Publicado en Madrid el 10/01/2024

Check Point Software alerta de los riesgos de los dispositivos IoT en la Sanidad: el 70% de los dispositivos médicos no cuentan con soporte

Los dispositivos IoT en el sistema sanitario están revolucionando la atención médica con numerosas innovaciones. En los hospitales se emplean para gestionar la energía, controlar los accesos, atender las condiciones de los quirófanos, para dirigir los sistemas de alarma contra incendios, entre otras muchas más medidas

El Internet de las Cosas Médicas (IoMT) ha revolucionado la industria de la salud. Los hospitales pueden mejorar la atención a los pacientes, reducir los costes y ser más eficaces empleando estos recursos tecnológicos. Las opciones para implementar IoMT en los hospitales son numerosas, desde servicios robóticos con los que se extrae sangre y se desinfectan los hospitales, hasta camas conectadas que son capaces de monitorizar el estado del paciente, su nivel de oxígeno, de sangre, automatizar la entrega de la medicina, alertas médicas, etc.

Check Point Research, la división de Inteligencia de Amenazas Check Point® Software Technologies Ltd. (NASDAQ: CHKP), un proveedor líder especializado en ciberseguridad a nivel mundial, ha detectado que la seguridad de estos dispositivos está desatendida y esto conlleva riesgos perjudiciales para el sistema sanitario.

Dificultades que entraña el IoMT

Asegurar los dispositivos IoT es complejo por la amplia gama de protocolos de comunicación que emplean y sus vulnerabilidades derivadas de sistemas operativos heredados, contraseñas débiles, dificultades de parcheo, accesibilidad física, configuraciones incorrectas del sistema operativo, falta de medidas de seguridad incorporadas y protocolos de comunicación no seguros.

Por ejemplo, muchos dispositivos IoMT continúan operando en la plataforma Windows 7. Esto supone una gran vulnerabilidad, dado que Microsoft ni siquiera continúa ofreciendo soporte para estos sistemas operativos y actualizar estos dispositivos supone un gran coste. Las estimaciones indican que el 70% de los dispositivos médicos no cuentan con soporte.

Otra de las grandes dificultades está relacionada con el uso de la tecnología SCADA, un sistema utilizado para supervisar y controlar dispositivos en tiempo real. En los hospitales se emplean para gestionar la energía, controlar los accesos, atender las condiciones de los quirófanos, para dirigir los sistemas de alarma contra incendios, entre otras muchas más medidas. Sin embargo, estos sistemas emplean contraseñas predeterminadas o fáciles de adivinar, por lo que se vuelven objetivos fáciles para los atacantes.

La necesidad de certificar los IoMT

La certificación es esencial para asegurar que los dispositivos médicos de IoT cumplan con los estándares regulatorios necesarios y con los requisitos de la industria de la salud. Así, se garantiza que los dispositivos estén diseñados con precisión, construidos con controles de calidad apropiados y tengan un rendimiento confiable. El proceso de certificación implica una serie de evaluaciones realizadas por autoridades regulatorias relacionadas con los siguientes temas:

Defender los dispositivos: la desprotección de estos dispositivos puede conllevar implicaciones financieras significativas debido a brechas de datos, juicios y penalidades regulatorias, consecuentes de los ciberataques. Es fundamental que los proveedores de atención médica inviertan en sistemas de seguridad integrales para mitigar estos riesgos y salvaguardar la estabilidad financiera. Por ello, deben ser evaluados por seguridad eléctrica, de software y mecánica, asegurando que no presenten ningún peligro para pacientes u operadores.

El paciente como prioridad: los ataques ransomware se han vuelto una preocupación significativa en los últimos años, ya que pueden comprometer los datos sensibles almacenados en los IoT, causando interrupciones y posibles daños a los pacientes. La industria de la salud debe implementar protocolos de seguridad estrictos para minimizar el riesgo de los ataques ransomware y proteger la integridad de los registros médicos. La protección de datos en este campo es crucial. Los dispositivos deben contar con medidas apropiadas para salvaguardar la privacidad de la información, prevenir el acceso no autorizado y mantener su integridad.

Normativa como bandera: los dispositivos IoMT deben cumplir con regulaciones y estándares aplicables. Asimismo, su certificación puede conllevar ciertas complicaciones debido a que las actualizaciones pueden enfrentar la necesidad de volver a certificarlo. Este procedimiento es muy costoso, por lo que muchos dispositivos IoT quedan desactualizados y sin parches.

Conectividad e interoperabilidad: en un ecosistema de atención médica conectada, la interoperabilidad es la clave. Los dispositivos deben ser compatibles entre sí y cumplir con ciertos protocolos de comunicación.

Rendimiento: los dispositivos deben demostrar precisión, exactitud y confiabilidad en sus mediciones.

"El uso de los dispositivos IoMT supone una gran innovación en la industria de la salud, ya que mejoraría considerablemente la atención a los pacientes. Sin embargo, para que esta práctica sea totalmente beneficiosa no puede desatenderse el sistema de seguridad de estos dispositivos", explica Eusebio Nieva, director técnico de Check Point Software para España y Portugal. "Unos dispositivos IoT desprotegidos suponen una puerta de entrada muy fácil para los atacantes, que conllevaría graves consecuencias para los pacientes y la industria".

Datos de contacto:
Everythink PR
Everythink PR
91 551 98 91

Nota de prensa publicada en: Madrid

Categorías: Nacional Medicina Madrid Emprendedores Software Ciberseguridad Dispositivos móviles Innovación Tecnológica