Informe de Respuesta a Incidentes de Ransomware en TechCo

Índice

---

1. Identificación de Activos y Vulnerabilidades

Activos Críticos Afectados

Activo	Impacto
Servidor de archivos	Datos operacionales cifrados (documentos, contratos).
Base de datos	Información sensible de clientes (nombres, tarjetas de crédito) comprometida.
Backups internos	Copias de seguridad inaccesibles (cifradas por el ransomware).

Vulnerabilidades Clave

- Falta de segmentación de red: Los sistemas de producción y backups compartían la misma red.
- Ausencia de autenticación MFA: El phishing aprovechó credenciales débiles.
- Backups no aislados: No se seguía la regla 3-2-1 (3 copias, 2 medios, 1 fuera de la red).

---

2. Protección: Medidas Preventivas

Políticas y Controles Necesarios

- Segmentación de red:
  - Aislar redes críticas (ej.: VLAN para backups, DMZ para servicios expuestos).
- Protección contra phishing:
  - Implementar MFA en todos los accesos.
  - Entrenamiento obligatorio en concienciación (simulacros de phishing).
- Backups resilientes:
  - Almacenar copias offline/air-gapped y en la nube (ej.: AWS S3 con versionado).
- Hardening de sistemas:
  - Deshabilitar macros en Office.
  - Parchear vulnerabilidades conocidas (CVE-2023-1234).

---

3. Detección: Alertas Tempranas

Herramientas Recomendadas

Herramienta	Uso
SIEM (Splunk/Wazuh)	Monitoreo de anomalías (ej.: múltiples intentos de cifrado de archivos).
EDR (CrowdStrike)	Detección de procesos maliciosos en endpoints.
IDS/IPS (Snort)	Bloqueo de tráfico malicioso en la red.

Protocolo de Alerta Temprana

1. Umbrales de alerta: Notificar al SOC si:
   - Un usuario ejecuta un archivo .exe desde un correo.
   - Hay intentos masivos de modificación de archivos.
2. Respuesta automática: Aislar automáticamente equipos infectados.

---

4. Respuesta: Plan de Acción Inmediata

Pasos a Seguir

1. Contención:
   - Desconectar los sistemas infectados de la red.

    - Deshabilitar cuentas comprometidas.
2. Análisis forense:
    - Identificar la variante del ransomware (ej.: LockBit, REvil).
    - Determinar el punto de entrada (ej.: correo phishing).
3. Comunicación:
    - Interna: Notificar al equipo legal y alta dirección.
    - Externa: Reportar a autoridades (INCIBE, GDPR si hay fuga de datos).

Roles y Responsabilidades

Rol	Responsabilidad
SOC Team	Contención y análisis técnico.
Legal/Comunicación	Gestionar comunicación con clientes y prensa.
TI/Operaciones	Restaurar sistemas limpios.

---

5. Recuperación: Restauración de Sistemas

Plan de Recuperación

1. Eliminar el ransomware:
    - Usar herramientas como Bitdefender Rescue CD para limpiar sistemas.
2. Restaurar desde backups limpios:
    - Priorizar datos críticos (base de datos de clientes).
    - Validar integridad de los backups antes de la restauración.
3. Continuidad del negocio:
    - Operar en modo crítico con sistemas redundantes (ej.: servidores en la nube).

---

6. Mejora Continua: Lecciones Aprendidas

Evaluación Post-Incidente

- Simulacros trimestrales: Ejercicios de ransomware con escenarios realistas.
- Auditorías de seguridad: Revisar políticas cada 6 meses (ej.: NIST CSF).

Integración de Mejoras

- Automatización: Implementar playbooks de respuesta en el SIEM.
- Cultura de seguridad: Premiar a empleados que reporten phishing.

---

7. Conclusión

El ataque a TechCo subraya la importancia de:
✅ Prevención proactiva (segmentación, MFA, backups).
✅ Detección temprana (SIEM, EDR).
✅ Respuesta rápida (protocolos claros y equipos entrenados).
Recomendación final: Adoptar un marco de seguridad como MITRE ATT&CK para mapear amenazas y defensas.