Investigación de un

PRÁCTICA 1.2

HECHO POR:
IZAN NAVARRO LUJÁN

INDICE

INTRODUCTION

En la era digital, los ciberataques se han convertido en una de las mayores amenazas para la seguridad de la información. Con el aumento de la dependencia en infraestructuras digitales y redes globales, los cibercriminales utilizan técnicas cada vez más sofisticadas para comprometer sistemas, robar datos o interrumpir servicios esenciales. Estos incidentes no solo afectan a grandes corporaciones, sino también a individuos, gobiernos y pequeñas empresas, poniendo en riesgo la privacidad, la economía y la estabilidad global.

El propósito de esta práctica es investigar un ciberataque reciente real para comprender mejor las tácticas, técnicas y procedimientos empleados por los atacantes, así como las vulnerabilidades explotadas. A través de este análisis, se pretende reflexionar sobre la importancia de las medidas de ciberseguridad y las estrategias de mitigación que pueden adoptarse para prevenir futuros incidentes.

EJERCICIO:

1. **Reconocer y retratar un reciente ciberataque significativo, explicando sus atributos, extensión y repercusiones para la entidad o dominio dañado.**

En mayo del 2021, el **Health Service Executive** (HSE) de Irlanda fue impactada por un ciberataque de ransomware (malware que rapta archivos o sistemas) orquestado por el grupo Conti. Este asalto daño gravemente los sistemas informáticos del HSE, impactando la accesibilidad y secrecía de los datos médicos y administrativos. El ataque ocasionó la desconexión de sistemas cruciales, inclusive aquellos de citas médicas, diagnósticos y laboratorios, conllevando a la masiva suspensión de consultas y retrasos en los tratamientos de pacientes, fundamentalmente aquellos con enfermedades serias como el cáncer.

2. **Examinar las debilidades explotadas durante el ataque, al igual que los instrumentos y tácticas empleadas por los atacantes.**

El grupo Conti usó técnicas complejas para infiltrarse en la red del HSE, entre ellas:

· Phishing dirigido: Envío de correos electrónicos falsos para obtener credenciales de acceso.

· Explotación de debilidades ya conocidas: Utilización de fallos de seguridad en sistemas obsoletos.

· Despliegue de ransomware: Empleo de malware para cifrar datos y exigir un rescate. Extracción de datos: Un robo de info sensible, sucediendo antes del cifrado.

· Dichas técnicas le dieron a los atacantes el control de los sistemas comprometidos y extorsionaron a la organización dañada.

3. **Valorar el impacto del ataque en aspectos economicos, operativos y de reputación, para la organización y las victimas.**

Económico: El gobierno irlandés no pagó el rescate, sin embargo, el costo del ataque fue importante, implicando gastos en la recuperación de sistemas, auditorías y medidas de mitigación.

Operativo: La interrupción de servicios médicos esenciales, perjudicó la atención del paciente, cancelando consultas y retrasando tratamientos cruciales.

Reputacional: La confianza pública en el sistema de salud disminuyó, afectando la percepción de seguridad y eficiencia del HSE.

4. **Analizar las medidas de respuesta y recuperación puestas en marcha por la organización atacada, y evaluar su eficiencia.**

HSE aplicó diversas acciones para paliar el impacto del ataque:

·Desconexión de los sistemas comprometidos: Para detener la propagación del malware.

·Restauración desde copias de seguridad: Recuperación de datos y sistemas afectados. Trabajando codo a codo con agencias de ciberseguridad: Nos juntamos con el Centro Nacional de Ciberseguridad de Irlanda y otros pa la analizar y parar la amenaza.

·Analizando y reforzando la seguridad: Revisamos las políticas y acciones de ciberseguridad para evitar problemillas.

Aunque algunos sistemas no funcionaron por un tiempo, las medidas nos ayudaron a recuperar los servicios poco a poco.

5. Reflexionar sobre las lecciones aprendidas a partir de este ataque y proponer recomendaciones para mejorar las defensas cibernéticas de organizaciones similares en el futuro.

Aquí lo que aprendimos de este ataque:

· Es importante actualizar los sistemas y poner parches de seguridad a tiempo, o no?

· Hay que hacer copias de seguridad siempre, y guardarlas bien protegidas.

· Siempre capacitar al personal, especialmente en saber si un correo es falso o no, ya ve.

· Colaborar de cerca con agencias y organizaciones, compartiendo información y las mejores formas de hacer las cosas.

Recomendaciones adicionales:

·Establecer medidas de acceso seguras, como la autenticación multifactor.

Hacer simulacros de cómo reaccionar ante incidentes, para estar listos cuando algo pase, jeje.

Establecer un plan comunicación diáfano, para informar pacientes y público si hay bretes de seguridad.

Promover inversión en tecnologías ciberseguridad hechas a la medida, pal sector sanitario.

6. **Comparar con otros ataques que acaban de ocurrir, buscando patrones y tendencias comunes en el escenario de amenazas actual, eso es clave.**

El ataque al HSE guarda similitudes con otros incidentes recientes en el sector, como lo del Hospital Clínic de Barcelona en 2023, vaya.

En ambos percances, usaron vulnerabilidades en sistemas viejos, echaron ransomware pa cifrar datos y sacaron mucha información delicada. Estos sucesos resaltan la tendencia de los cibercriminales a atacar infraestructuras críticas, más en salud, por el valor de la información y la prisa de los servicios.

7. Conclusión.

El ataque al sistema salud irlandés, destaca la urgencia de blindar las defensas cibernéticas en salud, sí señor. Implantar medidas preventivas, entrenar al personal y la colaboración entre instituciones, son esenciales para reducir riesgos y mantener servicios.