Curso: COMP 2700 – Ciberseguridad

Laboratorio: Laboratorio 1 – Análisis de Vulnerabilidades, Riesgos y Controles

Sección: 92249

Líder del grupo: Benyahir Y. Martínez Hermina

Integrantes:

- Benyahir Y. Martínez
- Jacob J. Desuza
- Emanuel V. Rodríguez
- John A. Valentín

Parte 1 – Panorama y Vulnerabilidades

1. **Selección del escenario:**

   - Escenario hipotético: El servicio online de un banco realiza un mantenimiento en su sitio web. Hay un error en el mantenimiento realizado y ahora los clientes pueden acceder a las cuentas administrativas del banco y con esto ven toda la información de los clientes. El banco no se percata y el error continúa por varias horas. Un usuario se da cuenta de esto y se aprovecha para hacer un ransomware con la información de los clientes.

2. **Identificación de vulnerabilidades:**

   a. **Vulnerabilidad técnica:** Los administradores del servicio en línea del banco no se percatan del error por varias horas.

   b. **Vulnerabilidad lógica:** Después del error en mantenimiento, los clientes pueden acceder a cuentas de clasificación administrativas, lo que les permite ver la información confidencial de otros clientes.

   c. **Vulnerabilidad humana:** La persona o equipo que se encarga del mantenimiento provocan el error de manera accidental**.**

Parte 2 – Análisis de Riesgos y Amenazas

Vulnerabilidad técnica: Los administradores del servicio en línea del banco no se percatan del error por varias horas.

Amenaza asociada: No es un error humano por parte que los administradores cuando establecieron el servicio este no presentaba ningún problema, sino que se demostró después. Tampoco es malicioso porque los administradores no tenían ninguna intención maliciosa al establecerlo.

Impacto en la CIA:

C – Debido a que el error no fue detectado por varias horas la confidencialidad de esos datos personales almacenados por el servicio pueden ser expuestos por otros usuarios del servicio.

I – Los datos de los clientes pueden ser modificados de manera errónea o borrados por parte del malfuncionamiento del servicio.

A – Cualquier persona que quería revisar o acceder a sus estados bancarios se puede encontrar con la información de otro usuario.

		Impacto	
Probabilidad	**Bajo**	**Medio**	**Alto**
Bajo	Bajo	Bajo	Medio
Medio	Bajo	Medio	Alto
Alto	Medio	Alto	Crítico

Justificación: Este error en el servicio del banco expone demasiada información personal de otros usuarios hacia otros usuarios que están utilizando el servicio y si uno de estos usuarios toma esa información ajena para hacer algo incorrecto, el riesgo de esta vulnerabilidad es demasiado alto.

Vulnerabilidad lógica: Después del error en mantenimiento, los clientes pueden acceder a cuentas de clasificación administrativas, lo que les permite ver la información confidencial de otros clientes.

Amenaza asociada: Es una amenaza humana debido a que fue accidentalmente provocada por error humano y podría ser explotada también por humanos. Puede ser considerada no maliciosa debido a que fue intencional pero también podría ser maliciosa porque alguien puede utilizar la información de los clientes para el mal.

Impacto en la CIA:

C – Si la información es accedida mediante la vulnerabilidad, se pierde completamente la confidencialidad debido a que un cliente que haya accedido ve la información de los demás.

I – La vulnerabilidad les permite a los usuarios acceder como administradores, lo que les permitirá eliminar y editar información, perdiendo la integridad de esta.

A - Los usuarios con intenciones maliciosas podrían eliminar o esconder información vital de los clientes, eliminando la disponibilidad.

	Impacto		
Probabilidad	**Bajo**	**Medio**	**Alto**
Bajo	Bajo	Bajo	Medio
Medio	Bajo	Medio	Alto
Alto	Medio	Alto	Crítico

Justificación: Se clasificó como critico debido a que las posibilidades de que la vulnerabilidad sea explotada son altas y esto significaría daños catastróficos para los clientes y el banco.

Vulnerabilidad humana: La persona o equipo que se encarga del mantenimiento provocan el error de manera accidental**.**

Amenaza asociada: Es una amenaza humana debido a que esta fue ocasionada por el grupo que se encargaba del mantenimiento. El personal no tenía ninguna mal intención para causar el problema debido que fue un accidente.

Impacto en la CIA:

C – El banco puede perder la confianza de sus clientes y sus inversores por este problema accidental que estos causaron en los datos sensibles.

I – Los datos pudieron haber pasado por algún tipo de corrupción modificándolos drásticamente por parte del accidente.

A – Alguien que utilice el sistema puede encontrase con los datos de otros usuarios y mal usarlos.

		Impacto	
Probabilidad	**Bajo**	**Medio**	**Alto**
Bajo	Bajo	Bajo	Medio
Medio	Bajo	Medio	Alto
Alto	Medio	Alto	Crítico

Justificación: En base a esta vulnerabilidad varios usuarios pueden hacer mal uso de la información de otros usuarios y también el banco podría perder estos como clientes debido a que el problema fue un accidente completamente arruinando su reputación.

Pate 3 – Ataques, Daños y Controles

1. **Vulnerabilidad técnica:** Los administradores del servicio en línea del banco no se percatan del error por varias horas.

   Ataques Posibles:

   Intercepción: Un cliente o atacante obtiene acceso a los datos sensibles de los clientes mientras que los usuarios continúan usando los servicios bancarios.

   Daños Esperados:

   Confidencialidad: Debido a que el error no fue detectado por varias horas la confidencialidad de esos datos personales almacenados son expuestos otros usuarios del servicio.

   Integridad: Los datos de los clientes pueden ser modificados o ser eliminados.

   Disponibilidad: Clientes pueden entrar al servidor, pero habrá errores al entrar.

   Reputación: El banco puede perder la confidencialidad del cliente al ellos no poder proteger sus datos y no arreglar a tiempo el error.

   Recurso/Dinero: Perdida de gran cantidad datos

   Control Inicial:

   Prevenir:

   - Revocar accesos innecesarios de las cuentas.
   - Forzar acciones inmediatas de credenciales.
   - Habilitar MFA

2. **Vulnerabilidad lógica:** Después del error en mantenimiento, los clientes pueden acceder a cuentas de clasificación administrativas, lo que les permite ver la información confidencial de otros clientes.

Ataques Posibles:

Modificación: Un atacante obtiene la oportunidad para entrar a los datos sensibles del banco y cambiar permisos dándose la entrada a sí mismo.

Daños Esperados:

Confidencialidad: Usuario maliciosos pueden entrar al sistema bancario del banco o los datos de un cliente.

Integridad: Registro financiero y balances de cuentas alterados

Disponibilidad: Al estar toda la información alterada del cliente, no hay una disponibilidad segura a la información.

Reputación: Perdida de reputación total, el cliente perderá la confianza del banco y se cambiará a otro banco.

Recurso/Dinero: Información sensible, multas y perdida de un aproximado de $1,000,000

Control Inicial:

Prevenir:

- Invalidar sesiones y tokens con privilegios de escrituras.
- Congelar escritura en producción. (solo lectura)
- Eliminar o limitar cuentas con acceso masivo.

3. **Vulnerabilidad humana:** La persona o equipo que se encarga del mantenimiento provocan el error de manera accidental**.**

Ataques Posibles:

Intercepción: Un atacante aprovecha el error para obtener acceso a la base de datos del banco.

Interrupción: El servidor se encuentra vulnerable a un malware que potencialmente afectaría todos sus datos.

Daños Esperados:

Confidencialidad: Los datos de la cuenta bancaria se ve expuesto a un atacante.

Integridad: Los datos pudieron haber pasado por algún tipo de corrupción.

Disponibilidad: Se pierde la accesibilidad a todas las cuentas bancarias debido al atacante quien tomó el control.

Reputación: Perdida de reputación debido a la perdida de datos personales, el cliente perderá la confianza en el banco.

Recurso/Dinero: Perdida de un aproximado de $1,000,000 en multas y al intentar de recuperar los datos.

Control Inicial:

Prevenir:

- Aislar el servidor vulnerable
- Restaurar datos desde snapshot/backup
- Revertir cambios realizados durante mantenimiento

Conclusión: ¿qué vulnerabilidad representa mayor riesgo y por qué?

Consideramos que la vulnerabilidad que representa mayor riesgo es la vulnerabilidad humana, debido a que no sabemos si fue un error o intencional (parte del empleado de mantenimiento). Esto puede tener un impacto fuerte en la reputación del banco, haciendo que clientes e inversionistas no quieran trabajar más con ellos. Adicionalmente, el banco se puede ver gravemente afectado, teniendo pérdidas económicas como: multas, recuperación de datos, mantenimiento y restauración de el servicio por completo.

Nombre del integrante	¿Qué realizó?	% del trabajo
Benyahir Y. Martínez	Parte 1, 2 y Conclusión	25%
Jacob J. Desuza	Parte 1, 3 y Conclusión	25%
Emanuel V. Rodríguez	Parte 1, 3 y Conclusión	25%
John A. Valentín	Parte 1, 2 y Conclusión	25%