Referencia de sitio de consulta:

Arghire, I. (25 de septiembre de 2023). *City of Dallas Details Ransomware Attack Impact, Costs.* SecurityWeek Cybersecurity News, Insights & Analysis. Recuperado el 29 de septiembre de 2023 de https://www.securityweek.com/city-of-dallas-details-ransomware-attack-impact-costs/

¿Cuál fue la falla?

La falla de seguridad informática en el texto fue la intrusión no autorizada de un grupo de ciberdelincuentes llamado Royal en la red de la ciudad de Dallas. Tuvieron acceso no detectado durante aproximadamente un mes antes de implementar un ataque de ransomware el 3 de mayo. Durante este tiempo, realizaron actividades de exfiltración de datos y preparación para el despliegue del ransomware.

¿Cuál fue la solución para eso?

De acuerdo con la noticia, la solución fue:

Aislamiento y Eliminación del Ransomware: La ciudad desconectó servicios y servidores de alta prioridad y comenzó operaciones de restauración, asegurándose de eliminar el ransomware de la red.

Notificación y Protección: La ciudad informó a la Oficina del Fiscal General de Texas y notificó a las personas cuya información personal fue comprometida. Además, se asignó un presupuesto de $8.5 millones para medidas de mitigación, recuperación y

restauración. Se implementaron servicios de protección contra el robo de identidad y fraude para las personas afectadas.

¿Cuál es la medida de prevención contra esa falla?

De las medidas de prevención pienso que las siguientes podrían resultar efectivas para dicha falla:

Mejora de la Detección y Respuesta: Implementación de sistemas avanzados de detección de intrusiones para identificar actividades inusuales en la red y responder rápidamente a posibles amenazas.

Educación y Concientización del Personal: Capacitación del personal y los usuarios finales sobre prácticas seguras en línea y cómo reconocer posibles amenazas de phishing o malware.

Actualizaciones y Parches de Seguridad: Garantizar que todos los sistemas estén actualizados con los últimos parches de seguridad para cerrar posibles brechas de seguridad conocidas.