STORMSHIELD

ARTÍCULOS DE OPINIÓN

¿SE LIBRARÁN ALGUNA VEZ LOS HOSPITALES DE LA AMENAZA CIBERNÉTICA?

Victor Poitevin
Editorial & Digital Manager, Stormshield

El volumen de incidentes de seguridad en las instituciones sanitarias se ha disparado entre 2020 y 2021: un aumento del 35 % en Estados Unidos, del 45 % en España y de hasta un 50 % en Alemania y Francia... Se trata de una situación crítica, dado que estos entornos sensibles necesitan una media de 28 días para volver a la actividad normal. A pesar de la ayuda y el apoyo de los Estados, ¿por qué los hospitales siguen siendo vulnerables en la actualidad?

Análisis y reacción de los expertos sobre un fenómeno que preocupa a los profesionales de la salud y al público en general.

INICIATIVAS PARA HACER FRENTE A LAS CIBERAMENAZAS

La fragilidad de las instituciones sanitarias se puso de manifiesto con la pandemia de COVID-19 a principios de 2020. En ese momento, los hospitales se vieron afectados y paralizados por los ciberataques casi a diario, independientemente de su tamaño o ubicación geográfica. AP-HP en marzo de 2020, Dax, Oloron-Sainte-Marie y Villefranche-sur-Saône en febrero de 2021, Arles en agosto de 2021, GHT Cœur Grand-Est en abril de 2022, y Corbeil-Essonnes más recientemente, en agosto de 2022. Una lista que parece interminable...

Sin embargo, **la vulnerabilidad de las instituciones sanitarias no es una novedad y lleva más de una década preocupando a los profesionales.** La primera iniciativa para hablar de ciberseguridad en las instituciones sanitarias se puso en marcha en Francia en 2011, en la ciudad de Le Mans. Con el deseo de reunirse e intercambiar opiniones, se organizó el primer Congreso Nacional de Seguridad de los Sistemas de Información Sanitaria bajo la batuta de **Vincent Trely**, CISO del Hospital Universitario de Le Mans. En 2013, también en Francia, la Ley de programación militar (LPM) consagró la noción de OIV (operadores de importancia vital). Este acrónimo clasifica un conjunto de empresas y organizaciones esenciales para la supervivencia de la nación. Si bien la lista no difundió públicamente, los grandes hospitales más importantes están incluidos. Ese mismo año, la American Association Hospital (AHA) comenzó a publicar alertas e informes sobre ciberataques a centros sanitarios en Estados Unidos. Unos años después, en julio de 2016, se adoptó a nivel europeo la Directiva NIS (*Network and Information Security*). En particular, prevé el refuerzo de la ciberseguridad para los operadores de sectores clave mediante la creación del concepto de OES (operadores de servicios esenciales), otro acrónimo que viene a complementar al de OIV. En 2017, la reestructuración de los Groupements de Coopération Sanitaire (GCS) de los centros sanitarios franceses permitía facilitar y desarrollar los intercambios entre los CISO de los grupos sanitarios.

Por tanto, la concienciación parece venir relativamente de lejos, al menos en cuanto a los profesionales del sector sanitario (como los CISO o la ANSSI). **¿Garantiza esto una cierta protección contra las ciberamenazas?** Por desgracia, la crisis sanitaria y la explosión de los ciberataques han minado este optimismo. Según el analista estadounidense **Brett Callow**, casi 170 ataques de *ransomware* han infectado casi 1800 clínicas y centros sanitarios en Estasdos Unidos durante el periodo 2020-2021. En Francia, la ANSSI informó de una media de un incidente por semana en un centro sanitario en 2021 y anunció que 27 centros habían sido víctimas de un ciberataque en el mismo periodo. Se trata de un triste récord.

Ante estos nuevos ataques, el sector ha vuelto a movilizarse. A partir de febrero de 2020, algunas empresas privadas de ciberseguridad ofrecen acciones gratuitas de apoyo a las instituciones sanitarias. Al mismo tiempo, la ENISA ha publicado una guía en la que se enumeran las 10 mejores prácticas que deben aplicarse en las instituciones sanitarias para hacer frente a las ciberamenazas. Posteriormente, en marzo de 2020, más de 3000

profesionales de la ciberseguridad se reunieron en la COVID-19 Cyber Threat Coalition para compartir análisis e indicadores de peligro. Los flujos de información sobre amenazas se producen de forma voluntaria y se comparten a través de la comunidad. En septiembre de 2020, el Estado francés se dotó de un fondo de 136 millones de euros con el plan France Relance, cuyo componente de ciberseguridad pretende intensificar la seguridad de las infraestructuras críticas, como las de los centros sanitarios. Unos meses más tarde, el Ministerio de Sanidad francés aumentó este presupuesto en 350 millones de euros para los hospitales. En abril y junio de 2021, el Gobierno alemán publicó una ordenanza destinada a obligar a los proveedores de servicios que utilizan infraestructuras críticas, incluidos los hospitales, a reforzar su ciberseguridad, mientras que las autoridades francesas incluyeron a 135 grupos hospitalarios en la lista de operadores de servicios esenciales (OSE). Por último, en agosto de 2022, el Gobierno francés anunció un presupuesto adicional de 20 millones de euros para la ANSSI con el fin de reforzar el apoyo a los centros sanitarios.

Ante la amenaza cibernética, los hospitales no están solos. Pero ¿es suficiente?

¿POR QUÉ LOS HOSPITALES SIGUEN SIENDO VULNERABLES?

Frente a estos recursos, apoyos e iniciativas, las instituciones sanitarias siguen siendo vulnerables. Pero ¿por qué? De hecho, **la razón principal parece ser simple, ya que la superficie de ataque de los hospitales es muy significativa.**

La renovación de los equipos informáticos en los entornos sanitarios genera las primeras limitaciones. Mientras que los equipos informáticos convencionales se renuevan cada 5 años, los dispositivos médicos tienen modelos de rentabilidad que pueden durar hasta 15 años. En consecuencia, los sistemas actuales incorporan tecnologías de final de vida útil que ya no se mantienen. «*Estas inversiones de decenas o cientos de miles de euros se realizan a lo largo de diez o quince años*», explica **Charles Blanc-Rolin,** antiguo CISO de un centro sanitario y responsable del proyecto de seguridad sanitaria digital en el GCS e-santé Pays de la Loire. *No es raro encontrar sistemas Windows o Windows XP que no tiene soporte desde 2014. A veces incluso con versiones aún más antiguas de Windows para las que ya no hay parches de seguridad. Encontramos verdaderos coladeros y sistemas muy vulnerables. A esto se añade el marcado CE, que es un requisito reglamentario para el fabricante. Pero también resulta restrictivo para el centro sanitario, que no puede aplicar ninguna modificación a este dispositivo, como la actualización de un parche de seguridad, sin perder este marcado CE*». Para evitar el riesgo de utilizar sistemas operativos sin mantenimiento, las políticas de seguridad informática deben poder adaptarse, como señala Charles Blanc-Rolin: «*Es importante tener un plan de continuidad de la actividad y un plan de recuperación, pero también es igual de primordial tener procedimientos degradados. En la actualidad, disponemos de muchas herramientas de seguridad, pero nos olvidamos de lo básico y de la flexibilidad necesaria*».

«No es raro encontrar sistemas Windows o Windows XP que no tiene soporte desde 2014. A veces incluso con versiones aún más antiguas de Windows para las que ya no hay parches de seguridad.»

Charles Blanc-Rolin, director del proyecto de seguridad sanitaria digital del GCS e-santé Pays de la Loire

Al mismo tiempo, **los hospitales están sometidos a una digitalización a marchas forzadas desde hace más de una década,** lo que genera otras limitaciones. **Jean-Sylvain Chavanne,** CISO del Hospital Universitario de Brest y del Grupo Hospitalario de Bretaña Occidental, explica: «*Por poner un ejemplo, el perímetro que hay que proteger para el Hospital Universitario de Brest está formado por 140 aplicaciones, 350 servidores virtuales, 6000 puestos de trabajo, 10 000 objetos conectados a la red, 20 000 equipos biomédicos (como bombas de jeringa, resonancias magnéticas, cámaras hiperbáricas, etc.) y 2,7 petabytes de datos brutos que hay que guardar. Esto hace que el perímetro sea muy amplio. Al mismo tiempo, los hospitales han sufrido un proceso de digitalización a marchas forzadas desde la década de 2010, financiado por una sucesión de convocatorias de proyectos, sin presupuestos asociados para mantenerlos. Automáticamente, los hospitales se encuentran con una gran deuda técnica que deben compensar sobre la marcha*». A raíz de esta digitalización, **las instituciones sanitarias también se han visto debilitadas por la democratización de los productos conectados**. La medicina y sus usos están en constante evolución y los campos diagnóstico por imagen, la hospitalización a domicilio y la identificación de pacientes han protagonizado una revolución gracias a estas innovaciones, como recuerda Charles Blanc-Rolin: «*Con los nuevos usos, como el seguimiento de pacientes con pulseras RFID, podemos saber exactamente dónde se encuentra el paciente dentro de un hospital para mejorar su atención. Por tanto, es necesario enmarcar estos nuevos usos digitales y añadir una capa de seguridad sin generar una deuda técnica*». Ante la multiplicación de estos objetos en los servicios sanitarios, la expansión incontrolada de la superficie de ataque es un problema que Jean-Sylvain Chavanne analiza a través de tres grandes riesgos: «*El primer riesgo es la falta de control sobre los objetos conectados que se despliegan en el sistema de información de un hospital. Este es el caso cuando un proveedor llega y se conecta a la red sin ninguna medida de seguridad. El segundo riesgo está en las relaciones contractuales. Si no hay contratos con subcontratistas o proveedores, no se exigen obligaciones de seguridad, como la actualización del software correspondiente. Y por último, el tercer riesgo es el propio software, una auténtica «caja negra». Si no sabemos lo que contienen, no podemos controlar la seguridad ni parchear las vulnerabilidades. El pasado mes de diciembre, esto ocurrió con Log4Shell, donde tuvimos que ponernos en contacto con 200 proveedores de equipos médicos para averiguar si su software lo llevaba incorporado o no*».

«Los hospitales han sufrido un proceso de digitalización a marchas forzadas desde la década de 2010, financiado por una sucesión de convocatorias« sin presupuestos asociados para mantenerlos. Automáticamente, los hospitales se encuentran con una gran deuda técnica que deben compensar sobre la marcha.»

Jean-Sylvain Chavanne, CISO del Hospital Universitario de Brest

Sin embargo, las personas también son un factor de vulnerabilidad en los hospitales. Ante la carencia de personal, los equipos de TI se centran en proporcionar información con rapidez. A veces esto puede significar ignorar las normas de seguridad obvias. En este contexto, los equipos de SSI de los hospitales conciencian a su personal y, en ocasiones, recuerdan libertades que los profesionales de la salud no deberían tener y que hay que deconstruir, como analiza Jean-Sylvain Chavanne: «*Actualmente, nuestro equipo de seguridad bloquea un mensaje de spam cada 50 segundos y un virus cada hora. Es necesario concienciar y educar sobre el hecho de que no tenemos plena libertad para utilizar el software que almacena y gestiona los datos sanitarios. Por ejemplo, el personal médico no debería tener los diagnósticos de sus pacientes en sus teléfonos personales. Recordamos las buenas prácticas durante todo el año*». Contamos con un personal médico sometido a una presión constante, que tiende a tomar atajos para centrarse en su deber de atención y al que hay que hacer que sea receptivo al tema de la ciberseguridad. Un verdadero reto para los CISO, que pueden inspirarse en la comunicación que el director de un hospital parisino envió a sus empleados.

Obsolescencia de los equipos, una cultura del riesgo que se debe perfeccionar, los problemas de contratación... Aún quedan muchos puntos por resolver en los hospitales para garantizar una verdadera ciberseguridad de estas infraestructuras vitales.

HACIA UN FRENTE AMPLIADO DE CIBERAMENAZAS EN TORNO A LOS DATOS SANITARIOS

Ante estas diversas dificultades, Charles Blanc-Rolin pone de manifiesto que **la cuestión vital de la seguridad en los centros sanitarios se refiere a los datos de los pacientes y a su tratamiento.** «*Los ciberataques de ransomware, en particular, pueden paralizar un hospital y reducir las posibilidades de tratamiento de los pacientes. Sin acceso a datos y diagnósticos, los profesionales sanitarios tienen que hacer medicina de guerra. Ello da lugar a un deterioro de la calidad de la atención. Este es el verdadero peligro*».

«Sin acceso a datos y diagnósticos, los profesionales sanitarios tienen que hacer medicina de guerra. Ello da lugar a un deterioro de la calidad de la atención. Este es el verdadero peligro.»

Charles Blanc-Rolin, director del proyecto de seguridad sanitaria digital del GCS e-santé Pays de la Loire

Sin embargo, los datos sanitarios también tienen otro interés para los ciberdelincuentes. Más allá del carácter personal y habitual de ciertos datos como el nombre, el apellido y la fecha de nacimiento, estos datos pueden contener a veces un aspecto mucho más personal que puede generar situaciones de solicitud de rescates aterradoras para las víctimas. Esto es precisamente lo que les ocurrió a los pacientes de Vastaamo en 2020. Esta agrupación de 25 centros de psicoterapia de Finlandia fue víctima de una filtración de datos que contenía el seguimiento psiquiátrico de estos pacientes. Según informó *VICE*, 30 000 pacientes habían recibido una solicitud de rescate que debía pagarse en 24 horas o se revelarían los datos. Se trata de una evolución en el método de los ciberataques, dado que el rescate se suele asociar generalmente a una empresa. Sin embargo, en este caso, los pacientes estaban en primera línea. Se han presentado más de 25 000 denuncias ante las autoridades, lo que hace que este ciberataque sea el mayor caso penal de la historia de Finlandia. Unos meses más tarde, la autoridad finlandesa de protección de datos multó a la empresa con 608 000 euros por infringir el Reglamento General de Protección de Datos. Francia no queda exenta, ya que durante el mismo periodo se robaron 500 000 historiales médicos de un grupo de laboratorios del oeste del país. Según un estudio estadounidense, en marzo de 2022, **los datos sanitarios valían 25 veces más que una tarjeta de crédito.**

Si los datos de salud son una ganancia financiera para los ciberdelincuentes, los datos del universo sanitario pueden ser un objetivo para los poderes del Estado. Obtener información sobre el desarrollo de vacunas durante la crisis sanitaria ha sido una prioridad para algunos países que no disponían de medios de investigación y desarrollo. Según el *Wall Street Journal,* al menos seis empresas farmacéuticas, incluidas Johnson & Johnson y Novavax Inc, fueron objetivo de ciberactivistas norcoreanos en el mismo periodo. A finales de 2020, el mismo grupo, haciéndose pasar por una agencia de contratación, se dirigió supuestamente a empleados de Astrazeneca con falsas ofertas de trabajo con el objetivo de que por la empresa circularan documentos que contenían virus maliciosos. Ese mismo año, en Francia, de los 24 incidentes registrados en el sector sanitario, siete afectaron a la industria farmacéutica, según **Charlotte Drapeau,** responsable de la oficina de Salud y Sociedad de la ANSSI. Una tendencia subyacente según el *HIPAA Journal:* el número de brechas importantes que implican el robo de datos sanitarios en Estados Unidos ha pasado de 368 en 2018 a 714 en 2021.

Para Jean-Sylvain Chavanne, todos los ciberataques dirigidos a las empresas farmacéuticas francesas no son obra de los clásicos ciberdelincuentes: «*Todas las empresas farmacéuticas francesas que han desarrollado una vacuna contra la COVID-19 han sido víctimas de un ciberataque. Ante tal constatación, resulta complicado interpretarlo como el resultado de acciones oportunistas de los atacantes. Se trata de un deseo de desestabilización o de espionaje industrial*».

Las razones de la vulnerabilidad de las instituciones sanitarias son, pues, complejas. Son herencia de los problemas estructurales del sector e indudablemente no se resolverán en unos meses. Para saldar las deudas técnicas, solucionar la falta de personal y reducir la superficie de ataque, el sector sanitario debe actuar desde ya. Y para ello, puede contar con el apoyo de los Estados para (re)hacer del hospital un espacio conectado y seguro.