Informe de Respuesta a Incidente de Ransomware en TechCo

1. Identificación

Activos Críticos Afectados:

- **Servidor de Archivos:** Contenía documentos operativos, informes contables, presentaciones internas, manuales técnicos y procedimientos críticos de negocio.

- **Base de Datos de Clientes:** Albergaba datos personales (nombre, dirección, correo, teléfono) y financieros (números de tarjeta, historial de pagos, contratos).

- **Sistemas de Backup Internos:** Incluían respaldos completos e incrementales de todos los servidores de producción. Los backups estaban almacenados en servidores conectados a la red principal, sin aislamiento lógico ni físico.

Vulnerabilidades Identificadas:

- Falta de segmentación de red que permitió el movimiento lateral del ransomware.

- Ausencia de filtros de contenido y análisis de comportamiento en el sistema de correo electrónico.

- Política de backups inadecuada: sin almacenamiento fuera de línea ni copias encriptadas fuera de la red interna.

- Falta de monitoreo centralizado de eventos de seguridad.

- Empleados no entrenados adecuadamente para detectar correos de phishing.

---

2. Protección

Medidas Preventivas Recomendadas:

- **Segmentación de Red:** Implementar VLANs para separar entornos de desarrollo, producción, respaldo y usuarios. Utilizar firewalls internos y listas de control de acceso (ACL).

- **Autenticación Multifactor (MFA):** Aplicar en todos los accesos remotos, paneles administrativos y aplicaciones sensibles.

- **Backups Resilientes:** Crear backups cifrados con firmas digitales, almacenados en medios offline y soluciones cloud con protección contra ransomware (WORM, versiones).

- **Concientización en Seguridad:** Campañas mensuales de capacitación, simulacros de phishing y boletines internos de ciberseguridad.

- **Actualizaciones y Parches:** Automatización de parches con validación previa en entornos de prueba.

---

3. Detección

Herramientas y Métodos Recomendados:

- **EDR (Endpoint Detection and Response):** Herramientas como SentinelOne o CrowdStrike para detectar actividades como cifrado masivo, creación de procesos anómalos o conexiones sospechosas.

- **SIEM (Security Information and Event Management):** Soluciones como Splunk, Graylog o QRadar para correlación de eventos y generación de alertas automáticas.

- **Sondas de Red (NDR):** Inspección de tráfico y detección de patrones anómalos.

- **Honeytokens:** Archivos falsos señuelo que activan alertas si son accedidos o cifrados.

- **Protocolos de Alerta Temprana:** Clasificación de eventos en niveles críticos, con alertas automáticas al CSIRT por email, SMS o dashboards.

---

4. Respuesta

Plan de Respuesta a Ransomware:

1. **Contención Inmediata:** - Aislar dispositivos infectados mediante herramientas de gestión remota. - Deshabilitar credenciales comprometidas.

2. **Notificación Interna:** - Activar plan IRP (Incident Response Plan). - Informar a todas las áreas operativas y de gestión.

3. **Investigación Técnica:** - Realizar análisis forense del archivo malicioso y vector de entrada. - Analizar registros del SIEM, firewall, endpoints y red.

4. **Comunicación Externa:** - Comunicar a clientes potencialmente afectados mediante email o canales oficiales. - Notificar a organismos reguladores como la Agencia Española de Protección de Datos (AEPD) si procede.

5. **Documentación y Reporte:** - Consolidar toda la información del incidente para auditoría y cumplimiento normativo.

Roles y Responsabilidades:

- **CSIRT:** Coordinación técnica de respuesta.

- **DPO:** Determina necesidad de reporte legal y análisis de impacto.

- **TI/Infraestructura:** Reinstalación y recuperación de sistemas.

- **Comunicación Corporativa:** Redacción de comunicados oficiales.

- **Alta Dirección:** Evaluación de decisiones legales, financieras y estratégicas.

---

5. Recuperación

Acciones para la Restauración:

- **Entornos Limpios:** Formatear sistemas comprometidos y reinstalar desde medios verificados.

- **Validación de Backups:** Asegurar la integridad mediante checksum y pruebas de restauración parciales.

- **Restauración Controlada:** Priorizar servicios críticos como bases de datos de clientes, portales web y correos corporativos.

- **Escaneo Post-Restauración:** Uso de herramientas antimalware y EDR para asegurar ausencia de persistencia del atacante.

Plan de Continuidad del Negocio (BCP):

- Activar servidores alternos en la nube si el entorno principal no está disponible. - Implementar soluciones SaaS temporales para funciones como correo, CRM y almacenamiento de documentos.

---

6. Mejora Continua

Post-Mortem:

- Reunión con todos los equipos implicados dentro de los 7 días posteriores al incidente. - Análisis de KPIs como tiempo de detección, contención y recuperación. - Identificación de procesos ineficientes o cuellos de botella.

Lecciones Aprendidas:

- Crear playbooks específicos para ransomware, phishing y exfiltración de datos.

- Simular incidentes reales cada trimestre para evaluar la preparación del equipo.

- Revisar y reforzar contratos con proveedores para asegurar SLA en ciberincidentes.

Conclusión: El ataque de ransomware a TechCo evidenció brechas significativas en protección, detección y respuesta ante incidentes. La implementación de un enfoque basado en el marco NIST, junto con un cambio cultural hacia la ciberresiliencia, será crucial para prevenir futuros eventos y reducir su impacto.