L'allarme riguarda defibrillatori, pompe di insulina, neuro-stimolatori, smartwatch e, ovviamente, pacemaker.

ATTENTI AL CARDIOHACKER

DOPO AVER PRESO DI MIRA GLI OSPEDALI, I PIRATI INFORMATICI PUNTANO A MINARE LA SALUTE DEI SINGOLI PAZIENTI COLPENDO I DISPOSITIVI MEDICI AVANZATI, CONNESSI GRAZIE ALLA TECNOLOGIA. SCOPO: ESTORSIONE, SOPRATTUTTO VERSO LE AZIENDE PRODUTTRICI. OGGI LA CYBERSICUREZZA DEVE ARRIVARE ANCHE LÌ.

di Stefano Piazza
e Luciano Tirinnanzi

L'espressione «colpire dritti al cuore» non è mai stata più calzante. Almeno non da quando si è scoperto che anche i dispositivi medici con una connessione wireless - dal pacemaker al defibrillatore, per fare un esempio concreto - possono essere «hackerati» da informatici malintenzionati, al punto che è per loro possibile alterarne il funzionamento o anche spegnerli causando problemi gravi di salute o addirittura infarti. Sembra una fake news da complottisti del nuovo millennio ma, purtroppo per i deboli di cuore (e non soltanto), la ricerca scientifica e alcuni importanti studi di settore sulla pirateria informatica - tra cui la Food and Drug Administration (Fda) statunitense - confermano che questo rischio esiste ed è concreto.

A parlarne per la prima volta al grande pubblico, però, fu nientemeno che Dick Cheney, ex vicepresidente degli Stati Uniti e portatore di un pacemaker dai primi anni 2000, che già nel 2007 pretese dai cardiologi la rimozione della funzione wireless dal proprio defibrillatore, proprio per paura di subire un attacco terroristico a suo danno. Allora il discusso (e detestatissimo) funzionario americano fu aspramente criticato per l'infondatezza delle sue affermazioni, ma il suo cardiologo, il dottor Jonathan Reiner, per prudenza sostituì davvero il defibrillatore cardiaco. «Mi sembrava una cattiva idea per il vicepresidente degli Stati Uniti avere un dispositivo che forse qualcuno poteva essere in grado di hackerare» dichiarò Reiner alla Cbs, aggiungendo criptico: «Ho temuto che qualcuno potesse ucciderlo».

Se all'epoca la notizia suonò come una provocazione o un capriccio da ricco funzionario statale, oggi la minaccia ai dispositivi medici è un filone da osservare con attenzione. Al punto che già nel 2017 la Fda ha chiesto il ritiro volontario di 500 mila pacemaker proprio perché ritenuti vulnerabili alla pirateria informatica, anche se all'epoca non erano ancora emerse segnalazioni di eventuali stimolatori cardiaci effettivamente violati. «L'hacking è sicuramente qualcosa di cui le persone con questi dispositivi devono essere consapevoli e sapere che è una possibilità», commentò al tempo David J. Slotwiner, a capo del reparto di cardiologia al New York Presbyterian Hospital-Queens, autore di una serie di pubblicazioni sui problemi di sicurezza informatica con simili tecnologie salvavita.

Se il concetto di violazione della privacy è quasi un vecchio refrain, con l'evolversi vertiginoso della tecnologia, nuove e sempre più maligne forme di cybercrime prendono corpo: poter manipolare i software medicali e creare un serio pericolo al cuore del bersaglio, nel vero senso della parola, è diventato (oltre che un potenziale incubo) una realtà.

«Gli attacchi informatici a scapito di reti informatiche ospedaliere e dispositivi medici sono purtroppo diventati una realtà»

Giulio Conte
cardiologo ed esperto di elettrofisiologia cardiaca

Gaetano Marrocco, professore ordinario di Campi Elettromagnetici dell'Università Tor Vergata di Roma e coordinatore del corso di studi in Ingegneria Medica, lo conferma: «Negli ultimi cinque anni sono stati registrati tra 150 e 200 attacchi hacker a dispositivi medici, fatti per estorcere soldi alle aziende che li producono, dimostrandone fragilità della sicurezza, o per minare la salute di personaggi politici. I dispositivi medici sono oggetti vulnerabili perché sempre più connessi e che a oggi non hanno nessun tipo di normativa che ne garantisce la sicurezza da questo punto di vista».

Va però chiarito che l'obiettivo del cyber criminale non è quasi mai direttamente il paziente che indossa un pacemaker e che magari si vuole colpire per ragioni personali; anche se, a dire il vero, vi sono più casi dimostrati di personalità diplomatiche che hanno avuto fastidi fisici causati dal bombardamento magnetico generato a distanza sui dispositivi di salute personali. Piuttosto, l'obiettivo è di norma nuocere alla determinata società che quei dispositivi medici li produce e li commercia, secondo una legge antica come il mondo e che la concorrenza aziendale ha fatto propria: *mors tua, vita mea*.

Danneggiare un dispositivo all'avanguardia, infatti - smartwatch, pacemaker, defibrillatori, pompe di insulina, neuro-stimolatori – rientra nella logica capitalistica della concorrenza sleale, e può determinare l'esclusione da appalti multimilionari con aziende ospedaliere, crolli in borsa, finanche il fallimento. Al punto che, come sottolinea ancora Marrocco, «oggi il tema della sicurezza cyberfisica dei dispositivi medici assume una significativa rilevanza per produttori, ospedali e pazienti soprattutto nell'attuale e futuro scenario di crescente interconnessione». Uno scenario e un settore dove peraltro l'informatica (telemedicina, tecnologie medico-scientifiche e sanità in Rete) ha fatto progressi significativi e di una portata tale da far immaginare che indietro non si può tornare.

A confermarlo è il professor Giulio Conte, caposervizio di Cardiologia dell'Istituto cardiocentro Ticino, a Lugano, ed esperto di elettrofisiologia cardiaca: «Quando si parla di cybersicurezza di pacemaker e defibrillatori, è doveroso precisare che i benefici terapeutici di tali dispositivi superano di gran lunga qualsiasi potenziale rischio per la sicurezza. Pertanto, il loro utilizzo è indispensabile e ha portato nei decenni a una significativa riduzione di mortalità e a un incremento della qualità di vita dei nostri pazienti».

Getty images (2)

150-200
Gli attacchi hacker ai danni di dispositivi medici registrati negli ultimi cinque anni, a scopo di estorsione.

Tuttavia, aggiunge Conte, «gli attacchi informatici, a scapito non solo delle reti informatiche delle strutture ospedaliere ma anche dei dispositivi medici con cui trattiamo i nostri pazienti, sono purtroppo divenuti una realtà. Ne è un esempio il richiamo della Fda statunitense dei quasi 500 mila pacemaker, che ha attirato l'attenzione sulle potenziali crepe nella sicurezza informatica di questi aiuti cardiaci impiantabili». Il punto è allora capire come ci si può difendere. «L'ottimizzazione della sicurezza informatica dev'essere una priorità di ogni struttura ospedaliera e deve basarsi sulla stretta collaborazione sia con le aziende produttrici che con le autorità di omologazione e controllo dei dispositivi medici» spiega ancora Conte.

Il fine è, per tutti, lo sviluppo di una strategia interna di monitoraggio della sicurezza, funzionale a tempestive azioni in caso di rischi o reali attacchi. Su questo aspetto numerose ricerche concordano che, per il monitoraggio a distanza, è indispensabile che l'accesso ai dati sensibili del paziente avvenga attraverso un'unica piattaforma dedicata online, previo inserimento di credenziali univoche; mentre chi progetta le tecnologie mediche salvavita deve aggiornare continuamente i software. Grazie anche a simili cautele, a oggi non si sono ancora osservati danni significativi ai pazienti portatori di pacemaker o defibrillatori come conseguenza di un attacco informatico. ■