Carlos Alberto Rasgo Solano

Paso 1: ¿Cuál es el ataque que nos afectó?

En nuestra empresa se afectaron los sistemas con un **ransomware**.

Causa:
Uno de nuestros funcionarios descargó e instaló un archivo APK con un troyano desde un sitio no oficial. Al ejecutar el archivo, el malware obtuvo sus credenciales y comenzó a propagarse. A partir de los logs del sistema, se detectaron múltiples intentos de ejecutar acciones sin autorización, lo cual activó las alertas de seguridad internas. Durante la investigación, se descubrió que varias áreas estaban afectadas, especialmente en la consulta de información desde la página web: los datos aparecían erróneos o sin sentido.

Además, uno de los signos más claros del ataque fue que varias pantallas de los equipos mostraban mensajes de rescate, confirmando así la naturaleza del ransonware.

Consecuencia:
Los sistemas de consulta de información de la empresa colapsaron, lo que afectó directamente la calidad del servicio a nivel global. Los usuarios externos comenzaron a recibir información corrupta o nula, lo que generó desconfianza y reportes masivos.

Solución:
Se decidió contactar a las autoridades competentes en delitos informáticos, además de consultar con la mesa directiva de la empresa. Se discutieron los posibles escenarios de respuesta, considerando que pagar el rescate no era una opción viable, ya que no garantiza la recuperación del sistema ni evita futuros ataques.

Paso 2: ¿Qué evidencias encontramos en los logs del sistema?

Recolección:
Se accedió a los logs de seguridad del servidor donde se detectaron los primeros accesos no autorizados desde la cuenta comprometida. Además, se revisaron los logs del sistema de base de datos, donde se encontró un aumento inusual de consultas erróneas e intentos de acceso simultáneo desde distintas ubicaciones.

También se analizaron los registros del servidor de correo y terminales de los usuarios, aunque no se detectó actividad sospechosa desde allí, lo que descartó el vector de phishing.

Análisis:
El análisis de logs reveló un patrón: tras la ejecución del troyano, el sistema intentó ejecutar procesos de cifrado en directorios compartidos. También se detectaron conexiones con direcciones IP externas desconocidas, lo que sugiere exfiltración o comando y control (C2).

Se utilizaron herramientas como **Splunk** para visualizar los patrones y **Wireshark** para inspección de tráfico en red.

Paso 3: ¿Qué sistemas fueron comprometidos?

Identificación:
Fueron comprometidos los servidores de base de datos principal, algunos escritorios de usuarios con acceso administrativo, y el sistema web de consulta. Se identificó que el ransomware se propagó a través de unidades compartidas internas y servicios que no contaban con autenticación multifactorial.

Evaluación del Impacto:

- **Disponibilidad:** El servicio de consultas estuvo fuera de línea por más de 12 horas.
- **Integridad:** Hubo manipulación de datos visibles en los formularios web.
- **Confidencialidad:** No se confirmó la extracción de datos, pero no se descarta el riesgo.

Paso 4: ¿Qué hicimos para contener y recuperarnos del incidente?

Medidas Inmediatas:

- Se desconectaron de inmediato los equipos afectados de la red.
- Se procedió a cambiar las credenciales de todos los usuarios con privilegios elevados.
- Se instalaron parches de seguridad y se actualizó el antivirus empresarial.

Plan de Recuperación:

- Se restauraron los servicios desde respaldos automáticos de la nube (último backup sin comprometer).
- Se habilitó un monitoreo continuo con alertas en tiempo real.
- Se realizó una auditoría de seguridad post-incidente para evaluar el nivel de madurez frente a ciberataques.

Comunicación:
Se elaboró un comunicado interno a todos los empleados y otro externo a los clientes, explicando la situación de forma transparente y detallando las medidas que se estaban tomando para garantizar la seguridad de la información. Cabe destacar que esto afecto

mucho la reputación y la percepción de confianza de los clientes sobre nuestros servicios, lo cual fue una de las afectaciones mas importantes.