Que no hackeen tu corazón

Esto va llegando a su fin. Hasta ahora hemos visto los **riesgos** que presentan los dispositivos médicos y hemos establecido una serie de posibles **controles** a fin de mitigar los mismos. Además, hemos observado la relevancia de la cual disponen este tipo de dispositivos en la industria.

En este post me gustaría hacer énfasis sobre algunos de los problemas más sonados en los últimos años en cuanto a dispositivos médicos respecta. No con el objetivo de asustaros o alarmaros sino de concienciar sobre la relevancia de todo lo expuesto hasta la fecha y la necesidad de informar a las autoridades pertinentes sobre este tipo de situaciones. Además, me gustaría exponer algunos de los motivos principales por los cuales el sector de la salud resulta el objetivo de tantos ataques.

¿Os acordáis de la empresa Medtronic?

En el tercer post hablamos sobre cómo esta empresa tuvo que retirar del mercado algunas bombas de insulina ya que resultaban vulnerables a ataques. No obstante, este tipo de vulnerabilidades no solo se limitan a las bombas de insulina.

A principios de este mismo año, por ejemplo, el Departamento de Seguridad Nacional de EE.UU advirtió sobre una vulnerabilidad crítica en el sistema de transmisión de datos de los implantes cardíacos de Medtronic. Este fallo permitía a los hackers modificar la configuración de los mismos. [1]

Si retrocedemos un poco más en el tiempo, en el año 2017 la FDA emitió la retirada de seis modelos de marcapasos producidos por la compañía Abbott debido a la presencia de una serie de vulnerabilidades. Estas vulnerabilidades permitían que usuarios no autorizados accedieran al dispositivo y modificaran el funcionamiento del marcapasos implantado. Esto podría resultar en daños para el paciente debido a un rápido agotamiento de la batería o a la modificación en la gestión de los latidos del paciente.

A fin de solucionar este problema la compañía desarrolló y validó una actualización correctiva para todos los dispositivos afectados. En este caso en concreto no resultó necesario intervenir a los pacientes a fin de retirar los marcapasos afectados. Sin embargo, al igual que con cualquier

actualización de firmware la FDA informó sobre la existencia de una serie de riesgos asociados a la instalación incorrecta de esta actualización. Entre estos riesgos se mencionaba la posibilidad de la pérdida de la configuración del dispositivo o incluso la pérdida completa de la funcionalidad del mismo. [2]

¿Y qué debe hacer una compañía ante estas situaciones?

A fin de detectar posibles problemas de seguridad relacionados con los dispositivos médicos, la FDA requiere la utilización de "Informes de Dispositivos Médicos". Los fabricantes están obligados a reportar eventos adversos a través de este tipo de informes. Mientras que se alienta a profesionales sanitarios, cuidadores o pacientes a presentar informes voluntarios sobre posibles eventos adversos que estos puedan apreciar. [3]

Uno de los errores más comunes que cometen los fabricantes a la hora de comunicar la situación a las organizaciones correspondientes es esperar demasiado. Y esto puede resultar comprensible hasta cierto punto. Las compañías pueden tener miedo a hacer público este tipo de situaciones debido a las consecuencias sobre su imagen corporativa, a las consecuencias económicas,…

Pero en realidad informar sobre los peligros no solo demuestra un buen hacer por parte de la compañía sino que demuestra una preocupación por la salud de sus clientes.

Los fabricantes necesitan entender que **alertar a las organizaciones pertinentes** acerca de problemas potenciales no siempre posee como desencadenante una retirada del producto del mercado. No hacerlo puede conducir, a su vez, a una mayor desconfianza por parte de los clientes o incluso a tener que hacer frente a multas cuantiosas.

Otro punto importante a considerar es la **transparencia**. Los fabricantes de dispositivos médicos deben ser francos sobre la verdadera naturaleza de la situación. Este no es el momento de endulzar los problemas. Los fabricantes deben estar preparados para divulgar el peligro potencial así como su alcance e impacto. [4]

Es importante entender que este tipo de organizaciones permiten actuar de forma más rápida al poder llegar a un mayor número de afectados.

¿Y porqué se producen tantos ataques contra este sector?

Después de investigar he podido encontrar una serie de razones [5] por las cuales el sector de la salud y por consiguiente, el de los dispositivos médicos, representan uno de los mayores objetivos para los hacktivistas:

- **La información privada de los pacientes posee alto valor económico para los atacantes:** Los hospitales almacenan una ingente cantidad de datos. Datos confidenciales que valen mucho dinero y que pueden ser vendidos fácilmente, lo que convierte a la industria médica en un objetivo cada vez más relevante.
- **Dispositivos médicos como punto de entrada:** Los dispositivos médicos como los rayos X, las bombas de insulina o los desfibriladores desempeñan un papel fundamental en la atención médica moderna. Sin embargo, este tipo de dispositivos pueden ser utilizados para lanzar un ataque sobre dispositivos mayores como pueden ser los servidores de un hospital. Incluso en el peor de los casos, los hackers pueden hacerse con el control completo de un dispositivo médico, impidiendo que las organizaciones sanitarias proporcionen a los pacientes la atención que requieren.
- **Acceso a datos remotos:** Conectarse a una red de forma remota puede resultar peligroso en caso de que no se tomen las medidas oportunas. De esto hablamos también en el post anterior, en el cual mencioné la necesidad de hacer uso de canales de comunicación seguros.
- **Los profesionales sanitarios no están concienciados sobre los múltiples riesgos tecnológicos existentes:** Cuando hablamos de seguridad, el eslabón más débil suele ser el empleado. El personal sanitario suele estar demasiado ocupado como para mantenerse informado sobre las últimas amenazas correspondientes a los dispositivos médicos. Sin embargo con que un solo dispositivo se vea comprometido, toda la red puede haber sido vulnerada.

Y ahora que ya tenemos una visión completa, me gustaría decir que a pesar de que los dispositivos médicos presenten múltiples riesgos y resulten vulnerables a ataques también facilitan la vida de muchas personas y permiten que muchas personas continúen con vida. Con el transcurso del tiempo cada vez obtendremos dispositivos médicos más seguros, eficaces y efectivos.

Ojala yo hoy no tuviera contenido para escribir este post, ya que eso implicaría que los dispositivos médicos serían completamente seguros. Ya es imposible cambiar el pasado y solo nos queda aprender de él para evolucionar hacia el futuro.

Ha sido un placer escribir para todos vosotros durante este tiempo pero esto ha llegado a su fin. Ha sido un periodo corto pero espero que os haya gustado. Como se suele decir coloquialmente “lo bueno, si breve, dos veces bueno”.

PD: Aunque se salga un poco de la línea argumental seguida durante este recorrido, no me gustaría acabar este post sin hacer mención a la necesidad de continuar investigando. Hace relativamente poco, por ejemplo, fue el día del cáncer de pulmón, una enfermedad que representa el 20,55% de defunciones en el territorio nacional. Además de resultar uno de los cánceres más letales, la calidad de vida de la cual disponen los pacientes supervivientes se ve considerablemente mermada. Es por ello que a través de este post me gustaría dar visibilidad a todas esas personas que sufren cada día las consecuencias de enfermedades como esta y recalcar la necesidad de continuar investigando. No solo en esta temática en concreto sino en la medicina en general. Solo a través de la investigación conseguiremos erradicar o paliar las consecuencias de este tipo de enfermedades y la tecnología puede resultar una gran fuente de ayuda. La investigación y cooperación son pilares fundamentales para continuar prosperando.

Y ahora sí que sí…**THE END**

Referencias

[1] <<Medtronic Conexus Radio Frequency Telemetry Protocol>>, CISA, acceso el día 30 de noviembre del 2019, https://www.us-cert.gov/ics/advisories/ICSMA-19-080-01

[2] <<Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott’s (formerly St. Jude Medical’s) Implantable Cardiac Pacemakers: FDA Safety Communication>>, FDA, acceso el día 30 de noviembre del 2019, https://www.fda.gov/medical-devices/safety-communications/firmware-update-address-cybersecurity-vulnerabilities-identified-abbotts-formerly-st-jude-medicals

[3] <<Medical Device Reporting (MDR): How to Report Medical Device Problems>>, FDA, acceso el día 30 de noviembre del 2019, https://www.fda.gov/medical-devices/medical-device-safety/medical-device-reporting-mdr-how-report-medical-device-problems

[4] <<Software is a top cause of medical device recalls: Here’s what you can do>>, Medical Design & Outsourcing, acceso el día 30 de noviembre del 2019, https://www.medicaldesignandoutsourcing.com/software-leading-cause-medical-device-recalls/

[5] <<9 reasons why healthcare is the biggest target for cyberattacks>>, Swivel Secure, acceso el día 30 de noviembre del 2019, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/