Publicado en el 05/10/2016

El hackeo no tiene limites y el nuevo blanco son las bombas de insulina

Cada vez más, las nuevas tecnologías se adaptan para poder hackear todo tipo de productos, lo último son las bombas de insulina

Actualmente el mundo está conectado, eso significa que mucha de la información que se utiliza día con día viaja de un lugar a otro de forma constante, por lo que se necesita el mínimo de seguridad para que esta información no caiga en las manos de alguien que pueda hacer un mal uso de todos esos datos. Lamentablemente algunas compañías pasan por alto estos elementos de seguridad al creer que sus dispositivos no son los suficientemente atractivos para ser hackeados.

La compañía Johnson & Johnson está emitiendo una alerta de seguridad a todos los usuarios de la bomba de insulina Animas OneTouch Ping, la cual se ha descubierto que posee una vulnerabilidad que podría hacer que las dosis de insulina se modificaran vía remota y sin que el usuario se entere.

Otra vez el problema de seguridad en dispositivos médicos

La bomba Animas OneTouch Ping salió al mercado en 2008, entre sus ventajas está el uso de un mando inalámbrico que le permite al usuario ajustar las dosis de insulina sin necesidad de tener que acceder al dispositivo, el cual casi siempre está debajo de la ropa. A día de hoy se estima que más de 114.000 usuarios usan diariamente esta bomba tan sólo en los Estados Unidos y Canadá.

Jay Radcliffe, investigador de la firma de seguridad informática Rapid7 y diabético, descubrió en abril de este año que las comunicaciones entre la bomba y el mando no contaban con ningún tipo de cifrado, lo que podría hacer que cualquier hacker con los conocimientos suficientes pueda tener acceso a esa información y modificar la dosis de forma remota, lo que podría poner en riesgo la vida del paciente.

Radcliffe informó de inmediato a J&J de la vulnerabilidad de su dispositivo, y desde entonces han estado trabajando para resolverlo. La compañía asegura que los riesgos de sufrir un ataque son mínimos, ya que se requieren amplios conocimientos técnicos, equipo sofisticado y estar a menos de 8 metros de la bomba para interceptar las comunicaciones, sin embargo la vulnerabilidad está ahí.

J&J ha enviado cartas a todos los usuarios de esta bomba donde les asegura que el dispositivo es seguro y pueden seguirlo usando, sin embargo se mencionan algunas recomendaciones para no ser blanco de potenciales ataques, como por ejemplo dejar de usar el mando y programar la bomba de forma manual, ya que para cifrar las comunicaciones se requieren modificaciones en la programación del software, algo que requeriría retirar todos los dispositivos del mercado para instalar la actualización, lo que representa dinero y tiempo, por lo que han decidido dejarlo así y únicamente emitir las recomendaciones de seguridad.

Lamentablemente este no es el primer caso de un dispositivo médico con vulnerabilidades, ya han surgido casos de marcapasos y desfibriladores que presentan el mismo patrón de comunicaciones sin cifrado, lo que ha provocado que la FDA esté iniciando una investigación para que las compañías responsables de estos casos, y que ponen en riesgo la vida de sus usuarios, tengan la obligación de solucionar este tipo de fallos, donde también se incluyen recomendaciones para que las compañías trabajen con investigadores de seguridad con el fin de mitigar este tipo de riesgos que empiezan a ser comunes.

La noticia El hackeo no tiene limites y el nuevo blanco son las bombas de insulina fue publicada originalmente en Xataka

Datos de contacto:

Nota de prensa publicada en:

Categorías: Hardware Ciberseguridad