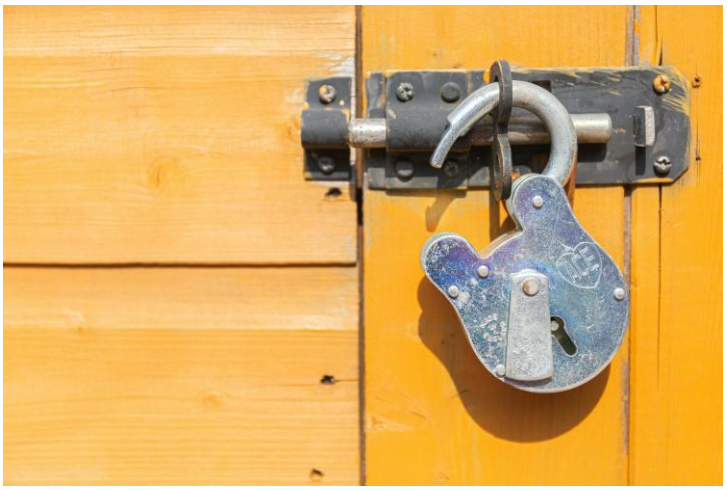
Plan de Respuesta a Incidente de Ransomware

Caso de Estudio: TechCo



NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Autor: Gustavo Rodil
Academia: 4Geeks Academy
Fecha: Septiembre 2025

Índice

1. Introducción

TechCo es una empresa ficticia dedicada a los servicios en la nube y a la gestión de datos confidenciales de clientes. Fue víctima de un ataque de ransomware a través de un correo de phishing, lo que permitió a los atacantes cifrar datos críticos y pedir un rescate millonario.

El objetivo de este informe es aplicar el marco NIST Cybersecurity Framework para elaborar un Plan de Respuesta a Incidentes, que permita identificar qué salió mal y proponer medidas de protección, detección, respuesta y recuperación.

2. Identificación

Activos críticos afectados:
- Servidor de archivos con documentos importantes.
- Base de datos de clientes con información sensible.
- Sistemas de copias de seguridad internos (también cifrados).

Vulnerabilidades detectadas:
- Red sin segmentación (todo estaba conectado en la misma red).
- Copias de seguridad almacenadas en el mismo entorno comprometido.
- No había un sistema de monitoreo en tiempo real.
- Falta de formación en los empleados (el phishing fue exitoso).

3. Protección

Medidas que habrían ayudado a evitar el ataque:
- Segmentación de red: separar producción, backups y usuarios.
- Copias de seguridad externas (por ejemplo, en discos duros desconectados o en la nube).
- Uso de antivirus y actualizaciones regulares para reducir vulnerabilidades.
- Capacitación básica en ciberseguridad: enseñar a los empleados a reconocer correos sospechosos.
- Gestión de accesos: dar a cada usuario solo los permisos que necesita.

4. Detección

Formas sencillas de haber detectado el ataque más rápido:
- Antivirus con alertas sobre archivos sospechosos.
- Sistemas de monitoreo que avisen si hay actividad rara, como muchos archivos cifrándose de golpe.
- Revisión periódica de logs del sistema.
- Pruebas internas (simulaciones de ataque) para comprobar si el personal detecta señales de phishing.

5. Respuesta

Pasos a seguir después de detectar el ataque:
1. Contener el ataque: aislar las máquinas infectadas y desconectarlas de la red.
2. Informar a la dirección y al equipo de TI para coordinar acciones.
3. Guardar evidencias para investigar después cómo ocurrió el ataque.
4. Comunicación interna y externa: explicar a los empleados la situación y, si es necesario, informar a los clientes de forma clara y honesta.
5. No pagar el rescate, ya que no hay garantía de recuperar los archivos.

Roles básicos:
- IT: contener y reparar sistemas.
- Gerencia: tomar decisiones y coordinar.
- Comunicación: informar a empleados y clientes.

6. Recuperación

Pasos para volver a la normalidad:
- Restaurar los datos desde copias de seguridad seguras (offline o en la nube).
- Reinstalar sistemas desde versiones limpias.
- Cambiar todas las contraseñas y reforzar la seguridad.
- Validar que los datos restaurados no estén corruptos.
- Mantener un plan de continuidad para que la empresa pueda seguir trabajando aunque algunos sistemas estén fuera de servicio temporalmente.

7. Mejora Continua

Después del incidente, TechCo debería:
- Revisar el incidente y aprender de los errores.
- Actualizar el plan de respuesta y repetirlo en simulacros.
- Medir indicadores básicos como: tiempo en detectar el ataque, tiempo en responder y tiempo en recuperar los sistemas.
- Seguir capacitando a los empleados para que sean la primera línea de defensa.

8. Conclusión

El ataque de ransomware contra TechCo mostró la importancia de estar preparados. La falta de segmentación de red, backups seguros y capacitación fueron claves en el éxito del ataque.

Con la implementación de un Plan de Respuesta alineado con el NIST, la empresa puede:
- Reducir el impacto de ataques futuros.
- Mejorar su capacidad de recuperación.
- Proteger mejor los datos de sus clientes.
- Reforzar la confianza y la continuidad de su negocio.

Como estudiante, este ejercicio me permitió comprender que la prevención y la educación del personal son tan importantes como las herramientas técnicas.