ELMUNDO.es

26/08/2011

El 'hacker' que destapó los problemas de seguridad de las bombas de insulina

Radcliffe muestra el aparato que usó para 'piratear' la bomba de insulina.| Ap

Actualizado **viernes 26/08/2011 19:05 horas**

Durante una conferencia sobre piratería informática celebrada a principios de agosto en Las Vegas (EEUU), Jay Radcliffe habló sobre los serios problemas de seguridad que había encontrado en unas conocidas bombas de insulina implantables. Advirtió de que cualquier 'hacker' podía hacerse fácilmente con el control remoto de esos dispositivos y manejarlos a su antojo. Es decir, podría alterar las dosis, los tiempos de administración y, por tanto, poner en riesgo la salud del paciente.

No se trataba de una afirmación de oídas, sino con conocimiento de causa. Radcliffe es diabético, lleva esas bombas y las ha 'pirateado' él mismo. En ese momento no acusó a ningún fabricante porque como reconoció a la prensa estadounidense "quería dar opción a la compañía de reparar sus problemas de seguridad". Sin embargo, tras ser ignorado en repetidas ocasiones -según su versión- y **ver que minimizaban sus advertencias**, ha decidido identificar al responsable de estas bombas 'inseguras', para ver si la presión pública les obliga a reaccionar. El señalado con el dedo es Medtronic, una de las mayores compañías del mundo de tecnología médica.

Ante esta acusación, Medtronic no ha tenido más remedio que salir a la palestra. Ha reconocido ciertos problemas de seguridad en su línea de bombas implantables, pero aseguran que **los pacientes que las usan pueden estar tranquilos** porque el riesgo de un "ciberataque" es extremadamente bajo. "Tendría que ser premeditado por alguien que intenta causar daño a una persona", indicó John Mastrototaro, médico y vicepresidente de investigación y desarrollo de la división diabetes de la compañía. "La probabilidad de que esto suceda accidentalmente es nula", afirma.

No obstante, Mastrototaro ha adelantado que ya se están tomando cartas en el asunto y que se ha ordenado un mayor control de las potenciales vulnerabilidades de seguridad en la próxima generación de bombas de insulina de la compañía que están en desarrollo. Sobre posibles cambios en las actuales, dice que sería difícil, pues **se exige la aprobación de la FDA** (la Agencia reguladora de los medicamentos de EEUU) para cualquier cambio en un producto así como para el uso de "parches" de software de un dispositivo.

La polémica de la 'ciberseguridad'

Las bombas de insulina han sido los últimos dispositivos médicos 'hackeados', pero no los únicos. Anteriormente, la misma polémica ya había girado sobre los marcapasos. Stuart McClure, vicepresidente senior de seguridad del productor de software McAfee explica que el debate sobre la ciberseguridad de estos productos -que ha ocupado espacio en diversas publicaciones científicas- generará cada vez más debate.

"Todos los dispositivos, incluidos los médicos, pueden ser vulnerados por piratas informáticos y **las empresas son tontas si creen que sus aparatos son inmunes**", expresó.

Tras la denuncia pública de Radcliffe, dos abogados -de California y Massachusetts-, ambos del Partido Demócrata, han solicitado a la Oficina de Contabilidad del Gobierno estadounidense que evalúe los esfuerzos que las autoridades hacen en la actualidad para identificar estos riesgos en implantes médicos que usan la comunicación inalámbrica.