Plan de Respuesta a Incidente de Ransomware

Basado en el NIST Cybersecurity Framework (CSF)

Caso de estudio: TechCo

Hecho por Mario Villalobos Rodríguez para 4Geeks Academy

Introducción

El presente informe desarrolla un plan completo y estructurado de respuesta a incidentes de ransomware alineado con el NIST Cybersecurity Framework (CSF). A partir del caso de estudio de la empresa ficticia TechCo, se definen medidas preventivas, mecanismos de detección, procedimientos de respuesta, estrategias de recuperación y un enfoque de mejora continua que permita reducir el impacto de incidentes futuros y reforzar la resiliencia organizativa.

1. IDENTIFICACIÓN (IDENTIFY)

La fase de identificación tiene como objetivo comprender el contexto operativo de TechCo, los activos críticos y los riesgos asociados. Los activos más relevantes incluyen los servidores de archivos corporativos, las bases de datos de clientes con información sensible, los sistemas de respaldo, la infraestructura de red y los usuarios finales. El incidente tuvo su origen en un ataque de phishing, evidenciando vulnerabilidades técnicas y organizativas, especialmente la falta de segmentación de red y de controles de concienciación del personal.

2. PROTECCIÓN (PROTECT)

Para prevenir ataques de ransomware y limitar su propagación, TechCo debería implementar un conjunto de medidas preventivas basadas en el principio de defensa en profundidad. Estas medidas incluyen la segmentación de la red mediante VLANs y firewalls internos, la aplicación del principio de mínimo privilegio, el uso de autenticación multifactor y la implantación de copias de seguridad inmutables y desconectadas de la red principal.

Desde el punto de vista organizativo, la adopción de políticas de seguridad de la información, políticas de gestión de accesos, políticas de backup y planes formales de respuesta a incidentes habría reducido significativamente el impacto del ataque. Asimismo, la formación periódica en detección de phishing y concienciación en ciberseguridad podría haber evitado el vector inicial del incidente.

3. DETECCIÓN (DETECT)

La detección temprana de un ataque de ransomware es clave para minimizar su alcance. TechCo podría haber utilizado soluciones SIEM para la correlación de eventos de seguridad, junto con herramientas EDR/XDR capaces de detectar comportamientos anómalos en los endpoints.

La implantación de un protocolo de alerta temprana habría permitido identificar indicadores de compromiso, como el cifrado masivo de archivos, picos inusuales de uso de CPU o accesos no autorizados. Dicho protocolo debería incluir alertas automáticas, escalado inmediato al equipo de seguridad y procedimientos claros de verificación del incidente.

4. RESPUESTA (RESPOND)

Una vez detectado el incidente, TechCo debe activar su plan de respuesta a incidentes. El primer paso consiste en la contención inmediata del ataque mediante el aislamiento de los sistemas afectados y la desconexión de los

equipos comprometidos de la red.

Posteriormente, el equipo de seguridad debe realizar un análisis forense para determinar el alcance del ataque, identificar el tipo de ransomware y preservar evidencias. La comunicación debe gestionarse de forma coordinada, informando a la dirección, al equipo legal y, si procede, a clientes y autoridades.

Rol	Responsabilidad
Equipo IT	Contención técnica y restauración de sistemas
Responsable de Seguridad	Coordinación del incidente
Dirección	Toma de decisiones estratégicas
Legal	Cumplimiento normativo y notificaciones
Comunicación	Gestión de la comunicación interna y externa

5. RECUPERACIÓN (RECOVER)

La fase de recuperación tiene como objetivo restaurar los sistemas y datos afectados de forma segura. TechCo debe reinstalar los sistemas desde entornos limpios, restaurar la información desde copias de seguridad verificadas y validar la integridad de los datos antes de devolverlos a producción.

Durante el proceso de recuperación, se deben activar planes de continuidad del negocio que prioricen los servicios críticos y permitan mantener operaciones mínimas. Una vez completada la recuperación, es necesario revisar y fortalecer la arquitectura de seguridad para evitar incidentes similares en el futuro.

6. MEJORA CONTINUA (IMPROVE)

Para evaluar la eficacia del plan de respuesta, TechCo debe realizar un análisis post-incidente basado en métricas como el tiempo de detección, tiempo de contención, impacto operativo y efectividad de la comunicación. Este análisis debe documentarse y servir como base para la actualización del plan.

La mejora continua debe apoyarse en simulacros periódicos de ransomware, auditorías de seguridad y programas de formación continua, garantizando que el plan evoluciona junto con las amenazas y mantiene su alineación con el NIST Cybersecurity Framework.