Informe de Respuesta ante Incidente:

TechCo bajo Ataque de Ransomware.

Marco de referencia: NIST Cybersecurity Framework

Empresa: TechCo

Tipo de incidente: Ataque de ransomware

Fecha del informe: 23/07/2025

Joel González.

1. Identificación de Activos Críticos y Vulnerabilidades

Activos Afectados y en Riesgo

- **Servidor de archivos:** Contiene documentos operativos esenciales.
- **Base de datos de clientes:** Almacena información personal y financiera.
- **Sistemas de backup internos:** Comprometidos por falta de segmentación.
- **Servidores de producción:** Infraestructura crítica para servicios en la nube.

Vulnerabilidades Detectadas

- **Falta de segmentación de red:** Permitió la propagación del ransomware.
- **Ausencia de autenticación multifactor (MFA):** Facilitó el acceso inicial mediante phishing.
- **Backups no aislados:** Al estar en la misma red, fueron cifrados.
- **Falta de capacitación en ciberseguridad:** Empleados no identificaron el correo malicioso.

2. Protección: Medidas Preventivas Necesarias

Controles de Seguridad Recomendados

- **Segmentación de red:** Dividir redes críticas (producción, backups, usuarios) para limitar propagación.
- **MFA obligatorio:** Evitar accesos no autorizados incluso con credenciales robadas.
- **Backups inmutables y fuera de línea (air-gapped):** Almacenar copias en ubicaciones físicamente separadas.
- **Política de ejecución de archivos:** Restringir la ejecución de macros y scripts no autorizados.
- **Simulaciones de phishing:** Capacitar empleados para identificar amenazas.

3. Detección: Herramientas y Protocolos de Alerta Temprana

Sistemas de Monitoreo Proactivo

- **SIEM (Splunk, IBM QRadar):** Analizar logs en tiempo real para detectar anomalías.
- **EDR (CrowdStrike, SentinelOne):** Identificar comportamientos sospechosos.
- **Honeypots:** Trampas para detectar movimiento lateral de atacantes.

Indicadores de Compromiso (IOCs) Clave

- **Actividad inusual en SMB/RDP:** Movimiento lateral del ransomware.
- **Conexiones a dominios maliciosos:** Detectables con DNS filtering (Cisco Umbrela).

4. Respuesta: Plan de Acción Inmediata

Fase 1: Contención

- **Aislar sistemas infectados:** Desconectar servidores afectados para evitar propagación.
- **Bloquear tráfico malicioso:** Reglas de firewall para cortar comunicaciones.

Fase 2: Erradicación

- **Eliminar ransomware:** Usar herramientas como Malwarebytes o reinstalar sistemas desde cero.
- **Rotar credenciales:** Cambiar todas las contraseñas y certificados.

Fase 3: Comunicación

- **Equipo interno:** Notificar al equipo legal y alta dirección.
- **Clientes afectados:** Informar bajo normativas de cumplimiento.
- **Autoridades:** Reportar a las autoridades competentes.

5. Recuperación: Restauración y Continuidad

Pasos Clave

1. **Restaurar desde backups limpios:** Priorizar datos críticos con verificación de integridad.
2. **Validar sistemas antes de reanudar operaciones:** Asegurar que no quedan backdoors.
3. **Plan de continuidad:** Operar con redundancia hasta recuperación total.

Lecciones Aprendidas

- **Pruebas regulares de restauración:** Asegurar que los backups funcionen.
- **Respuesta automatizada:** Implementar playbooks de respuesta.

6. Mejora Continua

Evaluación Post-Incidente

- **Ejercicios de simulación:** Simular ataques para probar el plan.
- **Auditorías trimestrales:** Revisar políticas de acceso y controles.

Actualización del Plan

- **Incorporar inteligencia de amenazas:** Monitorear TTPs (Tácticas, Técnicas y Procedimientos) de ransomware.
- **Automatización:** Integrar herramientas como Palo Alto Cortex para respuestas rápidas ante ante amenazas.

Conclusión

El ataque a TechCo evidenció fallos críticos en formación, protección, detección y respuesta. La implementación de medidas como segmentación de red, MFA y backups aislados, junto con un plan de respuesta formal, reducirá significativamente el riesgo futuro. La mejora continua y la capacitación son esenciales para mantener un entorno seguro.