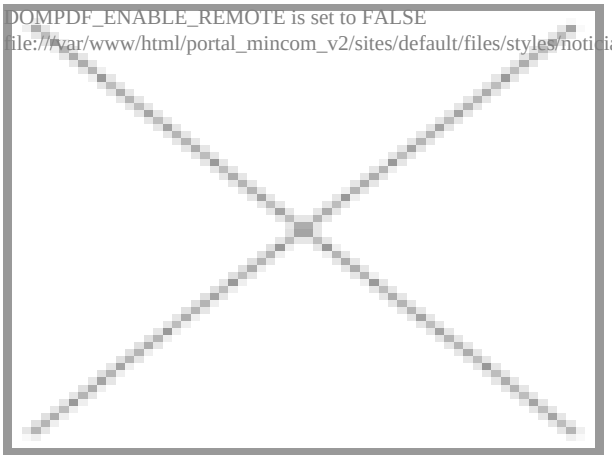

Fuente:
Diario TI

Existe una tendencia clara en la industria de la salud hacia la digitalización y la hiperconectividad que promete interesantes beneficios para pacientes y médicos por igual. Por ejemplo, en vez de tener que desplazarse los primeros a sus respectivos centros de salud, que en sí mismo puede ser todo un reto con determinadas dolencias, algunas tareas y chequeos rutinarios se pueden realizar en remoto, con la máxima comodidad para el paciente y con un importante ahorro de tiempo para todas las partes implicadas. Sin embargo, algunos de los sistemas empleados en estas tareas podrían no ser lo suficientemente seguros.

Uno de los casos examinados se conoció en agosto de 2016, cuando un grupo de investigadores de seguridad descubrió una vulnerabilidad en un marcapasos fabricado por uno de los principales proveedores del mundo de desfibriladores, marcapasos y otros equipos médicos. Estos investigadores comprobaron que los transmisores utilizados en un determinado modelo sufrían una vulnerabilidad que permitía chequear el estado del marcapasos y su configuración de forma remota, con el único requisito de que el paciente se encontrara físicamente en el radio de acción de dicho transmisor.

Más aún, se podría aprovechar esta vulnerabilidad para volver a configurar los dispositivos implantados y hacer que funcionaran de forma inapropiada, por ejemplo, administrando descargas innecesarias, en el caso de desfibriladores, capaces de agotar rápidamente su batería interna y hacer que el dispositivo falle en el momento en que más se necesita.

El fabricante del dispositivo lanzó una actualización de software para solucionar la mencionada brecha y la FDA (autoridad estadounidense administradora de alimentos y medicamentos) publicó una nota para informar a los pacientes y los médicos de los pasos necesarios para actualizar el software.

Si bien no se han reportado casos en los que los dispositivos afectados fueran sometidos a ataques reales, este incidente deja claro que la seguridad informática tiene que desempeñar un papel importante en el diseño de productos y dispositivos sanitarios. Hay mucho en juego: la reputación de un fabricante puede sufrir daños importantes si se suceden estos fallos de seguridad en sus productos. Y ya se sabe que los intereses financieros van de la mano de esta reputación. Pero mucho más importante es la vida de los pacientes que confían en estos dispositivos para sobrevivir, en el sentido literal de la palabra.

Pero este caso no ha sido el primero: en 2015, un investigador alemán logró desactivar la función de ventilación de un dispositivo de anestesia conectado a la red informática. Más tarde se señaló que parte del hardware funcionaba con un estandar de seguridad de 1990. Las vulnerabilidades del hardware médico han sido motivo de preocupación desde hace tiempo. Se han encontrado bombas de insulna vulnerables que permitián a sus atacantes administrar de forma remota dosis letales de este compuesto. Lo mismo sucede con algunas de las bombas de infusión de otros medicamentos que se utilizan con frecuencia en los hospitales. Cualquier equipo de hardware médico moderno y capaz de conectarse en red puede acumular varios años en

términos de seguridad. La razón es que la certificación para su venta sólo es válida para la configuración específica presentada por el fabricante y, dependiendo de la naturaleza del dispositivo, cualquier cambio en su configuración original requeriría una re-certificación.

Prevenir vulnerabilidades no es tarea fácil

Aunque sería fácil señalar las deficiencias de cualquier fabricante, hay que tener en cuenta que cualquier nuevo hardware, por sencillo que sea, o software usado en el sector salud tiene que someterse a pruebas rigurosas y necesita ser certificado antes de ser comercializado. Los criterios serán además más estrictos en función del papel que desempeñen estos dispositivos en la supervivencia de un paciente. Este proceso de certificación puede llevar años y ser muy costoso para los fabricantes. Hardware y software médico tienen además opciones muy limitadas cuando hablamos actualizaciones. A menudo estas actualizaciones y parches de seguridad para los dispositivos médicos son escasos y poco regulares, en el supuesto de que los haya.

Con la llegada de ransomware surge una posibilidad escalofriante: la amenaza real de que alguien sea capaz de extorsionar a los pacientes o a los centros de salud con la posibilidad de desactivar los sistemas vitales para los enfermos. Para hacer frente a este desafío, fabricantes e investigadores de seguridad no tienen más opción que mantener una estrecha colaboración y actuar de forma muy responsable cuando hablamos de revelar información, asegurando que ninguna vida se pone en riesgo como consecuencia de una vulnerabilidad en el software. Cada nuevo producto o dispositivo médico, por sencillo que sea, necesita de un cuidadoso proceso de evaluación capaz de establecer si sus utilidades son mayores que los riesgos de una conexión en línea. Además, los procesos de certificación deben acelerarse considerablemente pues la seguridad TI ha alcanzado la velocidad de crucero necesaria.

Por tanto, es de importancia crítica para la seguridad del paciente que los dispositivos médicos se apunten a la seguridad by design, es decir, esa seguridad que forma parte de la esencia del dispositivo y que está presente desde el momento en que era solo un concepto, tan importante como la propia función que realiza y por la que ha sido diseñado.

Disponile en:

https://diarioti.com/se-puede-hackear-un-corazon-humano/102963 [1]

Links
[1] https://diarioti.com/se-puede-hackear-un-corazon-humano/102963