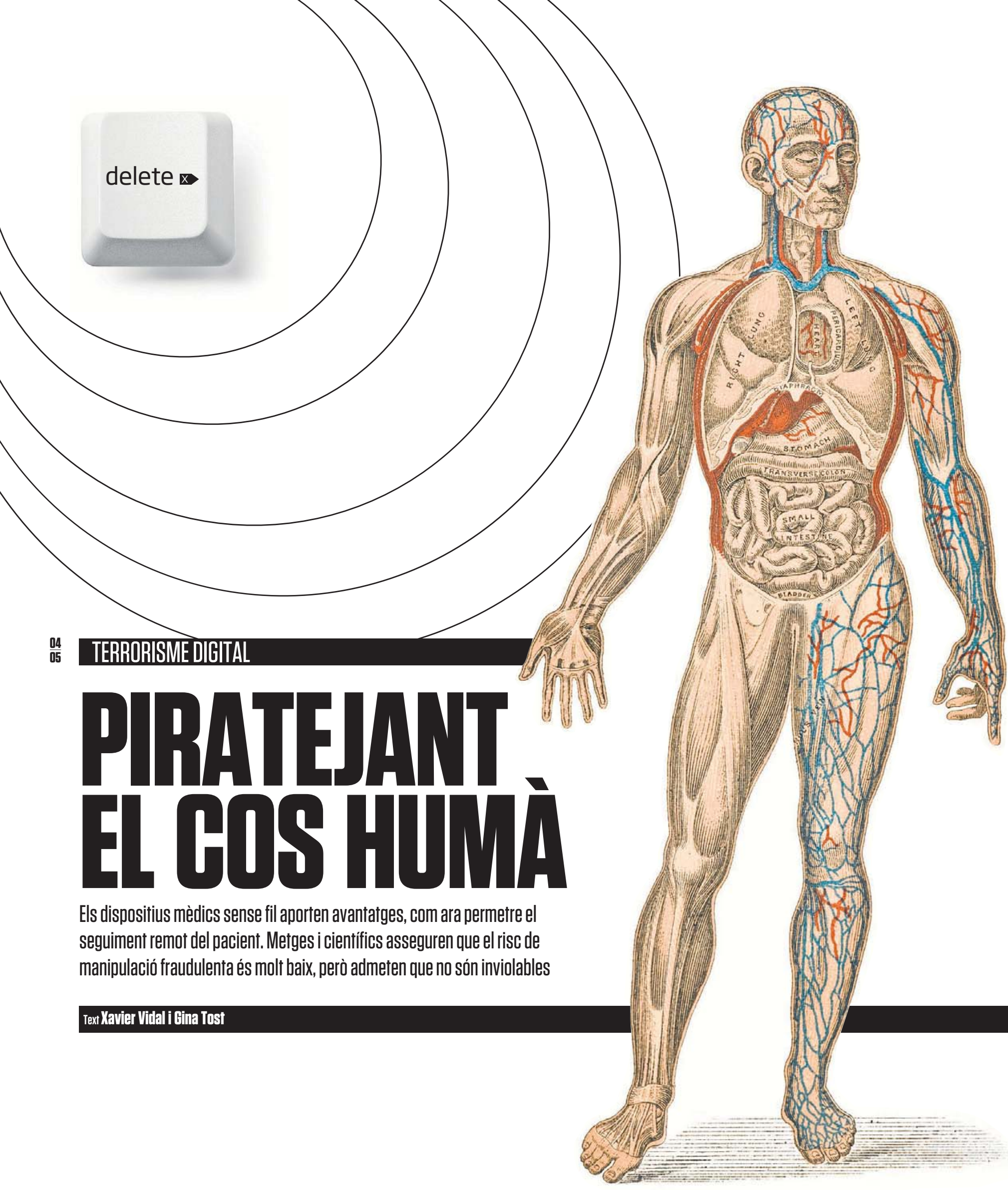


TERRORISME DIGITAL

PIRATEJANT EL COS HUMÀ

Els dispositius mèdics sense fil aporten avantatges, com ara permetre el seguiment remot del pacient. Metges i científics asseguren que el risc de manipulació fraudulenta és molt baix, però admeten que no són inviolables

Text **Xavier Vidal i Gina Tost**

Més de quatre milions de persones al món porten un marcapassos implantat al cos per ajudar a fer que el seu cor bategui. La UE acaba d'aprovar l'ús d'un marcapassos amb connexió sense fil. Però als EUA encara estudien la seguretat i altres aspectes d'un dispositiu tan essencial per a la vida humana davant la possibilitat de manipulació no autoritzada de manera remota.

Un dels *hackers* més prestigiosos del món, Barnaby Jack, estava a punt de demostrar públicament que podia parar un marcapassos sense fil quan va morir aquest estiu en circumstàncies encara no aclarides. Tot podria haver quedat en una teoria *conspiranoica* si no fos perquè l'ex vicepresident dels EUA Dick Cheney va declarar fa unes setmanes a la BBC que la funció sense fil del seu marcapassos va ser desactivada per por a un atac terrorista, com havia passat en la famosa sèrie televisiva *Homeland*. La pregunta ha sorgit els últims mesos entre experts informàtics i autoritats: ¿són prou segurs els dispositius mèdics connectats al cos humà?

L'empresa nord-americana IDD (Internet Identity), especialista a garantir la seguretat de grans marques en la seva dimensió *online*, afirma en el seu últim estudi que el 2014 podríem assistir als primers atemptats amb víctimes mortals a través d'internet. En el document posa com a exemple els marcapassos o els cotxes connectats a la xarxa. Si tenim en compte que, segons estudis de l'empresa de seguretat informàtica Symantec, el volum de recursos que mou el cibercrim supera al tràfic de drogues, és fàcil deduir que el cos humà pot convertir-se en un objectiu prioritari per als delinqüents informàtics.

Shawn Merdinger, un dels màxims experts en seguretat informàtica dels dispositius mèdics connectats, reconeix que l'atac remot a un marcapassos amb connexió sense fil és possible, tot i que "la possibilitat només existeix a nivell d'estats o agències d'intel·ligència". Aquests marcapassos, que transmeten la informació a través d'un senyal wifi, aporten molts avantatges. El metge pot rebre dades sobre el funcionament de l'aparell de manera remota i en temps real. El pacient s'evita trasllats i el facultatiu pot intervenir al moment si es presenten problemes cardíacs.

Per Marta Ferrero, cap del Servei de Cardiologia d'IdcSalud Hospital General de Catalunya, a casa nostra "no existeix la possibilitat de manipular les dades dels marcapassos de manera remota". I explica que aquesta protecció és deguda a la manera en què estan configurats els dispositius. "Només es pot rebre la informació, no modificar els paràmetres de funcionament des de la distància". En qualsevol cas, explica que la tecnologia permetria un altre tipus de configuració que fes possible aquesta modificació a distància. L'investigador de l'Institut de Bioenginyeria de Catalunya, Antoni Homs, especialista en nanotecnologia, reforça aquesta idea de seguretat: "Els marcapassos moderns fins i tot són immunes a les radiacions de microones que els afectaven fa uns anys. La seguretat és molt alta".

Neurotransmissors i bombes d'insulina

Però les alertes pel que fa al risc de terrorisme digital sobre el cos humà arriben des de fronts diversos. Neurotransmissors o bombes d'administració d'insulina, per exemple, estan en el grup de dispositius susceptibles de ser manipulats a distància. Ja fa més de dos anys Jerome Radcliffe, investigador i diabètic, va demostrar que podia alterar les lectures de la bomba d'insulina implantada al seu cos. Si les lectures es manipulen es provoca una administració incorrecta i, per tant, es posa en risc la vida del pacient connectat a la bomba.

Ara bé, no tots els dispositius mèdics connectats estan a l'interior del cos humà. Monitors de control, bombes administra-

LA MISTERIOSA MORT DE BARNABY JACK

El cos sense vida de Barnaby Jack, de 35 anys, va ser trobat al juliol a l'apartament on vivia a San Francisco. Era un dels *hackers* ètics més reputats i respectats per la comunitat internacional d'experts en seguretat informàtica. Una setmana després de la seva mort, Barnaby Jack tenia previst revelar al Black Hat de Las Vegas, un dels congressos més importants del món del *hacking*, com es podia manipular un marcapassos a distància per aturar-lo.

Jack s'havia fet cèlebre l'any 2010 en mostrar com es podia buidar un caixer automàtic a distància sense ni tan sols ser client del banc. D'això se'n va dir *jackpotting*. En els últims temps s'havia concentrat a estudiar les vulnerabilitats dels dispositius mèdics connectats al cos humà. A part de la manipulació a distància dels marcapassos amb connexió sense fil, Barnaby Jack ja havia demostrat també com és possible aturar una bomba d'administració d'insulina sense acostar-s'hi. I això era només el principi, perquè el *hacker* havia alertat de les deficiències i falta d'actualització de gran part del programari que fa anar els aparells mèdics dels hospitals.

Jack s'havia posat en contacte amb diverses companyies mèdiques per ajudar a resoldre les esquerdes de seguretat abans que altres amb més mala fe que ell provoquessin danys en les persones.

Fins que no s'aclareixi com va morir no s'acabaran les especulacions inquietants sobre si la seva va ser una mort per causes naturals o hi ha alguna conspiració al darrere. Molts experts s'exclamen que, quatre mesos després, encara no es coneguin les causes de la mort. El misteri continua envoltant la desaparició de Barnaby Jack.

4.000.000
Les persones al món que porten implantat un marcapassos

10 anys
La bateria dels marcapassos sense fil té una autonomia de fins a una dècada

dores de medicaments i sistemes d'assistència a les constants vitals són controlats sovint per programari dissenyat abans dels perills del món interconnectat. Un programari desenvolupat a partir d'un programari, l'anomenat SCADA, que permet controlar i supervisar processos industrials a distància. Una modificació de l'SCADA era responsable de fer anar, per exemple, les rentadores nuclears iranianes. La vulnerabilitat d'aquest programari va permetre que un virus militar, l'Stuxnet, prengués el control a distància i fes malbé gairebé el 80% de les rentadores iranianes.

De fet, les febleses de seguretat dels dispositius mèdics connectats va fer que a l'agost la FDA, la poderosa Agència d'Alimentació i Medicaments nord-americana, publiqués un document alertant dels perills i fent recomanacions molt concretes als fabricants. La FDA detallava un ampli catàleg de situacions de risc, des del robatori de les dades personals dels pacients, moltes vegades guardades en el mateix dispositiu, fins a l'apagada de les funcions mitjançant l'accés remot.

Per Alícia Casals, cap del grup de Robòtica de l'Institut de Bioenginyeria de Catalunya, el problema "no és tant del programari sinó dels tallafocs" usats per evitar una manipulació externa. Reconeix que la manipulació és possible, però que el risc és baix. "Aquests dispositius tenen un canal d'entrada i sortida, cosa que els fa potencialment més vulnerables. Però estan dissenyats de tal manera que el seu abast és molt curt: l'especialista ha d'estar pràcticament en contacte amb el pacient per limitar atacs incontrolats". En qualsevol cas, l'accés remot als dispositius mèdics dels hospitals és molt restringit. I, a més, segons explica la doctora Marta Fererro, cap del servei de cardiologia de l'Hospital General de Catalunya, "les plataformes per on viatja la informació són encriptades".

Més enllà del risc de pirateig voluntari dels dispositius mèdics connectats, el document oficial de l'Agència d'Alimentació i Medicaments nord-americana alerta sobre una amenaça molt més prosaica: les interferències de radiofreqüència dels aparells amb possibilitats de ser operats de manera remota. La FDA reclama "l'assignació d'una banda de freqüència exclusiva a tot el món". En aquest punt coincideix l'expert Shawn Merdinger: "Hi ha nombrosos senyals sense fil, des dels emesos pels telèfons mòbils fins als de les ambulàncies i els helicòpters. Fins i tot els comandaments a distància dels televisors dels pacients poden interferir. Tot això pot causar interferències amb els dispositius mèdics i el més preocupant de tot és que és molt difícil identificar on és l'origen de la interferència".

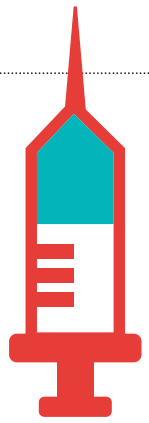
DESFIBRIL·LADORS AUTOMÀTICS

Els desfibril·ladors automàtics són uns dispositius semblants als marcapassos que controlen de manera continuada el ritme cardíac i ofereixen la possibilitat de fer un seguiment a distància de les arítmies. La telemetria es transmet a través de connexions sense fil a monitors externs i pot ser reenviada via satèl·lit. Així, els metges monitoren els pacients siguin on siguin; en contrapartida, creix el risc de manipulació no autoritzada.

Un dels principals avantatges de la connexió remota i la informatització dels aparells als hospitals és la capacitat d'emmagatzemar les dades mèdiques dels pacients. Això facilita, millora i agilitza els tractaments. Però la gestió d'aquesta informació requereix processos informàtics i no sempre és possible garantir que la seva seguretat és inviolable. Segons la cardiòloga Marta Ferrero, "el risc més alt que es podria córrer és que algú fora del sistema sanitari pogués accedir a la informació del dispositiu d'un determinat pacient; ara bé, es fan molts esforços per garantir la seguretat de la xarxa". El perill, però, ja és una realitat. Segons l'empresa de seguretat Symantec, el 10% dels hospitals dels EUA van patir algun atac informàtic el 2012.

La seguretat de les aplicacions mòbils

Al llarg del 2013 es van descarregar més de cent mil milions d'aplicacions, segons l'empresa especialitzada Gartner. I una part estan dissenyades per controlar els dispositius mèdics connectats al cos humà i enviar la informació al nostre metge. L'investigador Shawn Merdinger desgrana els riscos que se'n poden derivar. "La clau és el canal de comunicació



10%

Un de cada deu hospitals dels Estats Units va patir un atac informàtic durant el 2012

MARCAPASSOS SENSE FIL

Tenen unes dimensions d'entre 22 i 41 mil·límetres i es poden controlar remotament mitjançant un monitor o un telèfon intel·ligent. Els avantatges són clars: menys consum energètic (fins a 10 anys de bateria) i manipulació remota sense cirurgia. La seguretat, però, continua sent un tema que encara no està completament resolt.

entre el dispositiu i l'aplicació. Com es comunica l'aplicació amb l'oficina del metge? Com aïllem l'aplicació en qüestió, amb les dades que conté, de la resta d'aplicacions al telèfon? Com s'evita que un agent maliciós pugui substituir el propietari i col·locar un troià en el seu lloc?", s'interroga. Altres informes confirmen el perill. Segons el Mobile App Reputation Service de l'empresa Trend Micro, hi ha aproximadament un milió d'aplicacions amb programari maliciós. Shawn Merdinger recomana a "qualsevol persona que vulgui utilitzar una aplicació amb un dispositiu mèdic, que faci servir una tauleta o un telèfon intel·ligent aïllat, que contingui només aquesta aplicació". "No m'agradaria que el telèfon que controla la meva bomba d'insulina patís els mateixos riscos que el telèfon amb què navego per internet o entro a les xarxes socials", diu.

Nanotecnologia i roba intel·ligent

Si parlem de la possibilitat de piratejar el cos humà, la nanotecnologia i la roba intel·ligent són les pròximes fronteres a explorar. Els nous dispositius *weareables*, és a dir, vestibles, són capaços d'enviar dades mèdiques a través d'internet, i això implica riscos en la comunicació. Marc Torrent, mànager d'innovació i desenvolupament de l'empresa catalana especialitzada Cetemsa, indica que aquesta informació "ha de ser confidencial i protegida amb els mateixos mecanismes amb què es protegeix la informació als hospitals avui en dia; s'ha de transmetre per internet de manera encriptada i mitjançant connexions segures". Esclar que, vist com la NSA accedeix a les nostres dades més confidencials, no sembla que l'actual seguretat a internet sigui un estàndard prou ferm.

Pel que fa a la nanotecnologia, que en un futur podria dotar la medicina, per exemple, de dispositius biomèdics per distribuir medicaments directament a les cèl·lules malaltes, els reptes són més variats. Antoni Homs, especialista en la matèria, opina que "s'haurà de fer molt difícil suplantar les identitats o duplicar les claus d'accés a les dades clíniques o als mecanismes de control dels dispositius". La informació mèdica del nostre cos pot convertir-se en un capital molt valuós, i generar possibles negocis il·legals com ara el xantatge biològic: robar les nostres dades de salut i exigir un rescat a canvi de no fer-les públiques o desvelar-les a asseguradores.

Els avantatges dels dispositius mèdics connectats al cos humà semblen tan evidents com clara és també la necessitat de garantir la inviolabilitat de les comunicacions que fan servir.

Bombes d'insulina vulnerables

Centenars de milers de diabètics porten bombes d'insulina implantades al cos. Supleixen el dèficit de producció d'aquesta substància per part de l'organisme. Les bombes modernes monitoren el nivell de glucosa del pacient i l'envien a un monitor extern per radiofreqüència. El monitor es pot connectar a internet per facilitar el seguiment mèdic. El sistema facilita enormement la vida dels diabètics. Jay Radcliffe, diabètic expert en seguretat, va ser el primer a demostrar que les bombes d'insulina es podien manipular remotament. L'empresa de seguretat IOActive va confirmar que la manipulació es podia fer a una distància de fins a gairebé 90 metres del pacient. Medtronic, líder en fabricació de bombes d'insulina, va reconèixer que tot i ser molt difícil, la manipulació era possible. La seguretat en el programari de control de les bombes és molt gran, però el món de la delinqüència informàtica avança ràpidament. Symantec, una empresa especialitzada a combatre amenaces informàtiques, creu que el 2014 podria ser l'any de les primeres "morts per internet".