Pentesting Technical Report

4Geeks
Ph: +1 786 345 5555

0. Índice

1. Introducción

El principal objetivo de esta práctica sería crear un plan de respuesta(identificar,proteger,detener,responder,recuperar y mejorar) ante un ataque ransomware que ha sufrido una empresa ficticia.

2. Identificación

Un usuario de la empresa recibió un correo de phishing, que contenía un archivo adjunto malicioso y se hacía pasar por ser una factura,esto hizo que el empleado lo descargara, permitiendo al atacante instalar el ransomware, lo que supuso que se propagara el ransomware por todos los equipos a través de la red y encriptar archivos y encontrándose así un mensaje en el que se exige 50 Bitcoins para el rescate de los datos.

3. Protección

Para una mejor protección en un futuro, lo mejor sería:

1. Segmentar la red: con ello haremos que si atacan una parte de la empresa,el virus solo se pueda expandir por una parte de la red y no a toda la empresa.
2. Realizar copias de seguridad: al realizar copias de seguridad, prevenimos que en caso de ataque,podamos volver al punto de partida antes de que se iniciara este ataque,es decir, no se perdería información.
3. Monitorear la red: usando un EDR o un SIEM podríamos advertir en tiempo real de lo que se está descargando es un virus o no.
4. Gestión de privilegios: decidir qué usuarios tienen privilegios para realizar una tarea sería otra manera de protegernos,porque así una persona que necesite descargar algo, no pueda sino lo ordena el supervisor,o usuario administrador.

4. Detección

Para una mejor detección en un futuro, lo mejor sería:

1. Sistemas de monitoreo: implementar un IDS/IPS para advertir al usuario en tiempo real.

2. Usar un firewall o un WAF: al usar un WAF como podría ser Wazuh o usar un firewall,prevenimos ataques porque monitoreamos la red y podemos observar que queremos que entre y que no queremos que entre a nuestra red.
3. Filtrado y clasificación de correos: usar filtros avanzados para identificar el phishing y marcarlos como spam.

5. Respuesta

Para una mejor respuesta después de recibir un ataque, lo mejor es:

1. Aislar los equipos infectados de la red: así evitaremos que el ransomware se propague por toda la empresa.
2. Notificar al equipo de IT: ellos nos indicarán de una mejor manera y de forma ordenada que debemos de hacer.
3. No pagar el rescate: es lo recomendable ya que normalmente después del pago no se devuelven los datos robados.

6. Recuperación

Una vez se termina el ataque,debemos de volver a la “normalidad”, para ello deberemos de ser lo más cautos posible:

1. Limpiar y reinstalar los sistemas afectados.
2. Restaurar datos de copias de seguridad.
3. Verificar que no queda rastro ni existen “backdoors”
4. Probar la funcionalidad de los sistemas una vez restaurados
5. Reincorporar los sistemas a la red de forma gradual
6. Supervisar la red para prevenir anomalías o nuevos posibles ataques.

7. Mejora continua

Una vez ya hemos sido atacados, lo mejor que nos queda es aprender en la medida de lo posible para que no vuelva a ocurrir un incidente como este:

1. Realizar un informe post-incidente,con análisis ,causas y lecciones aprendidas.
2. Actualizar las políticas de privacidad de la empresa.
3. Mejorar controles de acceso y filtrado de correos.
4. Formar a los empleados y hacer pequeños simulacros para tenerlos preparados para incidentes.

5. Evaluar la eficacia del plan de respuesta y revisarlo

8. Conclusión

La empresa ficticia TechCorp Inc., que ha sufrido un ataque de ransomware mediante un correo de phishing, reconoce la importancia de contar con un plan de respuesta sólido basado en el marco NIST. Este plan establece las pautas necesarias para prevenir, detectar y mitigar futuros incidentes de seguridad. Gracias a las medidas adoptadas y a las lecciones aprendidas de este incidente, la organización estará mejor preparada para proteger sus activos críticos y garantizar la continuidad de sus operaciones.