Plan de Respuesta a Incidente de Ransomware

Caso: TechCo bajo ataque de ransomware

1. Identificación

- Activos críticos afectados:
- - Servidor de archivos → Documentos internos esenciales.
- - Base de datos de clientes → Información personal y financiera sensible.
- - Sistemas de respaldo → Backups cifrados por estar en la misma red.
- Vulnerabilidades detectadas:
- - Correo electrónico sin filtro antiphishing avanzado.
- - Falta de segmentación de red.
- - Backups no aislados.
- - Carencia de monitoreo en tiempo real.

2. Protección

- - Segmentación de red (aislar backups y producción).
- - Principio de mínimo privilegio.
- - Filtros antiphishing y sandboxing en correo.
- - Backups offline o en la nube inmutable.
- - Hardening en servidores (MFA, actualizaciones).
- - Capacitación en ciberseguridad.

3. Detección

- - EDR (Endpoint Detection & Response).
- - SIEM con alertas automáticas.
- - Monitor de tráfico anómalo.
- - Alertas de cifrado masivo.
- - Sensores honeypots internos.

4. Respuesta

- Plan inmediato:
- 1. Activación del Equipo de Respuesta a Incidentes (CSIRT).
- - Roles: líder del incidente, comunicaciones, infraestructura, legal, PR.
- 2. Contención inicial:
- - Desconectar hosts comprometidos.
- - Aislar segmentos de red.
- - Revocar credenciales comprometidas.
- 3. Erradicación:
- - Analizar vectores de ataque.
- - Eliminar binarios maliciosos.
- - Parchar vulnerabilidades explotadas.
- 4. Comunicación: interna, externa y legal.
- 5. Evaluación de alternativas: no pagar rescate, priorizar restauración.

5. Recuperación

- - Restaurar sistemas desde backups offline / nube.
- - Reconstrucción de infraestructura en entornos limpios.
- - Validación de integridad de datos.
- - Pruebas de continuidad del negocio.
- - Monitoreo reforzado post-incidente.

6. Mejora Continua

- - Post-mortem del incidente.
- - Simulacros regulares de ransomware.
- - KPIs de seguridad: MTTD, MTTR.
- - Actualización de políticas.
- - Cultura de seguridad continua.

Conclusión

- El caso de TechCo muestra que un ataque de ransomware puede paralizar una organización si no cuenta con segmentación, backups resilientes y monitoreo. Siguiendo el marco NIST, TechCo no solo puede contener y recuperarse, sino también evolucionar hacia un modelo de ciberseguridad más robusto.