CC5327-1 Introducción a la Seguridad Computacional
Profesores: Alejandro Hevia A. y Eduardo Riveros Roca
Auxiliar: Sergio Rojas H.
Estudiantes: Andrés Calderón, Nicolás Arancibia, Martín Bahamonde y Martín Rojas

Caso de Estudio 4

Ransonware

P1. Discutan qué datos personales y sensibles pudo haber obtenido el atacante en su institución.

Por las bases de datos disponibles sería posible obtener datos personales de los clientes, además de sus viajes pasados, y también información sobre los trabajadores.

P2. Definan un plan de ciber resiliencia para la organización y describan la infraestructura TI crítica necesaria para soportar funciones esenciales.

Primero tenemos el objetivo de:
- Garantizar la continuidad de operaciones esenciales como reservas, check-in y gestión de vuelos (considerando ataques de ransomware).
- Proteger los datos personales de clientes y empleados.

En cuanto a las estructuras criticas tenemos las siguientes:
- Amadeus Altea (PSS): Usado para la gestión de reservas, check in y compras de pasajes con APIs para microservicios. Si el ransomware alcanza los servidores intermedios que conectan front con altea, el sistema podría quedar inutilizable generando interrupción en venta y embarque de pasajeros.
- Clusters SQL: Encargado del almacenamiento de datos críticos como itinerarios o vuelos. Si se ataca afecta directamente a las reservas, check in y seguridad operativa.
- Back ups en frío: Esencial para el funcaccionamientonto ante eventualidades como el ataque de un Ransomware, el tener backups en frío ayuda a la vuelta al funcionamiento limitando la perdida de datos o el tener que pagar el rescate.

Finalmente el plan está compuesto de 5 etapas:

1. «Preparacion y prevención»: Primero se tienen que repasar las políticas de ciberseguridad de la empresa, clasificando los activos críticos y el respaldo de la información (definiendo periodos del back up en frío por ejemplo). Otro punto en esta fase es la separación de privilegios, aislar servidores de RRHH del resto del sistema (evitando movimientos laterales), se deberá repasar el control de acceso (IAM), implementando autenticación por multifactor para todo el personal con acceso privilegiado.

   Por otro lado se debe hacer un escaneo semanal automatizado en la infraestructura híbrida, en caso de que los sensores IoT estén defectuosos o comprometidos. Finalmente una actualización prioritaria en los componentes expuestos (endpoints y microservicios).

2. «Detección, Análisis y Monitoreo continuo»: Se deben setear alertas de comportamiento anómalo en el tráfico, como el DNS nocturno o accesos inusuales. Por otro lado mantener una busqueda activa de amenazas a través de una revisión constante de los logs sistemas de cloud junto con los endpoints mas criticos, los cuales a su vez se deberan mantener en constante auditoria en busca de posibles errores o vulnerabilidades.

3. «Respuesta ante incidentes»: Tener protocolos definidos para distintos tipos de ataque. Por ejemplo para Ransomware tener un aislamiento inmediato del nodo y comunicación interna, para la exfiltración de datos una notificación inmediata a las autoridades correspondientes (CSIRT). Otro punto importante es tener respuestas coordinadas y planeadas con el equipo legal y de comunicaciones para poder contestar a la prensa u otros medios de ser el caso. Finalmente tener un equipo de expertos entrenado para actuar ante incidentes incluso fuera del horario laboral.
4. «Recuperación y Restauración desde back ups en frío»: Usar el back up en frío (actualizado en periodicidades cortas) para tener una infraestructura lista para el levantamiento rápido de los micro servicios críticos en la continuidad del negocio, separado por área:

- Check in manual (si PSS cae).
- Emisión de pasajes offlinte y atención por call center reforzado (para responder a la crisis).
- Comunicaciones por canales seguros alternativos.

5. «Mejora Continua»: Efectuar un análisis post-incidente, que incluya una evaluación técnica, organizacional y comunicacional frente al suceso. Crear informes al directorio con propuestas de mejora. Finalmente una actualización constante de protocolos y sistemas (según disponibilidad de recursos) sumado a una capacitación cada 6 meses obligatoria para todo el personal (enseñar sobre phishing, manejo de datos, ransomware, buenas prácticas... etc).

P3. ¿Cómo sabe su organización si hay actividad de red anómala?

Se puede realizar un seguimiento de la actividad común realizada entre los empleados y en cuanto se tenga un comportamiento distinto a esta norma revisar el caso para identificar posibles amenazas.

Otra opción sería hacer un seguimiento de las IPs de los empleados para identificar casos en que se realicen conexiones desde IPs externas a los empleados de la empresa.

P4. ¿Qué sistemas redundantes deberían existir cuando los primarios son comprometidos? ¿Qué alternativas manuales existen a procesos críticos? ¿Por cuánto tiempo se pueden ejecutar?

Sistemas para acceder a las bases de datos de forma que se pueda mantener la continuidad de otros servicios que dependan de estas, además de métodos adicionales para acceder a servidores de la empresa.

Se pueden realizar de forma manual respaldos de bases de datos y similares, mientras que estos debiesen durar unas pocas horas para minimizar los tiempos de caída de los servicios.

P5. ¿Cómo debo notificar? ¿Qué notifico?

Se debe notificar mediante el principal medio de comunicación de la empresa, y dentro de lo posible notificar de forma presencial. Se debe notificar la situación junto con todo su contexto, cómo aparece el mensaje, el mensaje como tal, qué archivos o información están secuestrados, etc.

P6. Expliquen los pro y contras de pagar al atacante, además del valor de la información robada.

Pros:

- Mayor posibilidad de recuperar la información secuestrada.
- Posibilidad de que no se filtre el hackeo y así mantener la reputación de la empresa.

Contras:

- Se fomenta las practicas de los atacantes, lo cual incentiva que sigan intentando cometer estos crímenes.
- Si se revela que la organización pagó, sería un golpe hacia su imagen publica.
- Según la Ley N° 21.663, Ley Marco de Ciberseguridad se deben reportar los incidentes de ciber ataque a la Agencia Nacional de Ciberseguridad, y su incumplimiento puede resultar en multas, además, también se podría caer en el incumplimiento de la Ley N° 19.913 sobre Lavado de Activos y Unidad de Análisis Financiero (UAF) puesto esta estipula que cualquier actividad sospechosa que pueda servir al blanqueo de capitales debe reportarse a la Unidad de Análisis Financiero.

P7. ¿Cómo responde su institución a los medios? ¿Tienen mensajes prehechos? ¿Cómo comunicar a los clientes?

Dada la situación actual a la que se enfrenta la empresa se debiera mencionar que se está manejando la filtración lo mejor que se puede y que se hará todo lo posible para evitar que ocurra.

Seria ideal tener una serie de mensajes pre-hechos para las distintas situaciones a las que pueda enfrentarse la empresa.

Enviar un correo a los clientes informando de la situación por la que se está pasando, sin links externos ni documentos adjuntos.

P8. Luego de ejecutar lo anterior, qué desafíos identifican para mejorar la resiliencia de otras organizaciones.

Al enterarse de este ataque tomar medidas preventivas para evitar que pueda reproducirse el mismo problema y mejorar la seguridad en todos los sistemas informáticos.