Playbook del hacker: me cuelo en tu dispositivo médico (Parte 1/4)

Recientes demostraciones de dispositivos médicos con conectividad a la red muestran vulnerabilidades y potenciales amenazas de ciberseguridad. Muchos de estos dispositivos, que son de soporte vital (monitores de pacientes, bombas de infusión, ventiladores, etc.), residen en las redes de hospitales a lo largo del mundo. Incluso son más los dispositivos accesibles a través de la tecnología wireless (bombas de insulina y marcapasos, por ejemplo).

Estos dispositivos representan un arma de doble filo: tienen el potencial de transformar el cuidado de la salud pero a su vez exponen a los pacientes y a las organizaciones de la salud a riesgos de seguridad. Entre las consecuencias no intencionadas de la digitalización en el cuidado de la salud y el crecimiento de la conectividad en red están el ser hackeado, ser infectado con malware y ser vulnerable a accesos no autorizados.

En esta serie de 4 entradas, vamos a ver 4 formas/escenarios en los que los ciberdelincuentes se aprovechan de las vulnerabilidades de los dispositivos de propósito medico.

Dañar a pacientes atacando dispositivos médicos.

Este es el escenario más temido de todos: un hacker se cuela en un dispositivo de un paciente e “inyecta” código malicioso que causa daños o incluso la muerte al que lo lleva.

Dick Cheney, un señor amigable

Famoso es el caso del entonces Vicepresidente de los EEUU Dick Cheney, que allá por el año 2007 tenía tal miedo de que los terroristas hackearan su marcapasos que decidió deshabilitar su conexión wireless para evitar intentos de asesinato.

Unos cuantos años después, en Diciembre de 2012, la serie de ficción Homeland – **ALERTA SPOILERS!!!** – en uno de sus capítulos trato este mismo tema, retratando la muerte del (¿casualidad?) Vicepresidente de los EEUU cuando una organización terrorista hackea su marcapasos.

El investigador en ciberseguridad Jay Radcliffe encontró una vulnerabilidad que podía servir para hackear una bomba de insulina y disparar una sobredosis. Este tipo de ataques pueden estar dirigidos a un paciente en particular o ser generalizados a todos los pacientes que usen un dispositivo en particular. Afortunadamente, este escenario es muy raro que se de, pero los dispositivos de los que dependen pacientes de forma crítica deben ser analizados en profundidad para minimizar riesgos.

Mañana a la misma hora tendréis la segunda parte del Playbook.