Universidad Rafael Landívar
Facultad de Ingeniería
Seminario de casos

CASO NO.4

Caso “Ransomware Attack at Springhill Medical Center”

Grupo #23	Carné	Nota
Ximena Elizardi	1101720	
María José Martinez	1198320	
Christian Cifuentes	1066420	
Edrei Fratti	1292020	

Guatemala, 11 de septiembre del 2024

Contexto del caso:

En 2019, el “Springhill Medical Center” (SMC) Fue sujeto de un ataque de ciberseguridad de tipo “Ransomware” en el cual cualquier información o servidor dentro de una red local puede quedar “secuestrado”, los perpetuadores del ataque encriptan toda la información y al realizar un pago se puede liberar la información.
Debido al ataque, para evitar que este afectara más áreas, SMC decidió desconectar todos sus equipos de última tecnología, dejando únicamente en funcionamiento equipo bastante obsoleto que afectó la calidad de servicio del hospital además de dificultar las operaciones del staff operativo.
Como consecuencia de todo esto, no se logró detectar a tiempo una complicación de un parto relacionado con estrangulamiento del cordón umbilical de un bebé que más adelante terminaría falleciendo. Esto llevo a una demanda por desinformación fraudulenta, negligencia médica e incumplimiento imparcial de contrato, llegando a ser el primer caso de muerte causada indirectamente por un ciberataque.

Involucrados y qué papel juegan

- Teiranni Kid: Mujer que tuvo un parto con hipertensión y que su hija recién nacida falleció. Impartió una denuncia a SMC y a la Dra. Katelyn Parnell debido a la falta de información sobre el ciberataque que sucedió en su estadía médica.
- Banda Ryuk: Banda Rusa de hackers sospechosa al ciberataque ocasionado en CMS, y a los posibles candidatos del problema de este caso. Estos se conocieron por haber atacado aproximadamente 235 hospitales e instalaciones sanitarias en Usa.
- Katelyn Parnell: Doctora encargada del parto de Teiranni, se le acusa de no haber actuado correctamente o haberle informado a Teiranni la presencia de ciberataque que estaba presente en el hospital.
- Jeffery M. St Clain: Presidente y director ejecutivo (Veterano de SMC). Fue la persona encargada de dirigir al hospital durante el ataque y asimismo fue la encargada de que medidas eran necesarias para contener el ciberataque.
- Mark Kilborn: Director de información del hospital, fue la persona responsable de los analisis y sistemas de datos, teniendo en cuenta la importancia de la ciberseguridad.
- Paul Read: Jefe de enfermería, evaluar el trabajo de los enfermeros en turno cumpliendo los estándares de atención
- René Areaux: Director de operaciones en el hospital. Responsable de que todas las operaciones y funcionamiento del hospital se ejecuten de manera eficiente.
- Stephen Grigsby: Vicepresidente financiero, vela en la sostenibilidad y estabilidad económica del hospital en casos emergentes como lo fue el ciberataque.

- **Describir razones de la situación actual**
  - Ransomware: Un ataque de ransomware inhabilitó los sistemas informáticos del hospital, incluyendo los registros médicos electrónicos.
  - Impacto en la atención: La falta de acceso a información digital dificultó la atención a los pacientes. En un caso, la falta de monitoreo adecuado contribuyó a la muerte de un bebé.
  - Comunicación deficiente: El hospital no informó de manera clara y oportuna sobre el incidente, generando confusión y desconfianza.
  - Recuperación lenta: La recuperación de los sistemas tomó semanas, lo que prolongó los problemas operativos y expuso los datos de los pacientes a riesgos.

Hechos	Inferencias o supuestos
El hospital sufrió un ataque de ransomware por un grupo terrorista ruso.	El hospital evitó reconocer el ataque hasta el último momento posible para evitar perder clientes o que se viera afectada su reputación
El hospital declaró en 2015 su compromiso con la ciberseguridad asegurando que “Es importante la educación constante del usuario en hacer buenas decisiones con respecto a que colocan en el sistema”	El supuesto compromiso con la ciberseguridad fue una fachada para incentivar la imagen de seguridad del hospital y no se lo tomaron en serio, o por lo menos no totalmente.

Problema	Causa	Herramienta de análisis
Bloqueo en los sistemas cibernéticos	Ciberataque de Ransomware: Bloqueo en el acceso de data	Análisis de ciberseguridad
Deficiencia en la gestión de áreas	Falta de comunicación: Los doctores, los enfermeros y pacientes no se encontraban enterados del ciberataque que se estaba viviendo en el CMS.	Capacitación de personal sobre ciberseguridad. FODA
Muerte y demanda	Mala práctica de monitoreo y control: Inaccesibilidad de los sistemas pertinentes, como lo fue la unidad de parto y alumbramientos. Falta de información proporcionada de parte del hospital por el ciberataque.	Análisis de riesgos y fallos: Cumplimiento del código hospitalario (Salud),

1. **¿Manejaron en SMC la crisis de manera adecuada? Analiza la respuesta de SMC desde varios aspectos, incluyendo la comunicación en crisis, la respuesta inicial y los planes de continuidad del negocio.**

    - Plan de continuidad de negocio: El hospital no contaba con un plan sólido de continuidad de negocio, lo cual se refleja en el tiempo que tardaron en recuperar completamente sus operaciones y la calidad del servicio brindado durante el ataque. Dependían fuertemente de la tecnología, y al verse está comprometida, no lograron mantener el estándar de atención necesario. Además, la falta de suficiente personal capacitado para manejar la crisis empeoró la situación, ya que muchos empleados no estaban preparados para operar sin la tecnología habitual
    - Comunicación en crisis: Uno de los puntos críticos fue la falta de comunicación honesta y transparente tanto con los pacientes como con el personal. Si la comunicación hubiera sido efectiva y el personal médico hubiese tenido acceso a la información necesaria, es probable que la situación de la bebé Kidd se hubiera manejado de manera diferente, evitando su fallecimiento). Además, la comunicación interna durante el ataque fue deficiente, lo que resultó en decisiones inadecuadas por parte del personal, quienes no sabían cómo proceder.

- Respuesta inicial: Aunque la respuesta inicial fue rápida en términos de desconectar los servicios conectados a la red para mitigar el ataque, no fue suficiente. La falta de coordinación y comunicación sobre el estado del sistema y la implicación en los servicios críticos afectó negativamente la atención a los pacientes. El personal médico no fue informado adecuadamente, lo que llevó a una mala toma de decisiones en la continuidad del cuidado. De haber sido informado correctamente, se podrían haber priorizado ciertos servicios esenciales, como los monitores fetales, para garantizar la seguridad de los pacientes.
- Protección de la marca: En lugar de informar rápidamente sobre el ataque y las limitaciones tecnológicas críticas, SMC intentó proteger su reputación al no comunicar inmediatamente la situación. El hospital continuó aceptando pacientes, incluso cuando sistemas esenciales no estaban operativos, lo cual es indicativo de un enfoque centrado en evitar el daño reputacional en lugar de la seguridad del paciente. Esta falta de transparencia resultó en consecuencias graves, incluyendo la muerte de un bebé, cuando los monitores no pudieron detectar problemas durante el parto

2. **¿Deberían haber sido informados los pacientes sobre el incidente de Ransomware? ¿Debería el hospital haber cerrado sus servicios y desviado a los pacientes a otros hospitales?**

   Los pacientes debieron ser informados respecto al incidente que ocurría en el hospital ya que esto hubiera demostrado la transparencia y profesionalidad de SMC. Y no solamente estos puntos. Sino que la acción que mantuvo el hospital, en omitir u ocultar información a los pacientes generar una violación de ética médica, creando una deficiencia en la atención médica debido a la propagación del Malware a los sistemas o equipos especializados en el registro de datos y monitores de signos vitales aumentando el riesgo hacia los pacientes de enfermedades o incluso la muerte, como lo fue la hija de Teiranni Kid.

   El hospital sí hubiera considerado cerrar sus servicios o desviar a los pacientes a otros hospitales debido a la falta de recursos o herramientas adecuadas para atender a la población, sin importar la pérdida que conllevaría. Es primordial la seguridad del paciente y así no poner a ninguna persona en riesgo imprudentemente por la falta de capacidad en emergencias sin comprometer al hospital en alguna demando o incluso la muerte de un paciente como lo fue este caso. Otra opción que se puede considerar es que el hospital en estas adversidades reciba solamente a pacientes en estado crítico para ayudarlas manualmente y desviarlas a un hospital que cumpla con los equipos especializados sin ningún ciberataque.

3. **Si fueras el CEO/CIO de SMC, ¿cuáles serían las primeras cosas que harías al inicio del ataque?**

   Ante el escenario presentado donde posiblemente no se cuente con medidas de contingencia o prevención contra emergencias, las primeras acciones para tomar ante un ataque de ransomware serían enfocadas en la contención inmediata del incidente. Esto quiere decir desconectar los sistemas afectados para evitar la propagación del ataque y aislar la red comprometida. Es importante notificar a las autoridades, como agencias de ciberseguridad y el FBI, para que colaboren en la investigación y mitigación del ataque. Después, se evaluaría el alcance del ataque definiendo que servicios dentro del hospital pueden continuar operando, dependiendo de su criticidad y que tanto se vio afectada su calidad para informar claramente al personal para que no se tengan incidencias y redirigir a los pacientes entrantes a otros centros hospitalarios como a los pacientes y sus familias para que puedan tomar decisiones informadas respecto la salud de sus seres queridos. Incluso preparar documentos jurídicos para los pacientes que decidan continuar sus procedimientos en SMC estén totalmente conscientes del incidente y sus posibles consecuencias.

   Al mismo tiempo facilitar todas las herramientas necesarias para restaurar los servicios lo mas pronto posible. Una vez restaurados los servicios, se puede contemplar la creación de un plan de continuidad de negocio para evitar

4. **¿Hizo bien el hospital en no pagar el rescate? En general, ¿deberían las organizaciones pagar a los perpetradores de ransomware?**

   El hospital hizo bien en no pagar el rescate. Incluso SMC logró restablecer los sistemas de red interna y la página web publica sin pagar el rescate. Además, los posibles perpetuadores (Banda Ryuk) pueden aprovechar del rescate para seguir extorsionando o bien continuar atacando al hospital. Si se les pagara a los perpetuadores, el mismo SMC financiaría sus actividades mediante el pago y estos pueden estar afiliados a una red de organizaciones criminales, pudiendo perjudicar al hospital en sanciones financieras según el reglamento de leyes de Alabama donde se encuentra ubicado el hospital.

   Las organizaciones no deberían de pagar a los perpetradores de ransomware. Esto puede generar pérdidas financieras dentro de la organización por los altos costos que conlleva esto, teniendo en cuenta que también puede ser una extorsión donde el restablecimiento del ciberataque queda en el aire o en la decisión de los perpetuadores a su beneficio. Además del rescate, se pagaría la restauración de datos, ciberseguridad de red con mayor rigidez, auditorías internas y externas. E incluso dañando más la reputación e imagen de la empresa.

5. **¿Cómo deberían los hospitales y otras organizaciones gestionar la amenaza de las brechas de ransomware?**

   Adoptar un enfoque preventivo. Mejorar la ciberseguridad es una prioridad, implementando medidas como actualizaciones frecuentes de software, entrenamiento continuo en seguridad para el personal y auditorías regulares que identifiquen posibles vulnerabilidades. También es importante contar con copias de seguridad y frecuentes de los datos críticos, almacenadas en ubicaciones seguras y no conectadas a la red principal, lo que permite restaurar la operación sin necesidad de ceder a las demandas de los atacantes.

   Los hospitales deben tener protocolos claros de respuesta a incidentes que incluyan la comunicación efectiva, procedimientos de respaldo y la acción rápida de equipos especializados en ciberseguridad. Es importante revisar la seguridad en la cadena de suministro, asegurando que los socios y proveedores cumplan con altos estándares de protección para evitar brechas a través de terceros. La implementación de tecnologías de detección avanzada, como sistemas que identifiquen actividad inusual en la red, puede ser una herramienta clave para neutralizar amenazas antes de que causen daño.

6. **Lecciones aprendidas**

Analizamos las lecciones aprendidas en base a 5 factores:

- Factores Humanos: Es esencial establecer canales de comunicación claros y efectivos durante crisis como ciberataques. El personal debe estar informado de manera oportuna y transparente para evitar confusión y garantizar que puedan realizar su trabajo de manera segura. Además, es fundamental brindar apoyo emocional al personal para evitar el agotamiento y el estrés excesivo en momentos de crisis.
- Factores Técnicos: Las organizaciones deben mejorar su infraestructura de ciberseguridad, asegurándose de que los sistemas estén protegidos frente a amenazas como el Ransomware. Además, la dependencia de sistemas digitales requiere planes de contingencia más sólidos para garantizar la continuidad del servicio en caso de fallos técnicos.
- Factores Profesionales: Los procedimientos médicos y la toma de decisiones deben seguir siendo sólidos, incluso en situaciones de emergencia tecnológica. La falta de sistemas digitales no debe comprometer la atención médica, lo que subraya la necesidad de que los profesionales de la salud reciban capacitación continua en procedimientos manuales y uso de protocolos alternativos.
- Factores Informáticos: Es importante tener buena seguridad en los sistemas y una infraestructura fuerte para que los hospitales sigan funcionando bien y los pacientes estén seguros, especialmente en situaciones críticas. Desde el punto de vista de informática, los hospitales deben mantener sus sistemas actualizados, enseñar a su personal sobre seguridad digital y estar preparados con planes de acción en caso de un ataque cibernético o problema técnico.

Anexos:

Procedimiento para establecer un plan de continuidad de negocio y contingencia en casos de emergencias:

1. Establecer procesos críticos y prioridades. Posibles riesgos, amenazas, las posibilidades que sucedan estos riesgos, cuáles son las implicaciones que sucedan estos riesgos o amenazas.
2. Definir los tiempos de recuperación (Cuanto tiempo puede estar abajo los servicios dependiendo de su criticidad, en cuanto tiempo el servicio debe estar operando nuevamente)
3. Con base a lo anterior, establecer como se van a mitigar los riesgos encontrados (segmentación de red, periodicidad de backups, políticas de actualización, etc)
4. Definición de posibles alternativas que puedan existir para cubrir servicios críticos.
5. Realizar pruebas de restauración en ambientes de pruebas o sandbox.
6. Crear planes de capacitación para el personal.
7. Implementar el plan.
8. Mejora y actualización continua.

Tecnologías recomendadas para implementar el plan:

1. Anti-virus
2. Anti-Ransomware
3. Software de monitoreo de amenazas
4. Almacenamiento y organización de backups

Personal necesario:

1. DataBase Administrator (DBA)
2. Gerente de IT
3. Soporte técnico
4. Auditor de ciberseguridad.