Cuidado, los marcapasos también pueden hackearse

Publicado el: 05-04-2018

¡Cuidado! Los dispositivos médicos, incluidos los dispositivos electrónicos cardiovasculares implantables como los marcapasos o desfibriladores, pueden ser hackeados, como ocurre con el resto de los dispositivos electrónicos, como móviles, tablets u ordenadores. En un estudio publicado por Colegio Estadounidense de Cardiología en «Journal of the American College of Cardiology», advierte de este riesgo y propone algunas medidas para mejorar la ciberseguridad en estos dispositivos.

La ciberseguridad en el campo médico se refiere a la integración de dispositivos médicos, redes de computadoras y software. Si bien no ha habido informes clínicos reales de piratería maliciosa o inadvertida o ataques de malware que afecten a dispositivos cardíacos, recientemente se ha descubierto esta posibilidad. Las razones para hackear los dispositivos médicos incluirían motivos políticos, financieros, sociales y personales. Y los dispositivos pueden ser pirateados local o remotamente.

«La verdadera seguridad cibernética comienza cuando se diseña un software protegido desde el principio, y requiere la integración de múltiples partes interesadas, incluidos expertos en software, expertos en seguridad y asesores médicos», explica Dhanunjaya R. Lakkireddy, del Hospital de la Universidad de Kansas (EE.UU.) y autor del artículo.

Lo cierto es que los dispositivos médicos han sido objeto de piratería durante más de una década. El número cada vez mayor de dispositivos médicos que usan software ha creado la necesidad de proteger los dispositivos contra la interferencia dañina intencional en su funcionamiento normal. Las comunicaciones inalámbricas avanzadas entre los proveedores de atención médica y los dispositivos de los pacientes han creado la posibilidad teórica de desactivar las funciones, alterar la programación y retrasar, interferir o interrumpir las comunicaciones.

Hay una serie de posibles consecuencias clínicas que pueden resultar de la piratería de un dispositivo cardíaco. En pacientes con marcapasos, las preocupaciones consisten principalmente en sobredetección o agotamiento de la batería. Para los pacientes con desfibiriladores implantables, es posible que los hackers interrumpan las comunicaciones inalámbricas, lo que inhibe el valor de la telemonitorización y permite que el sistema no detecte ningún evento clínicamente relevante. La sobredetección puede inhibir la estimulación o dar lugar a descargas inapropiadas o potencialmente mortales. El agotamiento de la batería puede provocar que un dispositivo no pueda administrar terapias durante arritmias potencialmente mortales.

Redes hospitalarias

«En este momento, no hay evidencia de que una persona ajena pueda reprogramar un dispositivo electrónico cardiovascular implantable o cambiar la configuración del dispositivo», señala Lakkireddy. «La probabilidad de que un pirata informático individual afecte con éxito a un dispositivo electrónico implantable cardiovascular o sea capaz de dirigirse a un paciente específico es muy baja. Un escenario más probable es un ataque de malware o ransomware que afecte la red de un hospital e impida la comunicación».

¿Cómo afrontar el problema? Según el estudio, la ciberseguridad deberían abordarse durante las

pruebas de productos, tanto antes como después del mercado. Debido a que las vulnerabilidades cibernéticas pueden surgir rápidamente, se deben implementar procesos sólidos de post-mercado para monitorizar el entorno en busca de nuevas vulnerabilidades y responder de manera oportuna. Por ejemplo, sugieren, el firmware puede ser útil en dispositivos con posibles vulnerabilidades. Los médicos que manejan dispositivos cardíacos deben conocer los riesgos documentados y posibles de ciberseguridad. Deben establecerse sistemas para comunicar las actualizaciones en estas áreas de forma rápida y comprensible al resto del equipo clínico que administra pacientes con dispositivos.

«Dada la falta de evidencia de que el hackeo de dispositivos cardíacos es un problema clínico relevante, junto con la evidencia de los beneficios de la monitorización remota, se debe tener precaución al privar al paciente de los claros beneficios del monitorización remota», dijo Lakkireddy.

Fuente: https://netsaluti.com