Actividad 2.1 Análisis de riesgos.

Integración de seguridad informática en redes y sistemas de software

Grupo 402

José Antonio González Martínez - A01028517
Rodrigo Sosa Rojas - A01027913
Luis Daniel Filorio Luna - A01028418
Gabriel Muñoz Luna - A01028774

Osvaldo Cecilia Martínez

Fecha de entrega

29/08/2024

3 activos y 3 amenazas

Para la actividad seleccionamos STRIDE y los activos con sus respectivas amenazas que encontramos fueron

- Base de datos, la cual puede sufrir Tampering, Denial of Service, Information Disclosure
- Dispositivos de los programadores los cuales pueden sufrir Elevation of privilege, Tampering, Repudiation
- Servidor Web el cual puede sufrir Denial of service, Spoofing, Elevation of privilege

Tabla de Probabilidad/Impacto

	Probabilidad	Impacto
Base de datos:		
Tampering	Medio	Medio
Denial of Service	Medio	Alto
Information Disclosure	Alto	Alto
Dispositivos de programadores:		
Elevation of privilege	Alto	Medio
Tampering	Medio	Alto
Repudiation	Medio	Medio
Servidor Web		
Denial of service	Alto	Medio
Spoofing	Bajo	Bajo
Elevation of privilege	Medio	Bajo

(Aquí va el diagrama)

Análisis de Riesgos

Base de Datos

Revelación de Información (Impacto Alto, Prob. Alta) → Debido a la baja protección de los PDF enviados sin encriptación, el riesgo de que la información sea revelada sin autorización es muy alto. Esto debe ser evitado a través de algún tipo de encriptación de los PDF

Tampering (Impacto Medio, Prob. Medio) → Debido a que se pudo tener acceso a la base de datos consideramos que de misma forma se podría acceder a los mencionados y manipularlos a placer, sin embargo de la misma forma se tiene el backup lo cual nos da un daño medio al sistema.

Denegación de Servicios (Impacto Alto, Prob. Media) → El denegar los datos puede provocar que no se tenga un servicio durante un periodo de tiempo considerable lo cual puede llegar a afectar el funcionamiento del sistema en su totalidad

Dispositivos de programadores

Elevación de privilegios (Impacto Medio, Prob. Alto) → Al obtener permisos de administrador se puede llegar a manipular diversas secciones del sistema

Tampering (Impacto Alto, Prob. Media) → Al perder los programadores el acceso a los datos, es posible que puedan cambiarse datos, afectando la productividad y confiabilidad de la empresa

Repudiation (Impacto Medio, Prob. Media) → Debido a que la empresa recibió un ataque, es posible que algunos clientes decidan no recurrir a sus servicios nuevamente, lo que afectaría a la empresa

Servidor Web
Denegación de Servicios (Impacto Medio, Prob. Alto) → Al bloquear el servicio web se deniega acceso de los usuarios al sistema para poder hacer las solicitudes del sistema

Spoofing (Impacto Bajo, Prob. Bajo) → El robo de identidad permite poder acceder al sistema e interactuar con diferentes aspectos del servidor lo cual podría bloquear algunos componentes de dicho servidor

Elevación de privilegios (Impacto Bajo, Prob. Medio) → El acceso al servidor web solo está permitido para los programadores por lo que el que algún externo adquiera estos privilegios no representa un peligro tan alto ya que se puede detectar el origen del problema.

Matriz de riesgos

		Impacto		
		Alto	Medio	Bajo
Probabilidad	Alto	Alto	Alto	Medio
	Medio	Alto	Medio	Medio bajo
	Bajo	Alto/medio	Bajo	Bajo

Base de datos	
Tampering	Medio
Denial of Service	Alto
Information Disclosure	Alto
Dispositivos de programadores	
Elevation of privilege	Alto
Tampering	Alto
Repudiation	Medio
Servidor Web	
Denial of service	Alto
Spoofing	Bajo
Elevation of privilege	Medio bajo

Análisis de la matriz de riesgos

Base de Datos

- **Information Disclosure:** Evitarlo, esta es la de más alto riesgo en nuestra matriz de riesgo. Se deben implementar medidas de seguridad para evitar esto, como por ejemplo cifrar los datos.
- **Denial of Service:** Mitigarlo, aunque el impacto de este es alto se puede prevenir de manera efectiva en caso de llegar a suceder, que no afecte tanto, un ejemplo puede ser algún servicio que prevenga ataques DDOS,

- **Tampering:** Mitigarlo, este se puede prevenir de una buena manera aplicando certificados de autentificación para evitar que se manipulen los datos.

Dispositivos de programadores

- **Elevation of privilege:** Mitigarlo, se puede evitar haciendo un control estricto de los privilegios de cada usuario, para evitar que alguien reciba más.
- **Tampering:** Mitigarlo, tiene un nivel alto porque en las computadoras se maneja información y datos importantes, pero se puede prevenir con la automatización de identidad.
- **Reputation:** Aceptarlo, esta amenaza se puede aceptar siempre y cuando se haga un registro de cada acción que se realiza, y se realicen auditorías recurrentes.

Servidor web

- **Denial of service:** Mitigarlo, al igual que en la base de datos, se puede mitigar el impacto con diferentes recursos, como por ejemplo un firewall.
- **Elevation of privilege:** Aceptarlo, al ser bajo, se puede aceptar ya que se puede prevenir mientras se tenga un control de los privilegios de los desarrolladores.
- **Spoofing:** Aceptarlo, el riesgo es bajo y la probabilidad también, por lo que se puede aceptar y se puede mantener controlado siempre y cuando se tenga medidas básicas de seguridad.
-

Controles que se usarían

Base de datos

- **Information Disclosure:** Cifrar los datos y mantener el control del acceso a la base de datos, el cifrado de datos protege la información almacenada en la base de datos, aun y cuando se accede de manera no autorizada, el control de acceso nos permite saber quién ve y qué información puede ver.
- **Denial of Service**: Implementación de firewall y protección contra ataques DDOS, el firewall permiten tener una protección primaria evitando que llegue contenido malicioso a la base de datos, la protección DDOS permiten detectar cuando se está realizando un ataque DDOS asegurando que no se termine de concretar.
- **Tampering**: Implementación de un registro, el implementar un registro permiten que cualquier cambio realizado sea rastreado y evitando cualquier tipo de tampering

Dispositivos de los programadores

- **Elevation of privilege**: Implementación de un sistema de privilegios y control de acceso, al implementar un sistema de privilegios puedes asegurar que las personas tenga el mínimo de privilegios necesarios para realizar sus actividades y teniendo un control de acceso puedes revisar cuales son los privilegios que tienen y poder modificarlo a mejor.

- **Tampering**: Controles de cambio y supervisión en tiempo real, los controles de cambio te permiten evitar realizar cambios no autorizados en los archivos, al tener alguna herramienta de supervisión en tiempo real nos permite prevenir y alertar ante cualquier intento sospechoso.

- **Repudiation**: Implementación de Logs, al implementar un registro de las actividades realizadas por los programadores no se puede evitar decir que no se realizó algo que sí se hizo.

Servidor Web

- **Denial of service**: Obtención de otro servidor, al tener más servidores se puede tener una carga diferente en cada servidor, por lo que, en caso de que uno llegue a fallar o ser atacado se pueda seguir normal y que el otro funcione.

- **Spoofing**: Uso de certificados SSL, estos certificados permiten la comunicación usuario servidor de manera encriptada, lo que evita que se realice suplantación de identidad.

- **Elevation of privilege**: Control de accesos, esto permite tener el control de a qué partes del servidor tienen acceso limitado para que los usuarios accedan a algo que no deben.