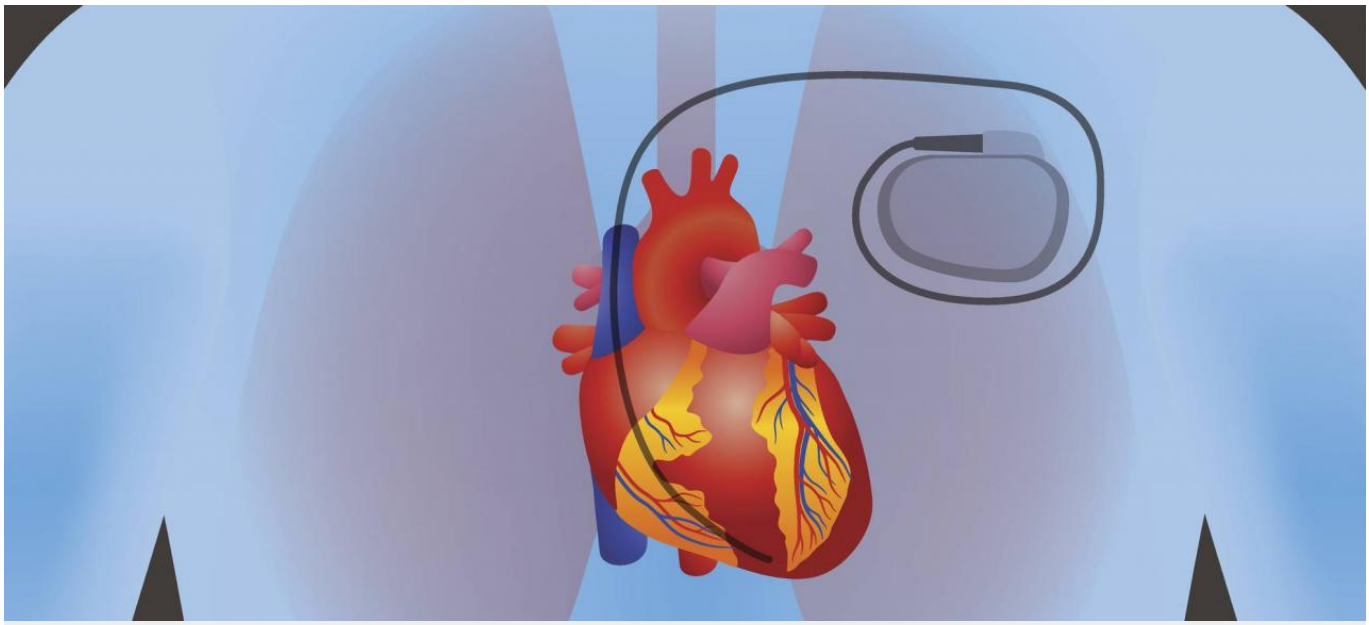
Tomasz Kobosz, 2017-09-01 13:01

Rozruszniki serca mogą być podatne na atak hakerów



Thinkstock/GettyImages

Stymulatory serca wyposażone są w funkcję bezprzewodowego dostępu. Umożliwia ona zmianę ustawień urządzenia bez konieczności nacinania powłok skórnych pacjenta. Niestety, może to także stanowić furtkę dla hakerów. Skutki włamania mogą być tragiczne.

Firma Abbott Laboratories wraz z Amerykańską Agencją ds. Żywności i Leków (FDA) wydały ostrzeżenie o podatności na zdalną, nieautoryzowaną modyfikację parametrów pracy partii ok. 465 tys. stymulatorów serca. Chodzi o urządzenia wyprodukowane przed 28 sierpnia 2017 przez firmę St Jude Medical (przejętą przez spółkę Abbott).

„Posiadający odpowiednią wiedzę haker mógłby uzyskać zdalny dostęp do stymulatora i sterować zdalnie (drogą radiowa) jego pracą” - napisano w liście rozesłanym przez firmę Abbott do lekarzy.

Pacjentów, którym wszczepiono stymulatory, poproszono o kontakt z lekarzem. Na szczęście luka jest możliwa do „załatania” poprzez zdalne wgranie nowszej wersji oprogramowania. Nie jest konieczna wymiana urządzeń, choć żadna ingerencja w oprogramowanie stymulatora nie jest w 100 proc. bezpieczna.

Zdaniem cytowanych przez "Science Alert" specjalistów w dziedzinie bezpieczeństwa cyfrowego, nie należy ulegać wrażeniu, że zdalne włamanie do stymulatora serca to science fiction, bo w rzeczywistości nie jest trudne do przeprowadzenia i może posłużyć np. jako metoda szantażu w celu wyłudzenia

pieniędzy. Wpływając drogą radiową na rytm serca, łatwo byłoby przekonać ofiarę, że jej życie lub śmierć zależy od jednego kliknięcia na ekranie komputera czy smartfona bandyty.

Zdaniem przedstawiciela FDA, jak dotąd nie odnotowano w USA ani jednego przypadku włamania do stymulatora serca. Wydaje się to jednak tylko kwestią czasu. Śledztwo dziennikarskie przeprowadzone przez portal "Ars Technica" wykazało, że zestawy urządzeń umożliwiające zdalny dostęp do stymulatorów można nabyć na czarnym rynku za kwotę od 15 do 3000 dolarów.