Jugar con vidas: los ciberataques a la sanidad son ataques a las personas

Marzo de 2021

Resumen ejecutivo

En línea o fuera de ella, atacar la sanidad es atentar contra las personas. Siendo un proveedor de servicios críticos y a menudo vitales, la sanidad debería estar fuera de cualquier intento o acción maliciosos, salvaguardada por y para todos, siempre, en condiciones que garanticen el respeto de la seguridad, la dignidad y la equidad humanas en los ecosistemas digitales. A estas condiciones las denominamos ciberpaz.

En marcado contraste con tales condiciones, desde noviembre de 2020, el número de ciberataques mundiales contra el sector sanitario ha aumentado un 45%, frente a una media del 22% de otros sectores . Sólo en noviembre de 2020, las organizaciones sanitarias de todas las regiones del mundo experimentaron un crecimiento significativo en el número de ciberataques, y tanto Europa Central como Asia Oriental y América Latina sufrieron incrementos superiores al doble[2].

El presente informe es una piedra angular del programa Cyber 4 Healthcare que el CyberPeace Institute puso en marcha en 2020 para ayudar a los profesionales de la salud a analizar los ataques que sufren y avanzar en las políticas de protección del sector y las personas a las que sirve. Nuestros objetivos son reducir el número y la magnitud de los ciberataques, imponer la responsabilidad y la rendición de cuentas de todos los actores y garantizar que las víctimas tengan voz y derecho a reparación.

Al consolidar la información que demuestra la complejidad, la magnitud y el alcance de la amenaza cibernética mundial para la sanidad, **este informe se centra por primera vez en el impacto de los ataques sobre las personas y la sociedad**. Tomando como base los testimonios de las víctimas, los informes sobre ciberseguridad, las iniciativas de carácter voluntario, los marcos jurídicos y la investigación empírica, el informe analiza la innovación técnica del modus operandi, la diversidad de los autores de las amenazas y sus motivaciones, la difícil aplicación de las normas y leyes nacionales e internacionales, y la escasa dotación de recursos del sector a pesar de existir un vibrante ecosistema de iniciativas con fines de asistencia.

---

[1] Check Point Software (2021) 'Attacks targeting healthcare organizations spike globally as COVID-19 cases rise again', Check Point Software, 5 January. Available at: https://blog.checkpoint.com/2021/01/05/attacks-targeting-healthcare-organizations-spike-globally-as-covid-19-cases-rise-again/ (Accessed: 12 January 2021).

[2] ibid

Desde el *ransomware* ("software de rescate") hasta las operaciones de desinformación relacionadas con la COVID-19, habida cuenta de que los incidentes apenas se denuncian, rara vez se atribuyen los ataques y los autores de las amenazas actúan con impunidad, el informe muestra que la responsabilidad es fundamental para cualquier solución sistémica.

Recomendaciones

En línea o fuera de ella, atacar la sanidad es atentar contra las personas. Con este informe pretendemos demostrar que, aunque los profesionales de la salud y los pacientes se enfrentan a una amenaza importante, que evoluciona y se agrava, **la acción colectiva es posible**. En él se pone de manifiesto la responsabilidad general que tienen los Estados en tomar la iniciativa para reducir los ataques a nivel mundial y en que los responsables de las amenazas rindan cuentas.

Estas recomendaciones se dirigen a los gobiernos, la industria, el sector sanitario, el mundo académico y la sociedad civil, con el propósito de conseguir un impacto duradero reduciendo los ataques a la sanidad. Las recomendaciones proponen:

1 Documentar los ataques y analizar su impacto humano y social

2 Mejorar la capacidad de respuesta y la resiliencia del sector sanitario a fin de:

2.1 Reforzar la ciberseguridad de la infraestructura sanitaria

2.2 Aumentar la capacidad y los recursos de la sanidad

2.3 Fortalecer la capacidad de respuesta de la sanidad a los ataques

3 Activar los instrumentos técnicos y jurídicos que permitan proteger la asistencia sanitaria con el objetivo de :

3.1 Reforzar el ecosistema jurídico y normativo

3.2 Mejorar el intercambio de información y las normas de presentación de informes

4 Exigir responsabilidades a los autores de las amenazas

El CyberPeace Institute se compromete a respaldar estas recomendaciones mediante:

- **Seguimiento continuo, documentación y difusión de información sobre los ataques a la sanidad y la aplicación o violación de leyes, normas y reglamentos**
- **Recopilación de testimonios de víctimas**
- **Apoyo y desarrollo de iniciativas de ayuda.**

También cooperará con diversos asociados para llevar a cabo análisis de vulnerabilidad y evaluaciones de riesgo de manera que se definan y evalúen con precisión las carencias de recursos humanos, financieros, gubernamentales, técnicos y de seguros necesarios para proteger la compleja y crítica infraestructura sanitaria. Aplicando un marco de responsabilidad determinado, se rastreará y registrará la responsabilidad en el ciberespacio para reducir la amenaza cibernética en el sector sanitario.

El Cyberspace Institute hará una campaña mundial y reunirá a todas las partes interesadas en torno a un objetivo sencillo: que todos los profesionales de la salud, los pacientes y las personas del mundo tengan derecho a beneficiarse de la asistencia sanitaria sin temor ni perjuicio, tanto en tiempos de conflicto como en época de paz.

¿Por qué se ataca al sector sanitario?

Los ataques con motivación financiera y política contra la sanidad aprovechan las vulnerabilidades de la frágil infraestructura digital del sector y las debilidades de su régimen de ciberseguridad.

El sector sanitario ha sido durante mucho tiempo objeto de ataques. Sin embargo, la pandemia de la COVID-19 ha exacerbado si cabe el panorama de amenazas del sector, exponiéndolo a una convergencia de peligros que puede atribuirse a tres factores clave:

- La sanidad se ha convertido en un objetivo escogido para los ataques de extorsión digital desestabilizadores debido a su **responsabilidad de mantener sistemas esenciales que aseguren la salud pública**. El imperativo de satisfacer las necesidades humanas vitales la convierte en un blanco singularmente vulnerable y, por tanto, lucrativo para los ataques de *ransomware*.
- Las organizaciones sanitarias son **depositarias de datos valiosos**. Si bien los historiales médicos se encuentran entre los datos más rentables del mercado negro, ya que se llegan a vender hasta por 250 dólares el expediente, la investigación médica ha demostrado tener un valor estratégico, especialmente durante la pandemia.
- La **posición estratégica** del sector sanitario durante la pandemia de la COVID-19 lo ha colocado en el centro de las rivalidades interestatales. En consecuencia, los Estados competidores han tratado de socavar las respuestas a la pandemia de los Estados rivales atacando la atención sanitaria y la confianza que las personas depositan en ella.

Estas amenazas se ven facilitadas por la **frágil infraestructura digital** del sector y su generalizada **falta de inversión en ciberseguridad**. La sanidad ha sido presionada para adoptar una digitalización rápida, y con ello también una zona de ataque cada vez mayor. Aunque algunas organizaciones sanitarias se han adaptado a estos cambios mediante la implantación de programas de ciberseguridad adecuados, gran parte del sector sigue sufriendo una carencia sistémica de recursos y de personal capacitado que proteja su infraestructura, a menudo compleja y anticuada. El sector seguirá siendo un objetivo preferente y una oportunidad si no se abordan sus vulnerabilidades.

[3] Choi, S. J., Johnson, M. E. and Lehmann, C. U. (2019) 'Data breach remediation efforts and their implications for hospital quality', Health Services Research, 54(5), pp. 971–980. doi: 10.1111/1475-6773.13203.

¿Cuál es el impacto real de los ataques a la sanidad?

Los ataques a la atención sanitaria causan daños directos a las personas y son una amenaza para la salud y la vida a nivel mundial.

La convergencia de los ataques a la infraestructura digital del sector, a su respuesta a la pandemia y a la confianza en la capacidad del sector para funcionar como es necesario está creando una **amenaza mundial para la salud y la vida humana**. Aunque los objetivos de los ataques suelen ser las organizaciones sanitarias o los proveedores de servicios cuyos datos o infraestructuras se han visto comprometidos (incluidos, entre otros, los hospitales y los proveedores de servicios sanitarios, las empresas farmacéuticas y los ministerios de sanidad), las verdaderas víctimas directas de los ataques son los profesionales sanitarios, los pacientes y la sociedad en su conjunto, que sufren a largo plazo. Si bien el fenómeno está poco investigado, los impactos documentados de las amenazas convergentes constituyen una preocupación inmediata y apremiante.

Los ataques contra hospitales y proveedores de servicios médicos tienen un **impacto físico en las personas**. Los hospitales afectados por el *ransomware* se han visto obligados a retrasar las intervenciones quirúrgicas, redirigir las ambulancias que atienden urgencias y volver a realizar procesos que requieren más tiempo. Este tipo de ataques puede repercutir en la capacidad de un hospital para prestar servicios eficientes a largo plazo, como demostró un estudio en el que se observó una mayor tasa de mortalidad entre los hospitales que habían sufrido una filtración de datos en los últimos tres años . En tiempos de la pandemia de la COVID-19, la interrupción de los servicios médicos puede influir negativamente no sólo en el curso de la enfermedad de un paciente, sino también en la propagación del virus.

El impacto psicológico de los ataques es mucho menos visible de forma inmediata pero, sin embargo, causa un sufrimiento importante. Durante un ataque desestabilizador, los profesionales sanitarios experimentan mayores niveles de estrés y ansiedad por encontrarse en una situación de tener que dar respuesta a un incidente, mientras que el miedo y la sensación de coerción, falta de control e impotencia prevalecen cuando se piden rescates. Tras una filtración de datos, la confianza en el sector sanitario se ve erosionada y los pacientes pueden experimentar sentimientos de violación, traición y mayor inseguridad cuando los ciberdelincuentes utilizan los datos sustraídos para perpetrar robos de identidad. A un nivel mucho más amplio, los ataques que afectan a las cadenas de suministro minan la confianza en el entorno técnico del sector sanitario.

Aunque el impacto directo de los ataques a la sanidad puede variar de un incidente a otro, **el impacto social** es muy parecido. Ya sea a través de la violación de registros médicos confidenciales, la interrupción de los servicios médicos o la difusión de desinformación sobre la COVID-19, los ataques contra el sector sanitario generan un **clima de miedo, confusión y desconfianza**. A su vez, esto impide la capacidad de respuesta del sector en tiempos de crisis de salud pública y afecta a la decisión del público de buscar un tratamiento óptimo.

[4] U.S. DoHHS (no date) Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, U.S. Department of Health & Human Services - Office for Civil Rights. Available at: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (Accessed: 17 February 2021).

El impacto comercial y económico de los ataques a la sanidad tiene efectos perdurables durante varios años después del propio ataque y sus costes pueden ser menos tangibles y difíciles de medir. Tras un ataque, las organizaciones sanitarias sufren un proceso de recuperación largo y a menudo de gran magnitud, que requiere financiación de contingencia para restaurar y mejorar sus sistemas, cubrir las sanciones reglamentarias, volver a formar al personal y gestionar el daño a la reputación. En algunos casos, estos costes pueden incluir el pago de un rescate, que se desaconseja encarecidamente por su probabilidad de incitar a demandas extorsivas similares en el futuro, sin garantía de que el pago del rescate produzca el resultado buscado.

¿Cómo se desarrollan y evolucionan los ataques sanitarios?

Los ciberataques aumentan a medida que evoluciona el arsenal de armas utilizadas para atacar la sanidad.

Además del aumento constante de las amenazas cibernéticas a la atención sanitaria acaecido en los últimos años, durante la pandemia de la COVID-19 el mundo ha asistido a una sorprendente intensificación y evolución de tres amenazas cibernéticas clave contra la atención sanitaria:

Los **ataques desestabilizadores** han afectado a la sanidad a nivel mundial; el *ransomware* constituye una amenaza especial debido a su capacidad para prestar servicios sanitarios vitales. Ya sea por casualidad u oportunidad, las operaciones de *ransomware* han evolucionado drásticamente en 2020 gracias a la adopción de tácticas de doble extorsión, que no solo encriptan datos sanitarios sino que también amenazan con filtrarlos. Estas tácticas y su evolución se han visto agravadas por la creciente connivencia entre los autores de ciberdelitos que buscan maximizar su eficiencia y beneficios. Cabe esperar una mayor evolución de este tipo de ataque mediante su amplificación con otros tipos de ataque (por ejemplo, DDoS) o la comercialización de datos sanitarios robados (por ejemplo, la extorsión de sujetos de atención sanitaria o la venta de expedientes médicos). El *ransomware* crea tanto un riesgo inmediato para la atención al paciente como un impacto duradero en las organizaciones sanitarias.

Las **vulneraciones de datos sanitarios** derivadas de ciberataques han aumentado sustancialmente en todo el mundo durante el transcurso de la pandemia, y en Estados Unidos se ha producido un incremento del 39% de 2019 a 2020 . Los cambios propiciados por la pandemia, como el trabajo a distancia y el aumento de la telemedicina debido a las medidas de distanciamiento social, han ampliado sin duda la esfera de amenazas para los datos sanitarios. En concreto, la situación de emergencia mundial ha realzado el valor de los datos relacionados con la COVID-19, tanto financiera como estratégicamente. En consecuencia, la atención sanitaria no sólo está cada vez más en el punto de mira de los ciberdelincuentes que pretenden rentabilizar los datos sanitarios, sino también en el de los actores estatales que buscan obtener una ventaja estratégica en la carrera por la investigación y el desarrollo de vacunas o la capacidad de respuesta ante una pandemia..

Algunas **operaciones de desinformación** se han dirigido a la atención sanitaria tanto directa como indirectamente, con el objetivo de explotar y contribuir a la ambigüedad de la infodemia de la COVID-19. Los actores estatales han robado, manipulado y difundido supuestamente información de organizaciones implicadas en la respuesta a la pandemia o el desarrollo de las vacunas contra la COVID-19. Al manipular y filtrar información auténtica, los autores de amenazas dan credibilidad a sus narrativas de desinformación. Estas operaciones de información facilitadas por medios informáticos amenazan con socavar la confianza de la población en las organizaciones sanitarias y, en última instancia, pueden impedir la respuesta a la pandemia.

¿Quiénes son los principales autores de amenazas?

Los ataques a la sanidad son delitos de bajo riesgo y alta recompensa. Actuando casi con impunidad, los delincuentes y los autores estatales están uniendo sus fuerzas contra la sanidad movidos por distintos motivos y agendas.

El mayor peligro para el sector sanitario lo representan dos tipos de autores de amenazas: los ciberdelincuentes y los actores estatales. La línea que separa a ambos es cada vez más difusa, ya que en los últimos años han aparecido **representantes patrocinados o financiados por el Estado** que actúan en su nombre, lo que complica aún más la atribución de los ataques.

Los **ciberdelincuentes** suponen una amenaza de alto riesgo e impacto para el sector sanitario. Motivados principalmente por el beneficio económico, los ciberdelincuentes, y más concretamente los operadores de *ransomware*, han atacado organizaciones sanitarias durante la pandemia a pesar de haberse comprometido a no actuar contra hospitales. La pandemia de la COVID-19 también ha propiciado un contexto en el que **actores estatales**, a menudo muy sofisticados, tratan de cambiar la realidad de la geopolítica mundial al cometer ataques en los que vulneran, roban, alteran o destruyen información. Desde marzo de 2020, diversos grupos de ciberespionaje patrocinados por el Estado han atacado instalaciones de investigación, desarrollo y ensayo de vacunas en un intento de obtener una ventaja competitiva.

Todos los tipos de autores de amenazas que atacan a la sanidad han podido actuar con casi total impunidad. La tasa de aplicación de la ley y de enjuiciamiento de los perpetradores de ataques contra la asistencia sanitaria es extremadamente baja. Esto se debe, en particular, a que apenas se denuncian los ataques, a la falta de recursos de las fuerzas del orden y del poder judicial y a las deficiencias en la atribución. Además, las oportunidades que ofrecen los instrumentos jurídicos, como la cooperación en materia de investigación, así como los mecanismos de aplicación o las sanciones, rara vez se utilizan de forma sistemática cuando se trata de ciberataques contra la sanidad, y se complican aún más debido a las agendas geopolíticas en el caso de los ataques estatales o patrocinados por el Estado.

¿De qué instrumentos se dispone para proteger la sanidad de los ataques?

Los Estados no están aprovechando todo el alcance de las normas y leyes disponibles para proteger la asistencia sanitaria.

Los ataques al sector sanitario han aumentado considerablemente durante la pandemia de la COVID-19, de forma paralela a la urgencia de la crisis sanitaria, y tienen consecuencias nefastas para el ejercicio de los derechos fundamentales. La reticencia generalizada a aplicar los marcos jurídicos y normativos existentes ha hecho que el sector sea más vulnerable. Se dispone **de muchos instrumentos y oportunidades-** desde la legislación nacional hasta el derecho internacional, pasando por las normas voluntarias no vinculantes- para hacer que los actores de las amenazas se responsabilicen de sus acciones, proteger las infraestructuras críticas y hacer más seguros los productos digitales. Lamentablemente, estas oportunidades también vienen acompañadas de los correspondientes **desafíos**.

En el marco de los procesos de las Naciones Unidas (GEG y GTCA) y las iniciativas de múltiples partes interesadas (por ejemplo, el Llamamiento de París), los gobiernos no han declarado de manera unánime que las instalaciones médicas y sanitarias no deben ser nunca objeto de ataques cibernéticos y han de estar protegidas sistemáticamente contra los mismos. Es más, no se han alcanzado acuerdos internacionales sobre los umbrales definidos para ejecutar los principios del derecho internacional, y no se aplican con regularidad normas voluntarias no vinculantes.

Estos retos acaban por inhibir la capacidad de un Estado para hacer frente a la impunidad en el ciberespacio. Este hecho se ve acentuado por la falta de capacidad de los organismos nacionales encargados de la aplicación de la ley y del poder judicial para actuar ante los casos extraterritoriales. Estos déficits subrayan la necesidad de una mayor responsabilidad y aplicación de la ley en el ciberespacio.

Los actores del sector pueden aplicar mejor las normas de las partes interesadas para proteger la asistencia sanitaria.

Las normas de múltiples partes interesadas, como las propuestas por los Principios del Llamamiento de París, el Acuerdo Tecnológico de Ciberseguridad y la Carta de Confianza, ofrecen iniciativas importantes y útiles sobre cómo los actores del sector pueden proteger mejor la asistencia sanitaria. La aplicación del diseño basado en la seguridad, la notificación de las vulnerabilidades, especialmente las de las infraestructuras críticas, y el fomento de la protección de los usuarios mediante acciones tangibles son medidas oportunas capaces de hacer frente a algunas de las amenazas urgentes contra el sector sanitario. La estandarización de estas normas, a través de marcos vinculantes, contribuiría sustancialmente a ofrecer una protección adecuada a los usuarios, los proveedores de infraestructuras críticas y los suministradores esenciales.

¿Podría un marco sólido de responsabilidad aumentar el comportamiento responsable en el ciberespacio?

Hoy en día no existe ningún mecanismo transparente e independiente para el seguimiento de la responsabilidad en el ciberespacio.

El Cyberspace Institute ha constatado que **corregir las deficiencias existentes en la responsabilidad** es un requisito previo para establecer la ciberpaz y garantizar la protección de las comunidades vulnerables, sobre todo en vista de la actual ausencia de documentación sistemática o de transparencia sobre la forma en que los actores malintencionados transgreden las leyes, las normas y los principios.

Corregir las deficiencias en la responsabilidad implica algo más que la mera atribución. También conlleva delimitar las funciones y responsabilidades de todas las partes interesadas, así como las leyes, normas y principios aplicables necesarios para garantizar la seguridad, la dignidad y la equidad en el ciberespacio. El marco de responsabilidad del Cyberspace Institute propone un modelo en el que las expectativas y los compromisos de todos los interesados en el ciberespacio se confrontan con su nivel de adhesión a estos compromisos y las consecuencias de su incumplimiento.

En la medida en que los productores de software, los fabricantes, las organizaciones sanitarias y los profesionales tengan la responsabilidad de asegurar la infraestructura sanitaria, los Estados serán capaces de operar a través de los niveles técnico, ético, judicial y normativo, y podrán establecer y exigir responsabilidades a través de la regulación y la aplicación de la ley y el orden. Los Estados tienen el poder único y, posiblemente, la responsabilidad de liderar la consecución y el mantenimiento de la ciberpaz en la sanidad. Un marco de rendición de cuentas riguroso y vinculante podría allanar el camino

.

¿Cómo suman sus fuerzas las distintas partes interesadas en apoyo del sector sanitario?

Las iniciativas de ayuda carecen de visibilidad, escala y sostenibilidad.

Al igual que los ciberdelincuentes y otros autores de amenazas han sumado fuerzas para atacar la sanidad, han surgido numerosas coaliciones para protegerla proporcionando un apoyo rápido y gratuito. Entre ellas se encuentran:

- **Iniciativas de resiliencia** para ayudar a las organizaciones sanitarias a prevenir y defenderse de los ataques mediante la concienciación, el intercambio de información y la provisión de herramientas y servicios.

- **Iniciativas de respuesta** para proporcionar conocimientos técnicos y de ciberseguridad en tiempos de crisis que permitan ayudar a investigar la amenaza y asegurar la infraestructura.

- **Iniciativas de apoyo a las víctimas** para ofrecerles asistencia práctica y psicológica tras los ciberataques.

Organizaciones de la sociedad civil, gobiernos, empresas privadas, instituciones académicas, organizaciones internacionales y profesionales de ciberseguridad de todo el mundo, están operando con modelos de asistencia ágiles y específicos, mientras proliferan las redes públicas-privadas, privadas-privadas y de voluntarios. Estas iniciativas han carecido a menudo de visibilidad, escala y sostenibilidad, pero han demostrado que existe una variedad de actores dispuestos a proteger la sanidad y que la **acción colectiva es posible**.

Conclusión

El informe es un esfuerzo inicial para determinar y evaluar los problemas sistémicos de ciberseguridad a los que se enfrenta la sanidad, y el ciberespacio en general. El análisis también ha puesto de manifiesto una laguna existente en la accesibilidad y disponibilidad de datos sobre los ataques a la sanidad, su magnitud e impacto real. Hoy en día no se dispone de una norma mundial para notificar los ataques, recopilar datos sobre los mismos y compartir la información. Asimismo, y podría decirse que como consecuencia, apenas hay investigaciones empíricas acerca del impacto a corto y largo plazo de los ciberataques en la sanidad y la sociedad, especialmente en la atención a los pacientes. **No puede haber respuesta sin conocimiento**. Las recomendaciones que se proponen en este informe pretenden llenar el vacío de conocimientos y el Cyberspace Institute se compromete a impulsar respuestas colectivas a los retos cibernéticos de nuestros días.

Las víctimas de los ataques contra la sanidad son variadas e internacionales, pero no por ello dejan de estar interconectadas. Los autores de amenazas, independientemente de su motivo, están poniendo en peligro vidas y la capacidad general del sector para prestar servicios cruciales. Hacer frente a este problema exigirá cerrar la brecha de la responsabilidad, según la cual esta no recae en una sola entidad, sino en todas las partes interesadas. Mediante una respuesta colectiva y coordinada, la confianza y la seguridad en el sector sanitario prevalecerán sobre el miedo y el daño.

Resumen ejecutivo ingles

Informe