Plan de Respuesta a Incidente de Ransomware: Caso TechCo

Basado en el Marco de Ciberseguridad NIST

Autor: Samuel Fecha: 22-01-2026

Contexto: Respuesta ante incidente crítico de Ransomware con compromiso total de datos y backups.

1. Resumen del Incidente (Executive Summary)

TechCo ha sufrido un ataque de ransomware devastador originado por un correo de phishing. El malware cifró servidores de archivos, bases de datos de clientes y, críticamente, los sistemas de copias de seguridad. Los atacantes exigen 50 BTC bajo amenaza de destrucción de datos. La falta de segmentación de red y monitoreo permitió la propagación lateral rápida sin detección.

2. Identificación (Identify)

Objetivo: Desarrollar la comprensión organizacional para gestionar el riesgo de ciberseguridad para sistemas, activos, datos y capacidades.

En esta fase, analizamos qué tenemos y qué falló en el inventario de TechCo.

2.1 Activos Críticos Afectados

Identificamos los activos que son vitales para la operación y que fueron comprometidos:

Servidor de Archivos Corporativo: Contiene la propiedad intelectual y operativa diaria. (Impacto: Alto - Parada operativa).

Base de Datos de Clientes (CRM/DB): Contiene PII (Información de Identificación Personal) y datos financieros. (Impacto: Crítico - Riesgo legal y reputacional).

Sistemas de Backup: Infraestructura de respaldo conectada a la red principal. (Impacto: Catastrófico - Impide la recuperación inmediata).

Endpoints (Estaciones de trabajo): El equipo del "Paciente Cero" (empleado que abrió el correo) y otros equipos infectados por movimiento lateral.

2.2 Vulnerabilidades Explotadas

Factor Humano: Falta de concientización sobre ingeniería social (Phishing).

Arquitectura de Red Plana: Falta de segmentación de red. Una vez dentro, el atacante tuvo acceso libre al servidor de archivos y backups.

Gestión de Backups Deficiente: Los backups no eran inmutables ni estaban aislados.

3. Protección (Protect)

Objetivo: Desarrollar e implementar las salvaguardas apropiadas para asegurar la entrega de servicios críticos.

Definimos qué controles debieron existir y cuáles se implementarán para evitar recurrencia.

3.1 Medidas Preventivas (Gap Analysis)

Segmentación de Red (VLANs): Separar la red de empleados, la red de servidores críticos y la red de gestión de backups. Si un empleado cae, el servidor no debería ser alcanzable directamente.

Principio de Menor Privilegio: Los usuarios estándar no deben tener permisos de escritura en carpetas críticas del sistema ni acceso administrativo local.

Estrategia de Backup 3-2-1:

- 3 copias de los datos.
- 2 medios diferentes.
- 1 copia fuera de sitio/offline (Inmutable). Esta medida habría salvado a TechCo.

Capacitación y Concientización: Simulaciones de phishing mensuales para educar al personal sobre no descargar adjuntos sospechosos ("facturas.exe" o macros de Office).

Filtrado de Correo Electrónico: Implementación de soluciones anti-spam y sandboxing para adjuntos de correo.

4. Detección (Detect)

Objetivo: Desarrollar e implementar las actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad.

TechCo detectó el ataque "cuando los archivos no abrían". Eso es demasiado tarde. Proponemos detección temprana:

4.1 Herramientas y Protocolos de Detección

EDR (Endpoint Detection and Response): Instalación de agentes en cada ordenador capaces de detectar comportamientos anómalos (ej. cifrado masivo de archivos en segundos) y bloquear el proceso automáticamente.

SIEM (Security Information and Event Management): Centralización de logs. Habría alertado sobre intentos de conexión inusuales o escala**da de privilegios tras la infección inicial.**

IDS/IPS (Sistemas de Detección de Intrusos): Para detectar tráfico de "Comando y Control" (C2) cuando el malware intenta comunicarse con los atacantes.

Honeytokens (Archivos Cebo): Archivos falsos en la red que, si son accedidos o modificados, disparan una alarma silenciosa inmediata.

5. Respuesta (Respond)

Objetivo: Desarrollar e implementar las actividades apropiadas para tomar medidas respecto a un incidente detectado.

5.1 Plan de Acción Inmediata

Aislamiento (Contención): Desconectar inmediatamente los equipos infectados de la red (cable e inhabilitar Wi-Fi). NO APAGAR los equipos (para preservar pruebas en la memoria RAM para análisis forense), a menos que el cifrado esté ocurriendo activamente en pantalla.

Evaluación del Alcance: Determinar qué segmentos de red están limpios y cuáles comprometidos.

Activación del Equipo de Respuesta (CSIRT):

- **Líder de Incidente (CISO)**: Toma decisiones estratégicas.
- **Técnico Lead:** Encargado de contención y análisis de malware.
- **Legal:** Evalúa implicaciones de protección de datos (GDPR/RGPD) y notificaciones obligatorias.
- **Comunicaciones (PR):** Gestiona la comunicación con clientes (transparencia controlada).

5.2 Estrategia frente al Rescate

Política: NO PAGAR el rescate.

Razón: No garantiza la recuperación de datos, financia el crimen y marca a TechCo como "pagador" para futuros ataques.

Comunicación Externa: Notificar a las autoridades competentes (Policía Cibernética / Agencia de Protección de Datos) dentro de las primeras 72 horas si hay datos personales comprometidos.

6. Recuperación (Recover)

Objetivo: Desarrollar e implementar las actividades apropiadas para mantener planes de resiliencia y restaurar capacidades.

Dado que los backups online están cifrados, la recuperación es compleja, pero el plan debe establecer:

6.1 Pasos para la Restauración

- **Limpieza**: Formateo a bajo nivel de todos los discos afectados. Reinstalación de sistemas operativos desde "Golden Images" (imágenes limpias y verificadas).
- **Recuperación de Datos (Escenario TechCo):**
- Intentar localizar copias "Shadow Volume" (si el ransomware no las borró).
- Buscar copias offline antiguas aunque tengan pérdida de datos reciente.
- Si no existen copias offline: Evaluación de impacto de pérdida total.
- **Hardening (Endurecimiento):** Antes de reconectar a internet, aplicar todos los parches de seguridad y cambiar todas las contraseñas administrativas.
- **Reanudación Escalonada**: Levantar primero servicios críticos (Base de datos) y luego servicios secundarios.

6.2 Continuidad del Negocio (BCP)

Mientras los sistemas se reconstruyen, activar procesos manuales o uso de servicios en la nube alternativos para mantener la operación mínima con los clientes.

7. Mejora Continua (Lessons Learned)

Objetivo: Aprender del incidente para mejorar la postura de seguridad.

Una vez superada la crisis, se debe realizar una reunión "Post-Mortem" o "Hot Wash":

7.1 Evaluación de Eficacia

Análisis de Causa Raíz (RCA): ¿Cómo entró exactamente el phishing? ¿Por qué el filtro no lo paró?

Métricas de Tiempo: Analizar el MTTD (Mean Time to Detect - Tiempo medio de detección) y MTTR (Mean Time to Respond - Tiempo medio de respuesta). El objetivo es reducirlos drásticamente.

Actualización del Plan: Incorporar el fallo de los backups en la nueva política. Implementar Copias Inmutables obligatorias desde hoy.

Auditoría Externa: Contratar un servicio de Pentesting para validar que las nuevas medidas de segmentación son efectivas.