WORKSHOP1

ETL

**EXTRACTION, TRANSFORMATION AND LOAD**

**Dayanna Vanessa Suarez Mazuera - 2221224**

**Ingeniería de Datos e Inteligencia Artificial**

**Semestre 5**

**Corte 1**

**ETL**

**C**

**Santiago de Cali, Valle del Cauca**

**2024 - 01**

RESPUESTAS

Tomando como referencia el caso anteriormente expuesto, estas son las respuestas de las preguntas enumeradas:

1. **C) Los funcionarios del área de tecnología**
2. **D) Los definidos en la valoración de activos**
3. **A) Todos los usuarios y contratistas del Banco Autónomo de Occidente**
4. **C) Plan de continuidad del negocio**
5. **A) Informando que las políticas y practicas del banco aseguran la información**
6. **C) Realizar copia de seguridad diaria de la base de datos y tener accesos restrictivos**
7. Podemos darnos cuenta de que el tipo de ataque fue un ransomware ya que cifró los archivos del contratista de tecnología y exigió un rescate de 10 bitcoins para descifrarlos. Como ya hemos visto anteriormente en clase, el objetivo de este tipo de ataque es bloquear el acceso a los archivos de la víctima y luego exigir el pago de la clave de descifrado.

Posibles causas de este ataquen podrían ser:

1. Ingeniería social, ya que el atacante utilizó técnicas de ingeniería social para engañar al contratista haciéndole creer que estaba recibiendo actualizaciones legítimas del agente de la VPN, ya que incluso lo llamaron 2 minutos después para actualizar además el firewall.

2. Falta de conciencia del personal, en esto hago referencia a la falta de conciencia sobre la seguridad que puede haber contribuido a que el contratista no sospechara de las solicitudes de actualización y que consecuente diera el permiso de acceso a su computadora personal.

Controles implementados:

1. Aunque se menciona que se brindó capacitación sobre varios métodos de ataque, centrarse únicamente en capacitar al personal técnico sobre el acceso remoto puede dejar brechas de seguridad por la no capacitación de otros empleados.

2. Al realizar su tranformacion digital, considero como punto crucial el trabajar en la política de acceso a la información, aunque en el caso no detalla la implementación y difusión efectiva de esta política podemos darnos cuenta que al no realizar una rápida aplicación de esta, se pudo efectuar el ataque.

3. La falta de planificación de emergencia también contribuyó a la pérdida de datos y a la interrupción de las operaciones del banco.

La respuesta del banco tiene aspectos tanto positivos como negativos:

Negativo por la falta de un plan de recuperación ante desastres y además de la pérdida de datos debido a la restauración de la copia de seguridad (que estaba en una cinta magnética hasta el 1 de julio de 2023) indicando una mala respuesta contra estos incidentes. Y positivo por la buena decisión de no pagar el rescate y seguir las recomendaciones de las autoridades de evitar financiar a delincuentes y tomar medidas para recuperarlo.

1. Como ya he mencionado anteriormente, algunas de las estrategias de la información podrían ser:

Concientización/ Capacitacion y Políticas de Privacidad

Esto con el fin de realizar programas orientados a todos lo empleados del banco, no solo el personal de la Tecnología, además es importante establecer unas políticas claras y comunicarlas hacia todo el personal sobre el acceso a la información y el manejo de datos privados.

Actualización de las copias de seguridad y Software

Plantear un horario de actualización de software y parches del sistema para asegurar a los empleados que se realizara de forma segura y controlada. Además de realizar una constante actualización de las copias de seguridad y almacenarlas en un entorno seguro, preferiblemente fuera de la red principal.

Segmentación de Redes

Como lo mencionamos en clases anteriores, esto ayuda a limitar la propagación del malware en caso de un ataque, evitando así que el atacante pueda acceder fácilmente a la red

Plan para contrarrestar ataques  
Desarrollar un plan de recuperación ante desastres para minimizar el tiempo de inactividad en el momento que surja un problema. La capacidad de restaurar rápidamente sistemas y datos es esencial para garantizar la continuidad del banco, además de que sea capaz de detectar que partes del sistema fueron vulnerados.