Cuando se habla de salud, aceptar riesgos no es una opción

En el anterior artículo pudimos ver como los dispositivos médicos pueden manipularse para administrar dosis fatales de insulina, para robar datos de pacientes o incluso para directamente dejarlos inoperativos. Estos escenarios no son ciencia ficción. Son muy reales y cada vez son más los dispositivos médicos como marcapasos, bombas de insulina o máquinas de resonancia magnética vulnerables a sufrir ataques.

Mientras investigaba me he encontrado con un artículo [1] en el cual se recoge como varios investigadores emularon el funcionamiento de un dispositivo médico en un sistema de señuelo. En el transcurso de seis meses, los malhechores se conectaron con éxito en más de 55.000 ocasiones al sistema e instalaron más de 300 malwares. Esto refleja lo expuestos que estamos ante este tipo de ataques. Los dispositivos médicos están constantemente en peligro de ser comprometidos y es por ello que todo lo expresado hasta este post cobra especial relevancia.

Cuando hablamos de temas tan sensibles como es el caso de la salud de las personas, aceptar los riesgos no es una opción.

¿Y entonces qué hacemos?

Tenemos que gestionar dichos riesgos. La seguridad del paciente debería ser ante todo la prioridad de todos los fabricantes de dispositivos médicos.

Esta gestión, además, no resulta opcional sino que es un requisito reglamentario en todo el mundo. La FDA de los EE.UU. lo exige en el Reglamento del Sistema de Calidad. Europa, a su vez, lo requiere en el nuevo Reglamento de Dispositivos Médicos.

Asimismo, Japón, Canadá, Australia, Brasil y todos los demás mercados importantes también requieren la aplicación de la gestión de riesgos, a la cual se hace referencia en sus reglamentos nacionales o en la norma **ISO 13485:2016**. [2] Esta norma internacional respalda la obligación de los fabricantes de asegurarse de que los productos cumplen sistemáticamente los requisitos normativos aplicables y las exigencias del cliente. [3]

Sin embargo, todos ellos se rigen por la norma **ISO 14971**, norma mundial para la gestión de riesgos de los dispositivos médicos. Esta norma aprobada por la FDA, especifica el proceso de gestión de riesgos mediante el cual un fabricante puede identificar los peligros asociados con su dispositivo médico, estimar y evaluar los riesgos, **controlar** estos riesgos y supervisar la eficacia de los controles a lo largo del ciclo de vida del producto. [4]

Parece fácil, ¿verdad? No obstante, la realidad es que la gestión de riesgos es uno de los aspectos más complejos del cumplimiento de las regulaciones.

En este post, en concreto, nos vamos a centrar en los controles para mitigar los riesgos asociados a este tipo de dispositivos.

¿Pero qué es un control?

Un control es un proceso en cual se toman decisiones y se aplican medidas que permiten reducir los riesgos a niveles especificados.

Para cada uno de los riesgos es necesario estimar el **grado de impacto** así como la **probabilidad** de que este ocurra. A partir de estos valores se puede estimar si el riesgo resulta crítico, moderado o bajo pudiendo detectar aquellos riesgos sobre los cuales deberemos aplicar controles. [5]

¿Os acordáis de los riesgos que mencionamos en el anterior artículo?

Los hemos mencionado un poco antes: accesos no autorizados, ataques contra la disponibilidad, robo de datos, cambio de ajustes de configuración, software y firmware no probado o defectuoso …

Ahora vamos a intentar establecer una serie de controles para mitigar dichos riesgos: [6][7]

- **Establecer controles de acceso:** Consiste en limitar el acceso al dispositivo médico conectado a través de técnicas como la doble autenticación, uso de tecnologías NFC, establecimiento de contraseñas,… Este tipo de medidas permiten reducir el número de accesos no autorizados, reduciendo de esta forma también las posibilidades de sufrir un robo de datos. Sin embargo, este tipo de medidas pueden resultar polémicas en determinados casos: ¿Establecemos una contraseña de acceso en un marcapasos? De esto hablaremos un poco más adelante.
- **Realizar actualizaciones periódicas:** Es necesario aplicar parches de seguridad al dispositivo médico con frecuencia de acuerdo con las pautas posteriores a la comercialización emitidas por la FDA.
- **Aplicar estándares de codificación:** Muchos ciberataques exitosos han explotado vulnerabilidades presentes en el código que no han sido probadas rigurosamente antes de su implementación en un entorno activo. Una de las normas más importantes de la industria es la emitida por la Comisión Electrotécnica Internacional (IEC), IEC 62304. Este estándar proporciona una serie de características robustas sobre cómo desarrollar mejor el código.
- **Aplicar la seguridad mediante el diseño:** Es fundamental la gestión adecuada del ciclo de vida del dispositivo médico. Tener en cuenta la seguridad desde el primer momento en el cual se va a diseñar el dispositivo resulta fundamental.
- **Hacer uso de canales de comunicación cifrados:** Los dispositivos deberían hacer uso de canales de comunicación debidamente encriptados a fin de comunicarse con el mundo exterior.

Pero los controles no solo se deben establecer, estos a su vez deben ser **auditados**. Realizar auditorías periódicas de los procesos y de la tecnología ayuda a identificar las amenazas y permite mitigar los riesgos. Esta labor recae sobre los **auditores,** es decir las personas responsables de velar por la cumplimentación de las regulaciones correspondientes y de evaluar los procedimientos llevados a cabo por la organización.

Cuando se trata de auditorías de dispositivos médicos, las **pruebas de**

penetración son un enfoque recomendado. Estas pruebas ayudan a evaluar lo fácil que es para los hackers violar la seguridad de los dispositivos para obtener recursos tales como datos, interrumpir operaciones o modificar sistemas que podrían afectar la salud del paciente.

Además, establecer controles no solo implica establecer iniciativas que solucionen el problema. Debemos ser conscientes también del ámbito en el cual se aplican. El otro día me enviaron una noticia en la cual el titular decía "Investigadores muestran la relación entre las brechas de datos y las tasas de mortalidad hospitalaria". [8] Al principio pensé que la relación entre ambos factores sería las consecuencias generadas por el ataque. Sin embargo, la relación que establecía el estudio yacía en las contramedidas aplicadas por los hospitales y su consecuente aumento en los tiempos de atención a los pacientes.

Al final intentamos blindar los dispositivos y se nos olvida que en este sector en concreto se necesita de dispositivos seguros y efectivos pero que a su vez resulten rápidos en caso de emergencia. Imaginaros un médico que tuviera que estar introduciendo una contraseña mientras el paciente se está muriendo.

¿Y qué pasaría si al profesional sanitario se le ha olvidado la contraseña?

Somos humanos, estas cosas pueden pasar. Desde un punto de vista tecnológico esto supone un reto ya que cualquier mala implementación posee como resultado lo mencionado en el artículo, un aumento en la tasa de mortalidad.

Es por ello que se debe establecer una alineación entre las medidas aplicadas y el ámbito del mismo. ¿De que sirve blindar un dispositivo si en caso de emergencia no podemos acceder a él? ¿Tal vez tengamos que hacer uso de nuevas tecnologías? Y estas tecnologías a su vez, ¿ qué riesgos presentarían?

Muchas preguntas a contestar cuyas respuestas no resultan sencillas. Sin embargo lo que sí sé es que necesitamos dispositivos seguros, efectivos y alineados con el trabajo que realizan los profesionales del sector. En el momento en que se consiga alcanzar todo ello será cuando este sector alcance su máximo esplendor, pudiendo todos los ciudadanos aprovechar las ventajas que nos aporta la tecnología sin miedo a que nuestra vida corra peligro.

Y hasta que el post de hoy.

Referencias

[1] <<Closing the Gap in Medical Device Cybersecurity>>, Knowledge Leader, acceso el día 22 de noviembre del 2019, https://www.knowledgeleader.com/knowledgeleader/content.nsf/web+content/hotissueclosingthegapinmedicaldevicecybersecurity

[2] <<ISO 14971 and the Basics of Medical Device Risk Management Explained>>, Oriel, acceso el día 22 de noviembre del 2019, https://www.orielstat.com/blog/iso-14971-basics-explained/

[3] <<ISO 13485 Certificación para los productos sanitarios>>, Lloyd's register, acceso el día 23 de noviembre del 2019, https://www.lr.org/es-es/iso-13485/

[4] <<Case study – Risk management for medical devices (based on ISO 14971)>>, IEEE Xplore, acceso el día 20 de noviembre del 2019, https://ieeexplore.ieee.org/document/5754492

[5] <<The definitive guide to ISO 14971 risk management for medical devices>>, Green Light, acceso el día 22 de noviembre del 2019, https://www.greenlight.guru/blog/iso-14971-risk-management

[6] <<The Internet of Medical Things – Anticipating the Risk>>, ISACA, vol 4 (2019): 27-32

[7] <<Medical device cyber security guidance for industry>>, Australian Government, acceso el día 22 de noviembre del 2019, https://www.tga.gov.au/sites/default/files/medical-device-cyber-security-guidance-industry.pdf

[8] <<Researchers Show Link Between Data Breaches and Hospital Mortality Rates>>, CPO Magazine, acceso el día 20 de noviembre del 2019, https://www.cpomagazine.com/cyber-security/researchers-show-link-between-data-breaches-and-hospital-mortality-rates/?mc_cid=61cc16581e&mc_eid=5a73407028