Introduccion

El presente informe detalla el Plan de Respuesta a Incidentes desarrollado para la empresa TechCo, tras el compromiso de su infraestructura crítica por un ataque de ransomware. El objetivo principal de este documento es proporcionar una estrategia estructurada y técnica que permita la gestión de la crisis actual y la mitigación de riesgos futuros.

Activos Críticos Afectados:

1. Servidor de Archivos: Motor operativo diario de la empresa.
2. Base de Datos de Clientes: Contiene información sensible (PII) y financiera; su compromiso implica riesgos legales (GDPR/LOPD) y reputacionales.
3. Sistemas de Backup: El activo más crítico para la recuperación, que falló al estar conectado a la red principal.
4. Estaciones de Trabajo: Puntos de entrada (endpoint) del malware.

Vulnerabilidades Identificadas

1. Falta de Concienciación: Factor humano vulnerable al phishing.
2. Arquitectura de Red Plana: Ausencia de segmentación que permitió el movimiento lateral del ransomware.
3. Backups Vulnerables: Almacenamiento de respaldos en la misma red de producción sin protección de inmutabilidad o "Air Gap".
4. Gobernanza Débil: Ausencia de un inventario de activos y de una estrategia de gestión de riesgos técnica.

Protección

Medidas Preventivas Propuestas:

- Gestión de Identidades y Accesos (IAM): Implementar Autenticación de Múltiple Factor (MFA) en todos los niveles y aplicar el Principio de Menor Privilegio, para que un empleado estándar no tenga permisos de escritura en servidores críticos.
- Segmentación de Red: Dividir la red en VLANs (Producción, Backups, Invitados, Administrativo) con firewalls internos para evitar que el ransomware se propague.
- Estrategia de Backup 3-2-1: Mantener 3 copias de seguridad, en 2 medios distintos, con 1 copia fuera de línea (offline) o inmutable (en la nube o cintas).
- Concienciación y Entrenamiento: Programa continuo de simulación de phishing para empleados.
- Protección de Datos: Cifrado de la base de datos de clientes en reposo.

Detección

Métodos y Herramientas:

- Implementación de EDR (Endpoint Detection and Response): Herramientas que detectan comportamientos anómalos (como el cifrado masivo de archivos) en las laptops y servidores en tiempo real.
- SIEM (Security Information and Event Management): Centralización de logs para identificar alertas tempranas (ej. múltiples intentos de acceso fallidos o tráfico hacia IPs maliciosas conocidas).
- Protocolo de Alerta Temprana: Configurar alarmas automáticas si se detecta la creación de archivos con extensiones conocidas de ransomware (ej: .locked, .crypto).
- Monitoreo de Integridad de Archivos (FIM): Alertar sobre cambios no autorizados en archivos críticos del servidor.

Respuesta

Plan de Acción Inmediato

- Aislamiento: Desconectar físicamente o mediante software los equipos infectados de la red para detener la propagación. No apagar los equipos (para preservar la memoria RAM para análisis forense).
- Análisis: Determinar la variante del ransomware (ej. LockBit, Conti) para verificar si existen herramientas de descifrado gratuitas.
- Contención: Bloquear los puertos y las cuentas comprometidas en el Directorio Activo.

Roles y Responsabilidades:

- Líder de Respuesta a Incidentes (CISO): Coordina la estrategia y toma decisiones críticas.
- Equipo Técnico (IT/Seguridad): Ejecuta el aislamiento, análisis forense y limpieza de sistemas.
- Departamento Legal: Evalúa la necesidad de notificar a las autoridades de protección de datos (por el robo de datos de clientes).
- Relaciones Públicas: Maneja la comunicación con clientes y prensa para mitigar daños reputacionales.

Comunicación:

- Interna: Informar a los empleados sobre la situación y prohibir el uso de equipos sospechosos.
- Externa: Seguir la política de "Transparencia Controlada". Notificar a clientes afectados solo cuando se tenga información veraz. Política de TechCo: No pagar el rescate (siguiendo recomendaciones del FBI/NIST).

Recuperación

Pasos para la Restauración:

- Saneamiento: Formatear y reinstalar sistemas operativos desde imágenes limpias (para asegurar que no queden "puertas traseras").
- Restauración de Datos: Recuperar la base de datos y archivos desde la copia de seguridad más reciente que sea íntegra y no esté cifrada.
- Validación: Probar los sistemas en un entorno aislado antes de volver a conectarlos a la red de producción.

Continuidad del Negocio:

- Habilitar sistemas temporales en la nube si la infraestructura física sigue comprometida.
- Priorizar la recuperación: 1º Base de Datos (Negocio), 2º Servidor de Archivos (Operación), 3º Resto de sistemas.

Mejora Continua

Método de Evaluación Post-Incidente:

- Reunión de "Lecciones Aprendidas": Analizar qué falló en la protección y por qué la detección fue lenta.
- Actualización del Plan: Modificar este plan de respuesta con base en la experiencia real del ataque.
- Pruebas de Estrés (Tabletop Exercises): Realizar simulacros semestrales de ransomware con la gerencia para asegurar que todos sepan cómo actuar.
- Auditoría Externa: Contratar una empresa de ciberseguridad para realizar un Pentesting (prueba de penetración) y verificar que las nuevas medidas de segmentación funcionan.

Conclusión

La implementación de este plan basado en el NIST Framework permitirá a TechCo no solo recuperarse del ataque actual, sino transformar su cultura organizacional hacia una de resiliencia cibernética, donde la seguridad no es un gasto, sino un pilar fundamental para la continuidad del negocio.