La Internet de las Cosas en la atención sanitaria: oportunidades y riesgos

Este informe defiende que los fabricantes deben integrar la seguridad en los dispositivos desde el principio, y no como idea tardía.

La Internet de las Cosas está ganado terreno rápidamente en la experiencia de consumo y la economía global, pero también puede ser profundamente personal. En el mundo de la atención sanitaria, los dispositivos médicos en red se están integrando en el tejido de la Internet de las Cosas: dispositivos que se llevan puestos, se ingieren temporalmente o incluso se introducen en el cuerpo humano para tratar enfermedades, administrar medicamentos y mejorar la salud y el bienestar generales.

Este informe, patrocinado por Intel Security y elaborado por Atlantic Council, explora los retos para la seguridad y las oportunidades sociales que existen para los dispositivos médicos en red. Hace recomendaciones a los fabricantes, los organismos reguladores y los profesionales de la salud para maximizar el valor que tienen para los pacientes y, a la vez, reducir los retos para la seguridad que tienen su origen en el software, el firmware y las comunicaciones de esos dispositivos.

Oportunidades

Llevamos puestos dispositivos conectados a redes para saber más de nosotros mismos, de nuestras dietas, programas de ejercicio y signos vitales. Los médicos son capaces de ajustar y optimizar dispositivos implantados como los marcapasos con mayor rapidez y precisión, sin tener que utilizar procedimientos médicos invasivos. En los hospitales, nuevos dispositivos se conectan a las redes para que la monitorización y los tratamientos sean más eficaces y menos costosos. Según una estimación, estas tecnologías podrían ahorrar 63 000 millones de dólares en los costes de la atención sanitaria durante 15 años, con una reducción del 15 % al 30 % en los costes de los equipos médicos.[1]

Este informe llama la atención sobre el delicado equilibrio que existe entre la promesa de una nueva era tecnológica y la capacidad de la sociedad para proteger los cimientos tecnológicos y de comunicaciones de estos innovadores dispositivos.

Reducción de los riesgos potenciales

Las ventajas de la atención sanitaria conectada implican también cuatro áreas de preocupación que se solapan. Una de ellas son los fallos fortuitos, que erosionan la confianza. Si se produjeran fallos de gran impacto, la sociedad opondría resistencia a utilizar dispositivos médicos conectados a las redes, lo que retrasaría su despliegue en años o décadas. La protección de la privacidad e información sanitaria confidencial de los pacientes es la segunda preocupación, ya que los hackers consideran que la información sanitaria es particularmente valiosa. La encuesta de PwC sobre el estado global de la seguridad de la información "Global State of Information Security Survey 2015" muestra que los incidentes relacionados con la seguridad de la información que denuncian financiadores y proveedores del sistema sanitario aumentaron un 60 % en 2014, y se incrementó casi el doble en comparación con los incidentes que se produjeron en otros sectores.[2]

Las interrupciones intencionadas también son un motivo de preocupación dado que los dispositivos médicos conectados a las redes son tan vulnerables como cualquier otra tecnología en red. Los hacktivistas, ladrones, espías e incluso los terroristas van detrás de las vulnerabilidades de la tecnología para cometer delitos y causar estragos. Cuando un dispositivo de red se conecta a una persona, las consecuencias de los ciberdelitos cometidos utilizando ese dispositivo podrían ser especialmente personales y amenazantes. Los ataques dirigidos contra las personas con la intención de hacer daño físico son poco probables. Sin embargo, hay una alta probabilidad de que se produzcan ataques que podrían causar interrupciones generalizadas. En teoría, un malware dirigido podría extenderse a través de Internet, y afectaría a todos quienes tuvieran un dispositivo vulnerable. Tal escenario se ha materializado en sistemas empresariales de TI y sistemas de control industrial, como puso de manifiesto el sofisticado ataque Stuxnet.

Actualmente, la atención del desarrollo y producción de dispositivos médicos se centra en las preferencias de los fabricantes y las necesidades de los pacientes. Los fabricantes y la Administración Pública deben también dirigir la atención a la implementación de un conjunto de estándares de seguridad o de prácticas recomendadas globales para que los dispositivos conectados a las redes puedan responder a los riesgos subyacentes.

Varias recomendaciones ayudarán a impulsar la innovación y, a la vez, reducir los riesgos para la seguridad. Este informe defiende que los fabricantes deben integrar la seguridad en los dispositivos desde el principio, y no como idea tardía. Como declaró Stuart McClure, exdirector de tecnología de McAfee, ante el Comité de Seguridad Interior del Congreso de EE. UU. en 2012, "La ciberseguridad tiene que incorporarse a equipos, sistemas y redes en la etapa inicial del proceso de diseño".[3]

Normativas en evolución

El informe recomienda implementar mejoras continuas con la colaboración del sector privado y de los sectores privado y público. De esta forma se logra una mayor coordinación y no más cantidad de normativas. Los organismos reguladores no siempre van al ritmo de los avances tecnológicos. Necesitan recibir comentarios de todas las partes interesadas en foros transparentes y de cooperación que salvaguarden la función independiente de esos organismos y evitar así que surjan dudas por connivencia con los fabricantes. De la misma forma, los fabricantes deben continuar mejorando la comunicación entre ellos.

El informe también recomienda un cambio evolutivo del paradigma de aprobación de las normativas en materia de dispositivos médicos para, de esta forma, incentivar la innovación. Además, permitiría que las organizaciones que prestan servicios sanitarios cumplieran los objetivos de las directivas y protegieran el interés general.

Algunos fabricantes de dispositivos médicos siguen utilizando tecnologías antiguas y se resisten a introducir innovaciones porque saben que las tecnologías antiguas obtendrán las aprobaciones de los organismos reguladores. Un proceso de aprobación más sencillo podría solucionar este problema. Un proceso mejorado debería impulsar la seguridad integrada en el diseño y, como mínimo, la posibilidad de aplicar parches a los sistemas después de desplegarlos.

Por último, el informe recomienda que exista una voz independiente que represente a los ciudadanos, especialmente a pacientes y sus familiares, como forma de buscar el equilibrio entre la efectividad, la facilidad de uso y la seguridad de los dispositivos que se implementen.

Más información

Lea el informe completo. Descargue *La Internet de las Cosas en la atención sanitaria: oportunidades y riesgos*.

Acerca de Intel Security

La tecnología tiene la capacidad de enriquecer nuestra vida, de transformar cómo vivimos y trabajamos. Pero cuanto más se integra la tecnología en nuestra vida, más debe integrarse la seguridad en la tecnología. Combinando la experiencia en seguridad de McAfee con la innovación, el rendimiento y la confianza en Intel, esa idea se está haciendo realidad. La seguridad está integrada en el diseño, integrada y siempre activa en todos los dispositivos, en todas las capas de los sistemas informáticos. Protege la valiosa propiedad intelectual, datos, dispositivos y la identidad. Por tanto, nuestra vida digital, personal y laboral, está segura. Por eso llamamos a nuestra estrategia "Security Connected" (seguridad conectada). Está presente en todas las arquitecturas, en todas las plataformas, desde el chip a la nube, desde smartphones y tablets a PCs, servidores, etc. La seguridad deja de ser discreta para integrarse de forma que esté tan generalizada como los propios ordenadores. Como primer paso, la seguridad de dispositivos móviles será gratuita en cualquier plataforma, en todo el mundo. Es el comienzo de un viaje lleno de posibilidades.

McAfee forma parte de Intel Security. Gracias a su estrategia Security Connected, la seguridad por hardware mejorada y el exclusivo sistema de información sobre amenazas Global Threat Intelligence, Intel Security desarrolla soluciones y servicios de seguridad proactivos y demostrados para proteger sistemas, redes y dispositivos móviles propiedad de las empresas o de uso personal, en todo el mundo. www.intelsecurity.com.

Acerca de Atlantic Council

Atlantic Council es una organización independiente que promueve el liderazgo y compromiso constructivos de EE. UU. en asuntos internacionales, basados en el papel esencial que la comunidad del Atlántico juega en la respuesta a los retos globales de hoy día. Para obtener más información, visite: **http://www.AtlanticCouncil.org**.

1. Peter C. Evans y Marco Annunziata, "Industrial Internet, Pushing the Boundary of Mind and Machines" (Internet industrial, más allá de los límites de la mente y las máquinas), **http://www.ge.com/sites/default/files/Industrial_Internet.pdf**, extraído de la ficha técnica NIST Cyber-Physical Systems Factsheet, **http://www.nist.gov/public_affairs/factsheet/cyberphysicalsystems2015.cfm**
2. **http://usblogs.pwc.com/cybersecurity/the-prognosis-for-healthcare-payers-and-providers-rising-cybersecurity-risks-and-costs/**
3. Declaración de Stuart McClure ante el Congreso de los Estados Unidos, Comité de Seguridad Interior, Subcomité de Supervisón, Investigaciones y Gestión, 24 de abril de 2012.

McAfee. Part of Intel Security.
Avenida de Bruselas n.º 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8500
www.intelsecurity.com