Ciencia y TECNOLOGÍA

Ven talento hacker en el país

México debe aprovechar el talento hacker que tiene para crear soluciones a grandes problemas, por lo que es importante acercar a las nuevas generaciones la tecnología, afirmó el cofundador y director de la escuela Dev.f. Un ejemplo es la competencia StartupBus, en las que el año pasado México se alzó con el segundo lugar gracias a una solución llamada Bridgefy para brindar conectividad en zonas de desastres o rurales.

Ciberataques a la salud

El ataque informático a dispositivos médicos es algo bastante real

DARDANE RODRÍGUEZ VERDUGO*
dardane.rodriguez@gmail.com

Foto: Cortesía

Los dispositivos con sistema inalámbrico son vulnerables de ataques cibernéticos.

Mucho se ha hablado acerca de los beneficios que acarrean las tecnologías de la información a la humanidad, las ventajas que éstas ofrecen, y cómo mejoran la calidad vida.

Sin embargo, al momento de abordar temas tan delicados como los ataques cibernéticos, resulta que éstos les son ajenos tanto a la opinión pública, como a los usuarios promedio, lo que más podría preocupar en este caso sería un robo de identidad, aunque los ataques informáticos pueden llegar a infligir daños serios en el mundo real.

A través de los tiempos y con la evolución de la tecnología se ha pensado que la mayor la amenaza de ésta se dará, en el mejor de los sueños de la ciencia ficción, cuando las computadoras se revelen contra la raza humana.

Sin embargo, el riesgo latente y real se encuentra en mano de los propios humanos los cuales, sobrepasando y utilizando a su favor los límites de la tecnología, realizan -o podrían realizar- ataques que atenten directamente contra la salud de una persona en específico dando como resultado acciones funestas.

El ataque informático a dispositivos médicos, a primera instancia puede ser difícil que se tome en serio, ya que suena demasiado descabellado; sin embargo, es algo bastante real.

ALGUNOS CASOS

Es un hecho que los marcapasos (desfibriladores implantables) son vulnerables. En 2012 con sólo una computadora portátil y algunos componentes informáticos de fácil obtención, Barnaby Jack, prolífico -y ahora difunto- hacker neozelandés, logró alterar el funcionamiento de uno de estos dispositivos médicos.

En la demostración del ataque, Jack mostró cómo es que podía provocar una descarga súbita de 830 voltios -suficiente como para causar la muerte del portador del dispositivo- de forma remota.

De la misma manera en 2011, Barnaby Jack había demostrado por primera vez como hackear bombas de insulina de manera inalámbrica. Dicha demostración fue hecha montando uno de estos dispositivos en un maniquí, diáfano el cual contaba con bolsas plásticas con líquido transparente simulando el páncreas.

El atacante obtuvo el completo control del artefacto, y con sólo presionar una tecla de su laptop, podía accionar la bomba para que ésta inyectara en repetidas ocasiones la dosis máxima de insulina en el páncreas simulado hasta que el depósito de 300 unidades se agotara. Esta dosis proporcionada a un paciente típico resultaría en algo fatal.

A principios de 2012 Barnaby realizó la misma demostración en una conferencia de seguridad en San Francisco, mostrando que el ataque se podía realizar de manera exitosa a una distancia de 90 metros.

Estos ataques no solo se pueden afectar en el área de la salud, también es posible hackear automóviles y otros medios de transporte.

En 2009 se demostró que era posible apagar el motor, falsear la lectura del velocímetro y hasta bloquear automáticamente los frenos de forma desigual, con esto se podrían desestabilizar un automóvil que viaje a altas velocidades.

Algunos investigadores han estudiado el sistema electrónico de los automóviles de hoy en día topándose con graves problemas de seguridad.

Estos problemas dentro de la industria se dan en su mayoría por la falta de actualizaciones y mejoras de los mismos, a diferencia de los equipos de cómputo o teléfonos inteligentes, los cuales reciben de manera constante parches de seguridad para evitar esta clase de fallos.

EN LOS MEDIOS

Temáticas como estas fueron tomadas en cuenta en algunas series televisivas populares, por ejemplo a finales de 2012, la serie "House of Cards", emitió en un episodio en el cual se mostró el asesinato de cierto vicepresidente al acelerar sus latidos del corazón llegando a inducir un ataque cardiaco.

Todo esto se dio gracias a un ataque informático dirigido al marcapasos de dicho personaje. Para la época en la cual el episodio fue emitido, dicho tema fue ridiculizado y tachado de poco realista, aunque más tarde se descubrió que el hecho se encontraba basado en un problema de seguridad real.

> En 2009 se demostró que era posible apagar el motor de un auto, falsear la lectura del velocímetro y hasta bloquear automáticamente los frenos de forma desigual, con esto se podrían desestabilizar un automóvil que viaje a altas velocidades.

En 2013 se hizo pública la noticia de que el ex vicepresidente de los Estados Unidos, Dick Cheney, había mandado desactivar en 2007 todas las funciones inalámbricas de su marcapasos, ya que desde entonces temía ser sujeto de algún ataque terrorista.

NO TODO ES PARANOIA

Para evitar algunos ataques de esta índole, algunos fabricantes han privado a su dispositivo de la opción para desactivarlos de manera remota.

En Estados Unidos, la Agencia de Alimentos y Medicamentos (FDA, por sus siglas en inglés) a partir de junio de 2013 pidió a los fabricantes de dispositivos médicos y a los hospitales que fortalecieran la seguridad en este aspecto, ya que la mayoría de los dispositivos modernos implantados se comunican con equipos de diagnóstico, utilizando un método de autenticación, el cual consiste en un nombre de usuario y contraseña.

En muchos casos, el nombre de usuario y la contraseña son el número de serie del dispositivo y el número de modelo.

El presidente y director general del Centro para Seguridad en Internet, William F. Pelgrin ha declarado que, hasta la fecha, no ha habido casos documentados de ataques con éxito a los dispositivos médicos móviles -a excepción de los casos antes mencionados-.

Sin embargo, el riesgo es real. Los dispositivos inalámbricos sin garantía son vulnerables a un ataque.

*El autor es profesor del área de Computación en la Universidad Tecnológica de Tijuana, campus Ensenada.