

Se dividen en dos grandes grupos:

Atacantes pasivos:

- aquellos que fisgonean por el sistema pero no lo modifican, ni destruyen.

Atacantes activos:

- aquellos que dañan el objetivo atacado, o lo modifican en su favor.

Personal de la Organización

Ataques Intencionados:

- efectos son extremadamente dañinos
- el propio personal de la organización conoce mejor los sistemas y sus debilidades

No intencionados:

- accidentes causados por un error o por desconocimiento de las normas básicas de seguridad.

Importante:

Las amenazas a la seguridad de un sistema provenientes del personal de la propia organización:

- **rara vez son tomadas en cuenta**

- **se presupone un entorno de confianza**

«cualquier persona de la organización, incluso el personal ajeno a la infraestructura informática puede comprometer la seguridad de los equipos»

Ex-Empleados

- antiguos empleados

- empleados que pasaron a la competencia.

- Personas descontentas con la organización

«Tratar de conectarse al sistema como si aún trabajaran para la organización (muchas veces se mantienen las cuentas abiertas por descuido). Conseguir el privilegio necesario, y dañarlo de la forma que deseen.»

Curiosos

- Persona con formación en la informática y las telecomunicaciones .
- Curiosas por naturaleza.
- intentan conseguir mayor privilegio
- intentan acceder a sistemas a los que oficialmente no tienen acceso.

Crackers

Intrusos que utilizan los sistemas para fisgonear, para utilizarlas como enlace hacia otras redes o simplemente por diversión.
-En redes generalmente abiertas, y la seguridad no es un factor tenido muy en cuenta en ellas.

Terroristas

Cualquier persona que ataca al sistema simplemente por causar algún tipo de daño en él.

Intrusos remunerados

Se trata de piratas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema, que son pagados por una tercera parte

Amenazas Lógicas

Todo tipo de programa que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello:

- **software malicioso (malware)**
- **error (bugs o agujeros).**

Malware:
Se cataloga como un código malicioso compuesto por gusanos, worms, spyware, troyanos, virus o script malintencionados que tiene como propósito infiltrarse y dañar un computador o sistema de información sin el consentimiento de los propietarios.

Software incorrecto

Errores cometidos de forma involuntaria por los programadores de sistemas o de aplicaciones.

A estos errores de programación se les denomina bugs, y a los programas utilizados para aprovechar uno de estos fallos y atacar al sistema, exploits.

Herramientas de seguridad

Cualquier herramienta de seguridad representa un arma de doble filo:

- De la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa.

- Un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos.

Puertas traseras

Atajos en los sistemas habituales de autenticación del programa o de un sistema.

Ej: un programador puede dejar atajos en las versiones definitivas de su software para facilitar un mantenimiento posterior, para garantizar su propio acceso, o simplemente por descuido.

Bombas lógicas

Las bombas lógicas son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas..
Al llegar aquí, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial.

Se pueden activar por:

- la ausencia o presencia de ciertos ficheros
- la ejecución bajo un determinado UID (User ID)
- la llegada de una fecha concreta

Canales encubiertos

Los canales encubiertos o canales ocultos son canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema.

- Es un proceso transmite información a otros (locales o remotos) que no están autorizados a leer dicha información.

Virus

Un virus es una secuencia de código que se inserta en un fichero ejecutable (denominado **huésped**), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.

Gusanos

Un gusano es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes.

- en ocasiones portando virus o aprovechando bugs de los sistemas a los que conecta para dañarlos.
- Son difíciles de programar su número no es muy elevado, pero el daño que pueden causar es muy grande:

Un gusano puede automatizar y ejecutar en unos segundos todos los pasos que seguiría un atacante humano para acceder a nuestro sistema, de ahí su enorme peligro y sus devastadores efectos.

Caballos de Troya

Los troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas (generalmente en detrimento de la seguridad) sin el conocimiento del usuario.

Como el Caballo de Troya de la mitología griega, al que deben su nombre, ocultan su función real bajo la apariencia de un programa inofensivo que a primera vista funciona correctamente.

Programas conejo o bacterias

Programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco, etc.).

- **Por sí mismos no hacen ningún daño**
- **Lo que realmente perjudica es el gran número de copias suyas en el sistema.**
- **Produciendo una negación de servicio.**

Técnicas salami

Robo automatizado de pequeñas cantidades de bienes, en general dinero, de una gran cantidad origen.

- El hecho de que la cantidad inicial sea grande y la robada pequeña hace extremadamente difícil su detección.

- Las técnicas salami se utilizan en sistemas bancarios, o software dedicados a contabilidad, facturación etc.

Recomendaciones contra Ataques

Virus y Gusanos

- Son los tipos más conocidos de software maligno
- Al ser ejecutados en un ordenador infecta otro software que este contenga

Como Protegerse

1) Tenga actualizado el sistema operativo y los navegadores web que utiliza.
2) Instale el antivirus y active el firewall y configúrelos para que se actualicen automáticamente.
3) Utilice contraseñas de alta seguridad.
4) Instale un programa antimalware que le proporcione protección en tiempo real.

Troyanos

Permite la administración remota de un ordenador de forma oculta sin la autorización del usuario.

Como protegerse :

1) Evite conectarse a una red WIFI abierta.

2) Active los controles de integridad de los archivos de sistemas.

3) Separe las cuentas de usuario de las cuentas administrador.

4) Use programas especializados para detectar posibles intrusiones.

5) Utilice cifrado de disco.

Phishing

Su objetivo es intentar obtener datos como usuarios . Usando técnica de suplantación de identidad.

Como protegerse:

1) No responda ningún correo electrónico o llamadas donde le soliciten información personal.

2) Teclee la dirección o URL para realizar visitas en sitios web y más si consulta entidades bancarias por la red.

Ataques informáticos a sitios web y servidores:

SQL Injection

- Es uno de los ataques más usados para obtener acceso a las tablas de bases de datos, donde incluye información del usuario con su contraseña.
- Este tipo de ataque es más común en organizaciones y negocios de comercio electrónico.

Este ataque se caracteriza por ser fácil de ejecutar, ya que utiliza una técnica que modifica la cadena de consulta en base de datos donde se encuentra una inyección de código en la consulta.

Como protegerse:

1) No utilice sentencias SQL construidas dinámicamente.
2) No utilice cuentas con privilegios administrativos.
3) No proporcione mayor información de la necesaria.
4) Verifique el tamaño como el tipo de datos de las entradas del usuario.

DDOS

Su objetivo principal es denegar el funcionamiento de sitios web, donde se vulnera la disponibilidad del servicio ya que cuando un usuario trata de ingresar al sitio este se encuentra fuera de servicio cumpliendo con el objetivo propuesto.

Distintos tipos de ataques DDoS

- **Ataques por volumen:** donde se intentan desbordar el ancho de banda de un sitio web.
- **Ataques de protocolo:** donde los paquetes intentan consumir servicios de red.
- **Ataques de aplicaciones:** donde las peticiones se hacen con el fin de explotar un servidor web mediante la capa de aplicación.

Como protegerse del ataque DDoS:

1) Restringir el uso de ancho de banda a los hosts que cometan violaciones.

2) Realice un monitoreo de las conexiones TCP/UDP que lleve a cabo el servidor.

3) Limite el número de conexiones concurrentes en el servidor.

Fuerza bruta

El objetivo de este ataque es intentar romper todas las combinaciones posibles de nombre usuario y contraseña.

Como protegerse del ataque:

1) Bloquee el número de intentos fallidos al introducir el usuario y la contraseña.
2) Utilice una contraseña segura de más de 8 caracteres realizando combinación de mayúsculas, minúsculas, letras y números.
3) Evite un nombre de usuario como admin, administrador.

Cross site Scripting

(XXS) permite inyectar scripts maliciosos en sitios web inofensivos, es utilizado para obtener acceso a una cuenta de usuario.

Como protegerse del ataque:

1) No confié en datos que vengan de usuarios externos.

Man in the middle

Se utiliza para supervisar la comunicación entre dos partes y falsifica los intercambios para hacerse pasar por una de ellas , este ataque es realizado utilizando la técnica de rastreo de puertos.

Como protegerse:

1) Utilice un sistema de cifrado fuerte entre cliente servidor mediante un certificado digital.
2) Evite que los usuarios puedan conectarse a una red wifi abierta.

Ataque de día cero

Tratan de explotar las vulnerabilidades que no han sido detectadas e informadas a la audiencia. Son vulnerabilidades desconocidas y que se presentan si aún no se cuenta con una actualización o parche que lo proteja de la vulnerabilidad.

Como protegerse :

1) Elimine del sistema aplicaciones que no utilice.
2) Mantenga actualizado los parches de los proveedores de los programas.
3) Utilice un sistema de prevención contra intrusos HIPS con el fin de detener otra amenaza.

Ingenieria Social

Es el arte de engañar a las personas.

- Las amenazas de la ingeniería social son más peligrosas, ya que es más difícil protegerse frente a ellas, debido a que el objetivo principal no solamente el sistema si no la víctima.
- Es una técnica de hackeo utilizada para extraer información a otras personas, teniendo como base la interacción social:

«Donde la persona que está siendo atacada no se da cuenta cuando suministra información personal que puede terminar en manos de un atacante.»

Como protegerse:

1) No revele datos confidenciales por ningún medio (llamadas telefónicas, personal desconocido o correos electrónicos no confiables).

2) Nunca ingrese a links de páginas web que lleguen por medio de email desconocidos donde le soliciten información confidencial y siempre digite la url de los sitios web al que desea ingresar.

3) Clasifique su información confidencial y destruya información que usted no utilice.

Sea reservado con su información , recuerde que es un activo propio que solo le pertenece al responsable.

Hacking Etico

- Es una metodología utilizada para simular un ataque malicioso sin causar daño con el fin de analizar las brechas de seguridad que contiene una red.
- Tiene como fin poder identificar los riesgos a los que se encuentran expuesta la red de una organización.
- Se basa en procedimientos basados en una investigación preliminar de análisis de vulnerabilidades

Procedimiento

1. Se identifican vulnerabilidades criticas del sistema

2. Se realiza la explotación de vulnerabilidades, donde se evidencia los puntos sensibles que se encuentran expuestos

3. Se procede a realizar un análisis con el fin de dar las respectivas recomendaciones de como mitigar las brechas de seguridad encontradas.