LA CIBERSEGURIDAD EN PRODUCTOS SANITARIOS, UN PILAR FUNDAMENTAL PARA LA PROTECCIÓN DE LOS PACIENTES

Si se acepta el concepto de la cuarta revolución industrial, el presente está caracterizado por la industria 4.0, definida como una tendencia hacia la automatización y el intercambio de datos, en particular dentro de las tecnologías de fabricación y desarrollo. Principalmente incluye los sistemas ciberfísicos, el internet de las cosas (IoT en sus siglas en inglés) y la computación en la nube.

STEFANO DE LUCA,
Consultor de regulación especializado en software como producto sanitario en Episkey Medical Consulting.

PALOMA LÓPEZ GUERRERO,
Directora de comunicación en Episkey Medical Consulting.

La industria 4.0 también se está desarrollando dentro del ámbito de las tecnologías de la salud. En concreto, el Internet de las cosas representa dispositivos con sensores, capacidad de procesamiento, software y otras tecnologías que recogen datos y los intercambian con otros sistemas o dispositivos. En estos últimos años se ha incrementado el número de dispositivos que dan soporte al diagnóstico médico o, incluso, se utilizan para tratar a pacientes o intervenir quirúrgicamente. El Internet de los objetos médicos (IoMT en sus siglas en inglés) puede encontrarse en dispositivos médicos y contribuye a reducir los costes sanitarios y mejorar el nivel de atención a los enfermos crónicos. Estos dispositivos sanitarios necesitan una conexión a internet para su correcto funcionamiento y, de esta manera, pueden acceder a una enorme cantidad de datos que pueden ayudar a tomar decisiones, vigilar y alertar de situaciones inseguras y agilizar la atención al paciente.

Todos estos dispositivos, una vez conectados a la red, presentan una oportunidad para que una parte malintencionada acceda a los sistemas del hospital, ya sea para obtener datos personales con fines financieros, políticos, o para atacar directamente los sistemas y provocar una monitorización errónea o alterar la configuración de cualquier dispositivo. El historial de un paciente contiene una enorme cantidad de información, desde datos demográficos y de contacto hasta información médica confidencial, datos financieros, de seguros y de la seguridad social, documentos de identidad y recetas médicas. Esta información vale hasta 10 veces más que la información de las tarjetas de crédito (Cartwright, 2023).

Como ejemplo, en 2017, la información difundida por algunos medios de comunicación puso de relieve más de 8600 de las denominadas "vulnerabilidades" contenidas en un único marcapasos, lo que obligó al fabricante a revisar y actualizar el software de 460.000 de sus dispositivos (IData Research).

Aunque su grado de seguridad varía debido a los diferentes requisitos normativos en la comercialización de productos específicos, algunas vulnerabilidades son

compartidas por todas las soluciones. Entre ellas se incluyen las limitaciones derivadas del diseño de los dispositivos, las políticas de los fabricantes y los riesgos específicos del entorno en el que operan (Greser, 2023).

La potencial vulnerabilidad de estas herramientas a los ciberataques puede tener implicaciones para el ámbito sanitario que van mucho más allá de un intento de pirateo en las redes sociales. Este artículo aborda la ciberseguridad demostrando cómo pueden mitigarse los riesgos de amenazas mediante requisitos normativos.

En la Unión Europea (UE) y en los Estados Unidos de América (EE. UU.), las autoridades competentes regulan rigurosamente la ciberseguridad de estos dispositivos médicos.

EE. UU.

En marzo de 2023, La Administración de Alimentos y Medicamentos de Estados Unidos (*Food and Drug Administration*, FDA en sus siglas en inglés) publicó un conjunto de directrices actualizadas sobre ciberseguridad de los dispositivos médicos: *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions.*

Hasta ese momento, solo existían normas de seguimiento post-comercialización de un dispositivo; simples avisos y retiradas que obviaban la gestión preventiva de riesgos, y su impacto en la salud del paciente. Los protocolos para la seguridad del ciclo de vida del dispositivo ni siquiera se contemplaban. A menudo, el fabricante no daba soporte a la versión usada, o no desarrollaba las actualizaciones pertinentes (denominada deuda tecnológica). Además, aunque los usuarios rechazaran ciertas actualizaciones, como las del software de un teléfono o un ordenador, algunas de ellas se "forzaban" sin poderlas retrasar o eliminar. Desafortunadamente, estas actualizaciones se debían a importantes fallos de seguridad identificados por el fabricante.

Los nuevos requerimientos

Todos los fabricantes deben facilitar, en su solicitud inicial para la venta en EE. UU., un plan exhaustivo de gestión de riesgos de ciberseguridad para abordar, en un plazo razonable, las vulnerabilidades y las amenazas posteriores a la comercialización. Sin embargo, no solo se debe destacar la gestión razonable de la seguridad a lo largo de todo el ciclo de vida del producto, sino que se debe proporcionar una descripción completa de los procesos de diseño, desarrollo y mantenimiento que garanticen la seguridad del producto en caso de vulnerabilidades críticas. Además, los fabricantes deben incluir una lista de materiales de software (*Software Bill of Materials*, SBOM en sus siglas en inglés) y otro software de código abierto y de terceros, firmware y binarios, recursos en la nube e interfaces de programación de aplicaciones (*Application Programming Interface*, API en sus siglas en inglés), acordes con los elementos mínimos de la Administración Nacional de Telecomunicaciones e Información del Gobierno de Estados Unidos (*U.S. Government's National Telecommunications and Information Administration*, NTIA en sus siglas en inglés).

Implicaciones jurídicas

Las guías de la FDA no establecen responsabilidades jurídicamente exigibles, sino que deben considerarse sólo como recomendaciones, a menos que se citen requisitos reglamentarios o legales específicos. Sin embargo, desde el día 1 de octubre de 2023, la FDA ha emitido ya

las primeras cartas de rechazo de aceptación (Refuse to Accept, RTA en sus siglas en inglés) de aquellas solicitudes que no cumplieran los nuevos requisitos de ciberseguridad. Además, si el dispositivo se desconecta, o se pierden datos de los pacientes, los fabricantes están sujetos a la ley de Portabilidad y Responsabilidad de Seguros Médicos (Health Insurance Portability and Accountability Act, HIPAA en sus siglas en inglés), o a la norma de infracción de la Comisión Federal de Comercio (Federal Trade Commission, FTC en sus siglas en inglés).

Para evitar estos imprevistos, la FDA ha desarrollado un manual de preparación y respuesta ante incidentes de ciberseguridad y el manual de modelado de amenazas en dispositivos médicos. Una documentación detallada es la mejor defensa de un fabricante a medida que se mueva por el campo minado de la ciberseguridad.

UE

La ciberseguridad de los productos sanitarios se ha convertido en una de las mayores preocupaciones de los legisladores médicos. Los riesgos de ciberseguridad se abordan en diversas leyes que se centran específicamente en los datos, la inteligencia artificial (IA) y las normas sectoriales (incluidas las específicas del sector sanitario).

El Reglamento Europeo de Productos Sanitarios 2017/745 (*Medical Device Regulation*, MDR en sus siglas en inglés) es la legislación que detalla los requisitos esenciales de seguridad y funcionamiento que deben cumplir los fabricantes para comercializar productos sanitarios en la UE. Estos requisitos, pertinentes desde el punto de vista de la ciberseguridad, se complementan con los del Grupo de Coordinación de Productos Sanitarios (*Medical Device Coordination Group*, MDCG en sus siglas en inglés), un organismo creado por la misma Comisión Europea para orientar sobre la regulación de este sector.

Junto con el Reglamento, la Directiva NIS2 establece medidas de gestión de riesgos de ciberseguridad y obligaciones de información para las entidades incluidas en su ámbito de aplicación.

Finalmente, el Reglamento General de Protección de Datos o Reglamento 2016/679 (*General Data Protection Regulation*, GDPR en sus siglas en inglés) contiene normas para el tratamiento seguro de los datos personales que establecen el principio de integridad y confidencialidad del tratamiento. El incumplimiento del GDPR, dependiendo de las circunstancias del caso, puede estar sujeto a multas administrativas de hasta 10.000.000 (€) de euros o hasta el 2% de la facturación anual global del ejercicio financiero anterior de la empresa.

La norma internacional IEC 81001-5-1: 2022, ya ratificada por la Asociación Española de Normalización en marzo de 2022, establece los requisitos de seguridad para el software sanitario. Se trata de una norma de procesos esencial para todo el ciclo de vida de la ciberseguridad. Sin embargo, las pruebas de penetración y *fuzzing*, ambas fundamentales para llevar a cabo una sólida estrategia de ciberseguridad, se describen solo de manera superficial.

Los auditores han emitido los primeros veredictos: diagramas inadecuados de arquitectura o de diseño del software, una gestión poco sistemática de los riesgos de ciberseguridad, pruebas de penetración malas o ausentes, y conocimiento insuficiente de los conceptos de seguridad son los errores que se deben evitar para enfrentar los desafíos asociados a la construcción de un modelo sanitario de mejor calidad, y realmente centrado en el paciente.

Las ciberamenazas a los dispositivos IoMT constituyen un auténtico reto para todas las partes interesadas. La cuestión de la ciberseguridad en la agenda de la regulación tanto de la Comisión Europea como de la FDA abarca este tipo de productos. Una normativa adecuada puede aumentar su seguridad y conducir a una mejor protección. En el caso de los productos sanitarios, los requisitos para los fabricantes derivan del MDR y el IVDR para los dispositivos comercializados en la Unión Europea.

En vista de los retos que plantea los dispositivos IoMT para los pacientes y usuarios, los trabajos relativos a este asunto deben tener la máxima prioridad para los organismos reguladores. Un retraso en la redacción de normas y reglamentos puede repercutir negativamente en el nivel de ciberseguridad. Desde el punto de vista de los fabricantes, es muy recomendable realizar una adecuada estrategia de regulación en la que la ciberseguridad tenga una posición esencial, de manera que se pueda comercializar el producto de la manera más segura para el paciente.

Referencias

• Cartwright, A. J. (2023). The elephant in the room: cybersecurity in healthcare. Journal of Clinical Monitoring and Computing, 37(5), 1123–1132. https://doi.org/10.1007/s10877-023-01013-5

• Greser, J. (2023). A step forward in health-related IoT cybersecurity: remarks on the proposal for a liability for defective products directive. Frontiers in Digital Health, 5, 1193255. https://doi.org/10.3389/fdgth.2023.1193255

• iData Research. Firmware Update to Address Cybersecurity Vulnera-bilities Identified in Abbott's (formerly St. Jude Medical's) ImplantableCardiac Pacemakers: Comunicación de seguridad de la FDA. 2017. Disponible en: https://idataresearch.com/firmware-update-address-cybersecurity-vulnerabilities-identified-abbotts-formerly-st-jude-medicals-implantable-cardiac-pacemakers-fda-safety-communication/.[fecha de acceso: 30 de noviembre de 2022].

• Directiva NIS2: Link: https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/aprobacion-directiva-nis2