Plan de respuesta e incidente de ransomware

En este plan se ven los casos propuestos para la empresa TechCo

Identificacion

Se tiene que identificar qué fue lo que falló en el sistema. En este caso, tenemos que evaluar lo siguiente
Activos críticos afectados: La base de datos de los clientes, documentos operativos en el servidor de archivos, y el sistema de backups interno.
Vulnerabilidades explotadas: Se ve que el factor humano fue la vulnerabilidad explotada por los atacantes. Adicionalmente la red sin segmentación, los backups conectadas directamente a la red principal y los permisos de escritura para usuarios estándar en carpetas de la red

Proteccion

Para evitar que esto se repita se recomienda realizar lo siguiente:
Segmentar la red en zonas para que una estación de trabajo no conecte directamente con los servidores de backup.
Crear estrategias de backup fuera del sistema como tal (Fuera de sitio) y realizar al menos 3 copias de datos.
Implementar los principios de privilegios y autenticación de multifactor en todos los niveles.
Implementar filtros de correos avanzados, protocolos SPF y DMARC.

Deteccion

Para la detección de distintas áreas de la empresa podríamos mencionar las siguientes medidas:
Implementación de un EDR para detectar comportamientos anómalos en los dispositivos.
Implementar un SIEM para centralizar logs de servidores y firewalls.
Utilización de honeypots de archivos para ver cómo los atacantes pueden atacar nuestras vulnerabilidades y alertar en caso de que sea requerido.

Respuesta

Una vez detectado los incidentes, se debe tener los roles, responsables y pasos de respuesta para incidentes:

Rol	Responsabilidad Principal
CISO / Líder de Incidente	Toma de decisiones estratégicas y aprobación de recursos.
Equipo Técnico	Aislamiento de sistemas, análisis forense y eliminación del malware.
Legal / Cumplimiento	Gestión de notificaciones de brecha de datos según regulaciones.
Comunicación Corporativa	Gestión del mensaje a clientes y prensa.

Como pasos se seguirán los siguientes:

1. Aislar el problema desconectando físicamente o mediante software los servidores afectados de la red para evitar que se propague por el resto de la red. No se debe apagar el equipo para mantener la memoria RAM.
2. Analizar la variante de ransomware y buscar posibles descifrados públicos.
3. Contener el sistema bloqueando el dominio e IP identificados en el correo malicioso.

Recuperacion

Para restaurar la confianza y la operación mitigando las posibles amenazas se debe hacer lo siguiente:

- Se debe reinstalar los sistemas operativos afectados desde cero
- Se restaura de manera gradual la base de datos de los clientes y luego los servicios operativos.
- Se escanear los backups con antivirus actualizados antes de volverlos a colocar nuevamente al sistemas.
- Informar a los clientes sobre los plazos estimados y retorno a la normalidad.

Mejora Continua

Para una mejora continua se debe hacer lo siguiente:

- Reuniones de lecciones aprendidas sobre incidentes recientes
- Utilizar las métricas de eficacia propuesta versus las métricas usadas en la respuesta de incidentes para saber puntos de mejora
- Simulacros de mesa para practicar la toma de decisiones bajo presión
- El equipo de ciberseguridad debe implementar las medidas y las capacitaciones sobre campañas de phishing.