Paco Sánchez Pérez (psanchezp@clinic.cat)
Daniel Gutiérrez Cerón (dgutier@clinic.cat)
Técnicos especialistas en Redes y Seguridad IT
Alejandro Nieto Esteban (anieto@clinic.cat)
CISO
Hospital Clínic de Barcelona

Cómo se vive y sobrevive a un ciberataque

Los ciberataques ya forman parte de las amenazas más frecuentes y temidas en todos los sectores, siendo el sector sanitario uno de los más afectados en los últimos años. Los atacantes no sólo buscan el robo de información sensible, su objetivo también es interrumpir servicios esenciales como la salud, privando a los ciudadanos de ser atendidos de forma eficaz con el fin de aumentar la presión de pago por el rescate que solicitan los cibercriminales. Desde el Hospital Clínic de Barcelona podemos dar fe de ello en base al ciberataque que padecimos.

Cronología del ciberataque

Según reveló el análisis forense, a pesar de que el ciberataque explotara el 5 de marzo de 2023, los ciberdelincuentes habían obtenido acceso semanas antes a partir de un ataque de fuerza bruta sobre el sistema de acceso remoto que empleamos para el teletrabajo. Una vez dentro del sistema, emplearon varias técnicas avanzadas de hacking para obtener los privilegios necesarios e ir descubriendo los recursos que después atacarían.

De forma sigilosa y sin levantar sospecha, imitando el comportamiento habitual de envío de datos que tienen otros equipos de la red en nuestro Hospital, estuvieron semanas transfiriendo datos desde las carpetas personales que los usuarios tienen en los servidores de ficheros de la red corporativa hacia servidores de los atacantes en Internet.

Tras haber completado la transferencia de datos procedieron a activar el ransomware, no sólo encriptando los datos que habían robado sino también los ficheros del sistema de virtualización de servidores, provocando así, además de la perdida de acceso a los datos, también la indisponibilidad de la mayor parte de los servidores y de las aplicaciones que éstos alojaban y que sustentan la mayor parte de actividad asistencial que realizan los profesionales sanitarios en su día a día.

Durante los días inmediatos al incidente se conoció que el responsable del ciberataque fue el grupo RansomeHouse, responsable de múltiples ataques a empresas en todo el mundo, y que solicitaban un rescate de 4,5 millones de euros por liberar el ransomware y no hacer públicos los datos robados. Evidentemente no se negoció el pago del rescate; además de no estar legalmente permitido tampoco garantiza que se recuperen los datos y finalice la extorsión, como así ha ocurrido en otros casos.

Impacto en la actividad asistencial

El impacto del ataque sobre los servidores provocó otros daños colaterales en muchos dispositivos, PCs y aplicaciones que usan los profesionales sanitarios para atender a los pacientes, dado que sin tener disponibles los servidores perdieron la totalidad o parte importante de su funcionalidad y accesibilidad a datos relevantes, como las historias clínicas o pruebas diagnósticas.

Ante esta situación se activan los protocolos de contingencia establecidos a nivel asistencial para seguir atendiendo la actividad en ausencia de los recursos tecnológicos habituales. Esto implica que gran parte de la actividad se realiza en papel, se requiere más personal y todos los procesos asistenciales se realizan de una forma más lenta a la habitual.

Las limitaciones que se generaron obligaron a reducir drásticamente la actividad habitual del Hospital, reduciéndola los dos primeros días a únicamente actividad asistencial urgente y hospitalizaciones, derivando el resto de actividad a otros hospitales. De la misma manera, durante la primera semana se

requirió desprogramar visitas a consultas externas, intervenciones no urgentes y tratamientos oncológicos de radioterapia. Algunos de los números más alarmantes de la actividad que se dejó de hacer fueron más de 300 intervenciones, más de 4.000 analíticas y más de 11.000 visitas a consultas externas.

Trabajo de TI para recuperar la normalidad

Ante la situación de caos generada por el gran impacto del ciberataque, al equipo de TI se nos presentó el mayor reto profesional que hemos vivido hasta el momento. La implicación personal de todos los miembros, la de la Agencia de Ciberseguridad de Catalunya, la de empresas colaboradoras y el trabajo en equipo coordinado con Dirección Médica, fueron clave para superar la situación tan adversa en la que nos encontrábamos.

Notificar el ciberataque a la Agencia de Ciberseguridad de Cataluña tan pronto como certificamos que habíamos sido atacados fue clave para afrontar la situación de una manera ordenada y eficaz. Trabajar con ellos nos permitió establecer el protocolo de actuación adecuado a estos casos, evitando dar pasos en falso y contando con recursos técnicos adicionales; además se coordinaron con los cuerpos policiales para investigar y perseguir el delito. El plan de trabajo que establecimos junto a la Agencia podemos resumirlo en las siguientes iniciativas:

• ***Aplicar medidas para erradicar el ciberataque.*** Evitando así que mantuviesen algún tipo de control sobre nuestros sistemas, para ello se bloquearon usuarios con el fin de evitar suplantaciones de identidad y el aislamiento completo de la red para evitar accesos desde el exterior.

• ***Realizar análisis forense de impacto y alcance.*** Este proceso revela la manera en que accedieron los atacantes, los sistemas que vulneraron y el impacto de sus acciones, descrito al inicio del artículo.

• ***Despliegue de equipos portátiles para el personal médico.*** Se desplegaron hasta 210 equipos nuevos contando con conectividad 4G para que pudiesen tener acceso a la historia clínica compartida. En paralelo se revisó la seguridad y se aplicaron actualizaciones a los equipos corporativos.

• ***Restauración de los datos.*** Realizado a partir de copias inmutables en cinta magnética, el tener una buena política de copias fue clave para que la restauración fuese exitosa; no disponer de esta opción hubiese dificultado muchísimo poder recuperar los sistemas afectados.

• ***Puesta en marcha de los sistemas afectados.*** Para cada uno de los sistemas restaurados se procedía a realizar análisis antimalware con el fin de detectar y eliminar una posible persistencia del ataque; además se aplicaron ajustes de seguridad a nivel de sistema operativo (aplicando parches de seguridad o reinstalando los sistemas cercanos a su obsolescencia) y aislando a nivel de red aquellos sistemas obsoletos sin posibilidad de actualización.

• ***Cambio masivo de contraseñas.*** Antes de realizar el cambio masivo se reforzó la política de contraseñas añadiendo mayor complejidad, rotación y activando el múltiple factor de autenticación al 100% de las cuentas. Por seguridad el cambio debía ser presencial, teniendo que desplegar dispositivos en distintas ubicaciones para atender a más de 8000 usuarios cubriendo todos los turnos horarios.

Todas estas iniciativas y procesos aplicados para conseguir restaurar los sistemas e ir recuperando la actividad asistencial en su plenitud han supuesto un gran desgaste, obligándonos a tratar y superar situaciones adversas inesperadas que se presentaban por sorpresa al tratar de aplicar las soluciones correspondientes a las iniciativas mencionadas. Es por este motivo que quisiéramos poner en valor el trabajo colaborativo entre profesionales, la capacidad de liderazgo de nuestros referentes en el área de TI y área médica para coordinarse y establecer prioridades a diario en los comités de crisis que se hacían, y también destacar la respuesta del personal asistencial que a pesar de trabajar en condiciones de adversidad siempre fueron comprensivos y tuvieron paciencia en recuperar las herramientas tecnológicas que les permitían recuperar la normalidad.

Reflexiones y conclusión

El ciberataque sufrido en nuestro Hospital, teniendo en cuenta la dimensión de su impacto y repercusión, ha significado un antes y un después en la manera en cómo se gobierna y gestiona la ciberseguridad tanto a nivel de administraciones públicas por parte del gobierno de Cataluña, como por parte de muchas instituciones a nivel particular.

Sin duda, ha servido de palanca de cambio para que todos tomemos conciencia de la importancia de establecer modelos de gobierno multidisciplinar (la seguridad no es sólo cosa de las áreas de TI), donde se establezcan controles de seguridad según la evaluación de los riesgos tecnológicos que presentan las soluciones implantadas y se elaboren planes de respuesta y continuidad ante incidentes de seguridad. Todo esto, pese a estar regulado en el Esquema Nacional de Seguridad (ENS) en su primer real decreto de 2010 y actualizado en 2022, siendo de obligado cumplimiento para las instituciones públicas, no se aplicaba de forma estricta.

Al ciberataque sufrido en nuestro Hospital le preceden otros como el Hospital de Berga, el Hospital de la Seu d'Urgell o el Consorci Sanitari Integral, produciendo interrupción de la actividad de los centros sanitarios en la mayoría de los casos. El cúmulo de ataques y las graves consecuencias que éstos han supuesto han hecho reaccionar a los organismos públicos competentes, los cuales han destinado 6,5 millones de euros en 2024 para impulsar y trazar un plan en ciberseguridad que permita reforzar la protección, la prevención y resiliencia de los organismos públicos de Cataluña, poniendo mucho foco en el

sector Salud. Actualmente la Agencia de Ciberseguridad de Cataluña ya ha activado el proyecto SOC-Salut, el cual consta de un sistema centralizado de alertas ante ciberataques, medidas de protección, capacitación y control de cumplimientos normativos, siendo 68 los centros sanitarios públicos catalanes adheridos a este proyecto. A nivel interno dentro de nuestro propio Hospital, como no podía ser de otra manera, ha resurgido el proyecto de adecuación al ENS, esta vez con más fuerza y apoyo tras la incorporación de la figura de nuestro CISO.

Los que llevamos años trabajando en la seguridad informática de un hospital conocemos las limitaciones que presentan muchas soluciones de mercado para poder adaptarse a las políticas de seguridad que establecemos, obligándonos en numerosas ocasiones a aplicar excepciones para no perder funcionalidades. En nuestro sector es común la existencia de soluciones diseñadas para dar una funcionalidad concreta, pero en las que no se han tenido en cuenta aspectos clave de seguridad durante la fase de diseño (por ejemplo, basándose en protocolos y/o configuraciones inseguras). Otra situación que suele darse es que a las áreas de TI nos pidan integrar soluciones en cuya decisión de compra no hemos participado, lo que implica que no se ha tenido opción de evaluar el cumplimiento de unos mínimos de seguridad y que la integración en nuestros sistemas pueda llegar a ser un verdadero quebradero de cabeza.

Por este motivo es muy importante tratar de impactar sobre los fabricantes y proveedores de soluciones e-health para que pongan foco en un diseño seguro, y por defecto, de las soluciones que ofrecen a nuestro sector. Para ello desde el Clínic, y dentro del proyecto de adecuación al ENS, estamos en proceso de revisión de los circuitos por el que se realizan compras de soluciones tecnológicas que después van a requerir integrarse en nuestro sistema, introduciendo cláusulas de cumplimiento de normativas de seguridad basadas en el ENS, ISO 27001 y RGPD.

En el Clínic, tras sufrir las consecuencias del ciberataque y vivir de primera mano la dureza y complejidad de afrontar la restauración de los sistemas afectados, hemos aprendido mucho, el grado de concienciación a nivel organizativo ha crecido considerablemente, ahora nadie cuestiona que se soliciten requisitos de ciberseguridad, y aunque nos queda camino por recorrer lo afrontamos con más fuerza que nunca.