Cyberdefence 24

aut. Piotr Mieszkowski 30.05.2017

CYBERATAK NA ROZRUSZNIK SERCA? TO NAPRAWDĘ MOŻLIWE!

Osoby zmagające się z problemami zdrowotnymi, coraz częściej muszą korzystać urządzeń elektronicznych podtrzymujących lub stabilizujących funkcje życiowe. Mogą one jak np. rozruszniki serca paść ofiarą ataku hakerskiego, którego konsekwencje będą opłakane.

Najbardziej narażone na ryzyko cyberataku są urządzenia mające usterki w oprogramowaniu sterującym. Jak podaje portal gizmodo.com, który poinformował o tym nowym cyberzagrożeniu, ostatnio okazało się, że ważne urządzenia medyczne, takie jak pompy insulinowe i stymulatory serca, posiadają te same luki, co np. czajniki do herbaty połączone z siecią w ramach IoT, czyli internetu rzeczy.

W niedawno przeprowadzonym badaniu naukowcy z firmy zajmującej się cyberbezpieczeństwem WhiteScope przyjrzeli się rozrusznikom serca i defibrylatorom pochodzącym od czterech różnych producentów, a także systemom służącym do ich monitorowania i podtrzymywania. Znaleźli 8 000 różnych luk w kodzie urządzeń serca. Jest to bardzo duża liczba.

Naukowcy z WhiteScope stwierdzili, że wszystkie cztery urządzenia miały poważne problemy, w tym systemy oprogramowania, które nie były aktualne oraz zawierały prywatne dane pacjenta, które nie zostały zaszyfrowane. Gdy urządzenia zostały podłączone do systemów monitorowania, nie trzeba było loginu i hasła by sprawdzić do kogo należą i do czego służą te urządzenia oraz co zawierają.

Zdaniem naukowców przeprowadzających test urządzeń do wspomagania akcji serca pod kątem ich podatności na cyberwłamania, bezpieczeństwo stymulatorów serca jest poważnie zagrożone atakami hakerskimi. Informacja ta ma szczególne znaczenie w związku z atakiem ransomware Wanna Cry, który miał wpływ na działalność wielu szpitali na całym świecie. W przypadku WannaCry hakerom udało się zaatakować po raz pierwszy na świecie urządzenia medyczne, w tym przypadku sprzęt szpitalny firmy Bayer.

Czytaj też: Oprogramowanie ransmoware WannaCry stworzyli Chińczycy?

Cyberatak na sprzęt danego pacjenta może zagrażać jego życiu, ale nie tylko, gdyż po włamaniu do urządzenia hakerzy mogą wejść także w posiadanie jego dokumentacji medycznej, historii choroby, danych osobowych etc. Przed tym zjawiskiem od lat ostrzegają eksperci ds. cyberbezpieczeństwa. Już w 2013 roku hakerzy z grupy Barnaby Jack twierdzili, że są w stanie przejąć kontrolę nad rozrusznikiem serca z odległości nie dalszej niż 50 stóp i wywołać śmiertelne wstrząsy przy użyciu urządzenia.

Należy pamiętać, że aktualnie wiele nowych urządzeń medycznych ma wbudowaną opcję bezprzewodowego łączenia się z internetem. Były wiceprezydent USA Dick Cheney kazał lekarzom wyłączenie takiej funkcji w jego rozruszniku, gdyż było ryzyko, że może zostać użyty w cyberataku

przez cyberterrorystów.

Pomimo tego, że urządzenia medyczne są często stare i nieaktualne, a zatem bardziej podatne na ataki, do tej pory nie było znanych przypadków hakerów szkodzących pacjentom poprzez wykorzystanie tych luk. Jednak Agencja Żywności i Leków, FDA (Food and Drug Administration) oraz inne agencje są coraz bardziej zaniepokojone, co może się zdarzyć w niedalekiej przyszłości. W styczniu br. FDA wydała ostrzeżenie, że niektóre implanty serca mogą ulec cyberwłamaniu i zostać przeprogramowane w celu wysłania potencjalnie śmiertelnych sygnałów lub wstrząsów.

Jesienią ubiegłego roku firma Johnson & Johnson poinformowała swoich klientów, że jej pompy insulinowe mają luki w zabezpieczeniach, które hakerzy mogliby wykorzystać do wdrożenia potencjalnie śmiertelnego przedawkowania insuliny.

Według informacji portalu gizmodo.com, coraz więcej jest urządzeń medycznych dostępnych na rynku, które komunikują się bezprzewodowo, a zatem i zagrożenie atakami hakerskimi na te urządzenia. Według jednego z ostatnich badań tylko 17 proc. producentów urządzeń medycznych podjęło jakiekolwiek kroki w celu zabezpieczenia swoich produktów przed cyberatakami.