

INFORME DE PLAN DE RESPUESTA A INCIDENTE DE RANSOMWARE

1. Identificación

En esta fase se analiza el alcance del incidente y el entorno de riesgo de TechCo. El objetivo será entender que tenemos y como de expuesto estaba.

Activos críticos afectados

- Servidor de Archivos: Crítico para la operatividad diaria ya que su pérdida paraliza la productividad.
- Base de datos de clientes: Es un activo de alto valor ya que contiene información de identificación personal y datos financieros. Su compromiso implica riesgos legales.
- Sistema de backup: Es un activo de recuperación. Al estar conectado a la red principal pasaron de ser una solución a parte del problema.

Análisis de vulnerabilidades:

- Factor humano: Falta de concienciación en seguridad por parte del personal
- Arquitectura de red simple: Falta de segmentación de red sin haber barreras entre estaciones de trabajo para aportar una seguridad minima.
- Gestión de backups deficiente: Los backups no eran inmutables ni estaban fuera de línea permitiendo que el ransomware los cifrara

2. Protección

Medidas preventivas recomendadas

- Segmentación de red: Al dividir la red en subredes, los usuarios generales no deben tener visibilidad directa a los servidores de backup o BBDD críticas.
- Estrategia de backups 3, 2, 1:
 - 3 copias de los datos
 - 2 medios diferentes
 - 1 copia fuera del sitio.
- Formación y concienciación: Campañas de simulación de phishing para entrar a los empleados y sean capaces de identificar correos sospechosos.
- Control de acceso: Los empleados no deben tener permisos de escritura en carpetas críticas del servidor.

3. Detección

Métodos y herramientas de detección

- EDR: Un EDR detecta comportamientos anómalos, como la encriptación masiva de archivos en poco tiempo.
- SIEM: Se utiliza para correlacionar logs.
- IDS/IPS: Se utiliza para monitorear el tráfico de red interno en busca de firmas de ransomware conocido.

4. Respuesta

Equipo de respuesta ante incidentes - roles

- Gerente: Toma las decisiones finales y coordina al equipo
- Analista técnico: Encargado de la contención técnica y análisis forense.
- Cumplimiento de normativas: Evalúa la notificación obligatoria a las autoridades
- Comunicación: Maneja la información hacia empleados y clientes para controlar.

Flujo de respuesta

- Detección y validación: Confirmaremos que el ransomware y no un fallo del sistema
- Contención:
 - aislamiento de la red
 - hibernar o suspender los equipos para preservar la memoria para el análisis forense
 - Bloquear en el firewall las IPS sospechosas y los puertos de comunicación hacia el exterior.
- Erradicación:
 - Identificar el principal pc afectado
 - Eliminar el malware de todos los sistemas afectados usando herramientas antimalware especializadas
 - Reforzar los filtros de correos
- Análisis: Determinar si hubo exfiltración de datos antes del cifrado

5. Recuperación

Plan de restauración

- Limpieza y reinstalación
- Recuperación de datos
- Verificación
- Reconexión gradual

Continuidad del negocio mientras los sistemas estan caidos:

- Activar el proceso manual para la atención al cliente
- Informar a los cliente sobre retrasos sin dar mucho detalle técnico

6. Mejora continua

Plan de acción

- Actualizar el plan de respuesta con tiempos reales obtenidos
- Implementar inmutabilidad en los backups como prioridad
- Contratar un servicio de SOC externo a TechCo no tuviese la capacidad