ERIC GROSSERMANN
Digital Forensics Examiner

Plan de Respuesta a Incidente de Ransomware basado en NIST

4Geeks Academy

Estudiante: Eric Grossermann
Fecha De Entrega: 12/17/25

Identificación
Mediante el analisis de respuesta de incidentes , se Identifico que ese momento la red no contaba con una segmentación adecuada, no había un protocolo de alerta temprana ni sistemas de monitoreo en tiempo real dando como resultado los siguientes activos críticos de la compania TechCo que han sido comprometidos por el ataque en cuestion, la cual se clasifica de la siguiente manera:

Servidor de archivos	Afecta operaciones diarias, trabajo interno
Base de datos de clientes	Riesgo legal, reputacional, financiero
Backups	Ultima linea de defensa
Red interna	Permite propagacion lateral
Usuarios	Punto inicial del ataque

Que activos son indispensables para que TechCo opere?
los activos indispensable para que operen principalmente son los servicios en la nube y gestionar datos, al recibir un ataque deja expuesto la disponibilidad del servicio y un riego a su economia.

Que pasa si ese activo deja de funcionar?
La empresa puede experimentar , perdidas economicas y falta de seguridad de los clientes al estar expuesto sus datos y disponibilidad de sus servicios.

Que activo fue el objetivo principal del atacante?
La **base de datos de clientes,** por que contiene datos sensibles de los clientes que no deben ser manipulados por personas externas, y contienen un valor economico lo cual sirve como presion para secuestrar los datos y exigir un rescate.

Los servicios en la nube dependen de la red interna y de la base de datos de clientes para funcionar. El servidor de archivos tambien depende de la red y de los permisos de acceso como los backups que estaban dentro de la misma red, lo cual dio pie a que el ransomware se propagara y cifrara tanto los datos de produccion como los de respaldo, provocando un fallo en cadena y haciendo que la recuperacion de los datos fuera mucho mas dificil.

Protección y Detección
TechCo podria haber detectado el ataque de ransomware en fases tempranas mediante la implementacion de un sistema de monitoreo y analisis de logs centralizado (SIEM), el cual habria permitido identificar actividades anomalas como la ejecucion de procesos sospechosos, cifrado masivo de archivos y accesos inusuales a sistemas criticos.

Herramientas como Wazuh habrian facilitado la correlacion de eventos y la generacion de alertas tempranas en fase 1.

Adicionalmente, la capacitacion del personal en identificacion de correos de phishing habria funcionado como un mecanismo de deteccion temprana, permitiendo reportar el incidente antes de que el ransomware se propagara.

Por ultimo, el uso de controles de accesos y privilegios limitados, habria permitido detectar intentos de escalacion de privilegios, los cuales suelen ser indicadores tempranos de compromiso.

Respuesta y Recuperación
Al detectar un ataque de ransomware, la prioridad es contener el incidente para evitar su propagacion, aislando los sistemas comprometidos y limitando acceso. Las decisiones deben ser tomadas por un equipo multidisciplinario que incluya personal tecnicos, gerenciales y legales.
Asimismo, es fundamental evitar acciones impulsivas como el pago Inmediato del rescate, la eliminacion de evidencia o la comunicaion descontrolada, ya que estas pueden agravar el impacto del incidentes y romper la confidencialidad ,la integridad y la disponibilidad de la compania.

En Este Caso Si la deteccion falla y el ransomware compromete tanto los sistemas de produccion y los backups, la organizacion se enfrenta a un escenario critico con opciones limitadas. En este contexto, una reconstrucción completa de los sistemas desde cero puede ser necesaria para garantizar la eliminacion total de la amenaza y restaurar la confianza en la infrestructura.

Esta desicion implica asumir un Impacto economico significativo y posibles perdidas de informacion, ademas de riesgos reputacionales y legales relacionados con la exposicion de los datos de clientes, lo que refuerza la importancia de contar con mecanismo de deteccion temprana efectivos.

La recuperacion se basa en restaurar unicamente desde fuentes confiables, priorizando los sistemas criticos para el negocio. Antes de reanudar operaciones normales, los sistemas deben ser validados para asegurar que esten libres de malware. Durantes este proceso, la

organizacion debe apoyarse en planes de continuidad del negocio que permitan seguir operando de forma limitada mientras se completa la recuperacion total.

Finalmente, para una respuesta efectiva, es fundamental definir y documentar los pasos que el equipo debe seguir una vez detectado el incidente, asignando roles y responsabilidades claras, así como estableciendo lineamientos de comunicación interna y externa.

Mejora continua →
Como parte de la mejora continua, TechCo debe implementar medidas orientadas a fortalecer su postura de seguridad y prevenir incidentes similares en el futuro. Entre estas medidas se incluyen la mejora de los mecanismo de deteccion temprana, la segmentacion de la red, el aislamiento de los sistemas de respaldo, la capacitación constante del personal y la aplicacion de controles de acceso mas estrictos.

Las lecciones aprendidas del incidentes permiten identificar que la falta de visibilidad, preparacion y segmentacion aumento significativamente el impacto del atacante. Por ellos, la integracion de estas lecciones en el plan de respuesta y la realizacion de simulacros periodicos permitiran a la organizacion estar mejor preparada antes futuras amenazas.

GROSSERMANN
PENTESTER
CYBER SECURITY