Anestezjologia • Ratownictwo • Nauka • Praktyka / Anaesthesiology • Rescue Medicine • Science • Practice

ARTYKUŁ POGLĄDOWY / REVIEW PAPER
Otrzymano/Submitted: 10.05.2023 • Zaakceptowano/Accepted: 28.09.2023

Bezpieczeństwo zdalnej kontroli kardiologicznych urządzeń wszczepialnych w ujęciu medycznym i kryminalistycznym

Safety of remote control of cardiological implantable devices from a medical and forensic perspective

Katarzyna Knap[1], Szymon Nawrocki[2]

[1] Wydział Lekarski, *Collegium Medicum* w Bydgoszczy, Uniwersytet Mikołaja Kopernika w Toruniu

[2] Wydział Stosowanych Nauk Społecznych i Resocjalizacji, Instytut Profilaktyki Społecznej i Resocjalizacji, Uniwersytet Warszawski

Streszczenie

Celem artykułu jest przedstawienie zagadnień związanych z bezpieczeństwem zdalnej kontroli kardiologicznych urządzeń wszczepialnych. W związku z czym skupiono się na aspekcie medycznym tak, by móc ukazać jakie zagrożenia niesie za sobą niedbałość w zakresie cyberbezpieczeństwa tych urządzeń. Aspekt kryminalistyczny skupia się na przedstawianiu potencjalnych motywów jakimi mogliby kierować się cyberprzestępcy w celu przejęcia zdalnej kontroli nad sprzętem medycznym, a także metodami jakich mogliby do tego użyć. Przedstawione zostały także środki prewencyjne jakie należy stosować w celu zapobiegania incydentom związanym z cyberbezpieczeństwem, zaprezentowano trójstopniowy podział ról w zakresie dbania o bezpieczeństwo urządzeń wszczepialnych. *Anestezjologia i Ratownictwo 2023; 17: 245-253. doi:10.53139/AIR.20231728*

Słowa kluczowe: cyberprzestępczość, kradzież danych, telemonitoring, zdalna kontrola kardiologicznych urządzeń wszczepialnych

Abstract

The aim of the article is to present issues related to the security of remote control of cardiac implantable devices. Therefore, the focus was on the medical aspect to be able to show what risks are posed by negligence in the field of cybersecurity of these devices. The forensic aspect focuses on presenting the potential motives that cybercriminals could use to take remote control of medical equipment, as well as the methods they could use to do so. Preventive measures that should be used to prevent incidents related to cybersecurity were also presented, and a three-stage division of roles in the field of ensuring the security of implantable devices was presented. *Anestezjologia i Ratownictwo 2023; 17: 245-253. doi:10.53139/AIR.20231728*

Keywords: cybercrime, data theft, telemonitoring, remote control of cardiac implantable devices

Cel pracy

Celem pracy jest zaprezentowanie zagrożeń jakie mogą wystąpić w przypadku ataku na kardiologiczne urządzenia wszczepialne. Postawiono w niej następujące pytanie badawcze: Czy zagrożenia związane z telemonitoringiem kardiologicznych urządzeń wszczepialnych są rzeczywiste i czy należy się ich bać? Aby na nie odpowiedzieć autorzy skupiają się na interdyscyplinarnym podejściu do przedmiotowego zjawiska, w tym celu zaprezentowany przedmiot jest zarówno w ujęciu medycznym jak i kryminalistycznym, co pozwala na szersze spojrzenie na to zagadnienie. Istotnym celem było wskazanie kierunku w jakim należy kroczyć w celu polepszenia cyberbezpieczeństwa zdalnej kontroli kardiologicznych urządzeń wszczepialnych. Przeanalizowano w tym celu incydenty jakie wystąpiły w przeszłości i opracowano trójstopniowy podział ról w zakresie dbania o bezpieczeństwo urządzeń, które działają w ramach telemonitoringu.

Materiał i metody

W niniejszej pracy autorzy skupiają się przede wszystkim na jakościowej analizie treści, która była przeprowadzona na podstawie fachowej literatury przedmiotu, a także dokonano przeglądu źródeł internetowych pochodzących ze specjalistycznych stron branżowych. Praca uzupełniona jest o element badań własnych polegający na wystosowaniu zapytań do firmy dostarczającej usługi związane z kardiologicznymi urządzeniami wszczepialnymi.

Wstęp

W dobie powszechnego dostępu do najnowszych rozwiązań technologicznych, z każdą mijającą dekadą obserwowany jest rozwój skutkujący wzrostem zasobności rynku wszczepialnych urządzeń medycznych. Celami obieranych strategii firm produkujących wyroby medyczne są m.in. zwiększanie dostępności terapii i komfortu pacjenta, stopniowe odciążenie służby zdrowia na całym świecie oraz zwiększanie bezpieczeństwa stosowanych środków.

Obecne na rynku urządzenia diagnostyczne i terapeutyczne, mogą być zarówno wszczepialne, jak i noszone na ciele pacjenta oraz używane zarówno w placówce medycznej jak i w domu pacjenta. Medyczne urządzenia bezprzewodowe spełniają swoje funkcje wykorzystując komunikację za pomocą fal radiowych, Wi-Fi oraz Bluetooth [1]. Dostęp do sieci komórkowej oraz Internetu umożliwia wykonanie takich procedur jak zdalny monitoring niektórych urządzeń wszczepialnych (m.in. Abbot – Merlin.Net™, Biotronik - Home Monitoring™, Boston Scientific - Latitude™, Medtronic - CareLink™). Udowodniono, iż zdalne monitorowanie zmniejsza liczbę wizyt pacjenta na oddziale ratunkowym, pilnych wizyt w gabinecie lekarskim oraz całkowite wykorzystanie opieki zdrowotnej przez pacjentów z implantowanymi kardiowerterami-defibrylatorami lub defibrylatorami do terapii resynchronizującej [2,3]. Przyczyniają się do tego między innymi możliwość wczesnego wykrycia napadów migotania przedsionków, co pozwala na profilaktyczne włączenie do terapii leków antykoagulacyjnych i obniżenie ryzyka sercowo-naczyniowego [4].

Czy jest się czego bać?

Obecnie stosowane urządzenia do zdalnego monitorowania kardiologicznych urządzeń wszczepialnych zapewniają bezpieczeństwo na zadowalającym poziomie, niemniej w mediach, jak i w opracowaniach naukowych można spotkać się z opiniami mówiącymi o zagrożeniach, jakie niesie za sobą ta technologia. W związku z tym pojawia się pytanie, czy jest się czego bać? Postęp zawsze budzi obawy, jednakże trzeba mieć na uwadze, że „*zhackowanie*" takiego urządzenia nie jest wcale proste, nie oznacza to jednak, że nie jest niemożliwe [5]. Każde urządzenie, które komunikuje się za pomocą sieci może zostać przejęte. Niemniej w przypadku urządzeń o tym charakterze należy zastanowić się nad tym, co musiałoby skłonić przestępcę do ataku i czy rzeczywiście chciałby przyczynić się do ewentualnej śmierci człowieka, która mogłaby podlegać klasyfikacji jako zabójstwo. Przestępstwa przeciwko życiu są zagrożone jednymi z najbardziej surowych sankcji karnych. Ponadto zabić człowieka można w inny, mniej skomplikowany technicznie sposób, zwłaszcza jeśli jest to osoba, która ma problemy z sercem.

Atak na pacjenta w celu wyłudzenia pieniędzy przypominający *ransomware* (jest to typ szkodliwego oprogramowania, które przez szyfrowanie blokuje dostęp do systemu komputerowego, albo uniemożliwia odczyt danych [6]) jest również mało prawdopodobny. Po pierwsze taka osoba musiałaby być poinformowana o tym, kiedy i jak ma zapłacić okup, taka informacja musiałaby się wyświetlić na monitorze urządzenia

służącego do nadzoru urządzenia wszczepialnego, co nawet jeśli byłoby technicznie możliwe to od razu zaalarmowałoby pacjenta, który zadzwoniłby do szpitala a o sprawie dowiedziałaby się dzięki temu firma dostarczająca urządzenie. Co więcej odbiorcami tych urządzeń są przede wszystkim osoby starsze, które najprawdopodobniej nie potrafiłyby zapłacić środkami płatności, które uniemożliwiłyby łatwe namierzenie sprawcy (np. kryptowaluty). Atak na konkretną osobę nie miałby sensu, gdyż od razu alarmowałby firmę, jak i organy ścigania, co więcej można by to potraktować jako usiłowanie zabójstwa, w związku z czym ryzyko mogłoby się okazać zbyt duże dla przestępcy. Dostrzegamy jednak element, który jest w stanie znaleźć się w zainteresowaniu cyberprzestępców. Są to bazy danych firm dostarczających oprogramowania, które uzupełniane są każdego dnia przez tysiące pacjentów na całym świecie. W przypadku ich wycieku firma, która przetwarza te dane, czy też sam szpital w mniejszej skali mogliby mieć bardzo duże problemy ze względu na skutki jakie niesie za sobą takie zdarzenie. Taki scenariusz jest bardziej prawdopodobny ze względu na to, że cyberprzestępca nie ryzykowałby już odpowiedzialnością za usiłowanie zabójstwa, a odpowiadałby tak jak w przypadku zwykłego ataku ransomware. Istotnym jest także, by personel placówki medycznej obsługującej pacjenta należycie podchodził do kwestii związanych z cyberbezpieczeństwem, chodzi tu przede wszystkim o komputery i stosowane zabezpieczenia.

Wpływ hackingu urządzenia na zdrowie i życie pacjenta:

1) Zagrożenia związane z utratą danych osobowych:
   A) Głównym oraz najbardziej potencjalnym zagrożeniem tak jak wspomniano jest kradzież danych osobowych pacjenta, będących częścią dokumentacji medycznej wgranej do urządzenia. Każde urządzenie posiada własny numer seryjny, będący jego identyfikatorem. Istnieje możliwość zaprogramowania numerów seryjnych połączonych elektrod w pamięci urządzenia. W trakcie lub tuż po implantacji urządzenia personel medyczny dokonuje kodowania danych osobowych pacjenta przy użyciu programatora urządzeń wszczepialnych. Do danych tych należą m.in. imię, nazwisko, PESEL, data urodzenia, data wszczepienia urządzenia, wskazanie do implantacji, objawy, informacje o tym czy pacjent jest zależny od stymulacji a także imię, nazwisko i numer telefonu operatora/asystenta [7].
2) Zagrożenia związane z narażeniem życia lub zdrowia pacjenta:
   A) Zagrożona stymulacja z powodu *oversensingu* - zwiększonej czułości urządzenia na pobudzenia własne układu bodźco-przewodzącego, nie będące zespołem QRS i nie dające dostatecznego efektu hemodynamicznego. Ma to szczególne znaczenie u pacjentów zależnych od stymulacji, gdyż w wyniku jej braku może nastąpić asystolia, a w konsekwencji omdlenie lub zgon [8]. W przypadku użytkowania wszczepialnego kardiowertera-defibrylatora błędna analiza pobudzeń elektrycznych przeprowadzona przez urządzenie może doprowadzić do nieadekwatnych wyładowań, w tym również wyładowań zagrażającym życiu pacjenta. Dotyczy to także silnych zakłóceń elektromagnetycznych, które mogą towarzyszyć elektrokoagulacji, spawaniu oraz pracy przy transformatorach elektrycznych wysokiego napięcia [3].
   B) Nagłe rozładowanie baterii może skutkować brakiem stymulacji, niedostarczeniem terapii, brakiem monitoringu oraz zapisu danych we wszystkich rodzajach wszczepialnych urządzeń kardiologicznych. Przed całkowitym rozładowaniem, w przypadku przejścia urządzenia w tryb ERI (Elective replacement indication) może nastąpić zmiana trybu stymulacji w tryb VVI (stymulacja komorowa hamowana własną aktywnością komór), zmiana częstości stymulacji oraz zmiana napięcia stymulacji [9]. Powyższe zmiany mogą dawać obraz kliniczny zaostrzenia choroby będącej przyczyną wszczepienia urządzenia, nasilenia subiektywnych odczuć pacjenta oraz w szczególnych przypadkach odczuwalną przez pacjenta stymulację nerwu przeponowego [10,11]. Stadium drugim rozładowania baterii jest tryb EOL (end of life) lub EOS (end-of-service) - skutkuje on wystąpieniem objawów klinicznych choroby podstawowej i brakiem funkcjonowania urządzenia [12,13].
   C) Zmiany wartości częstości stymulacji, zawarte

przez Muddy Waters w raporcie przeciwko Saint Jude Medical (obecnie: Abbott) mogą dotyczyć stymulacji ze zbyt wysoką częstością. Zbyt szybka stymulacja prowadzi do tachykardii, która może powodować objawy, wśród występujących: uczucia kołatania serca, ból w klatce piersiowej, duszność, zawroty głowy i stan przedomdleniowy [14]. Poza kwestią szybkiej stymulacji, raport traktuje również o możliwości zamierzonego rozładowania baterii o czym wspomniano w poprzednim akapicie.

D) Zakłócenie bezprzewodowej komunikacji urządzenia ze zdalnym monitoringiem jest możliwe dla hackera operującego na tej samej częstotliwości co wszczepione urządzenie. Skutkiem takiego ataku może być brak wykrycia epizodów arytmicznych przez obsługę telemonitoringu i brak podjęcia działań terapeutycznych przez personel medyczny [3].

E) Przerwanie transmisji radiowej do stacji telemonitoringu jest możliwe przy nadmiernej częstości połączeń telemetrycznych. Zachodzi ono w celu ochrony żywotności baterii, przy nadal zachowanej podstawowej funkcji urządzenia (tj. stymulacji o określonej częstości 60/min.) oraz hamowania stymulacji przy wykryciu potencjalnych pobudzeń własnych. Zjawisko to wykazano na modelu Assurity SR Pacemaker firmy St. Jude Medical [15].

Możliwości przejęcia urządzeń w celu wyrządzenia szkody dla życia i zdrowia pacjenta

W celu ingerencji w funkcjonowanie kardiologicznych urządzeń wszczepialnych cyberprzestępca może korzystać z wielu metod, niemniej potencjalne ataki mogłyby się opierać na jednym z poniżej wymienionych wariantów:

1) Zakłócenie lub przejęcie komunikacji między urządzeniem a monitorem przy użyciu radia programowalnego SDR w celu przechwycenia komunikatów przekazywanych za pomocą sygnałów radiowo – falowych (RF) [23]
2) Ingerencja w działanie urządzenia poprzez wgranie szkodliwego oprogramowania poprzez port USB Monitora[23]. Warto w tym miejscu zaznaczyć, że ten wariant jest mało prawdopodobny ze względu na to, że sprawca musiałby mieć bezpośredni dostęp do urządzenia ofiary.
3) Wprowadzenie *malware* poprzez *backdoor* oprogramowania monitora w celu późniejszej ingerencji w funkcjonowanie urządzenia [23]. Wbrew pozorom nie jest to wcale niemożliwe ze względu na to, że *backdoory* pozostawiane są przez programistów dość często, a wykrywane są dopiero po latach. W założeniu ma on ułatwić pracę, niemniej w momencie, gdy cyberprzestępca uzyska do takiego dostęp może on z łatwością manipulować kodem oprogramowania, jednocześnie zakłócając prawidłowe funkcjonowanie. Może być także pozostawiony przez hackera, który dostał się do oprogramowania w inny sposób.
4) Wysyłanie ciągłych zapytań w celu nawiązania połączenia i wysyłania poleceń do urządzenia [23]. Takie działanie pozwalałoby na szybsze rozładowanie się baterii, co może zagrozić już zdrowiu i życiu pacjenta. W momencie, gdy urządzenie funkcjonuje w sposób normalny bateria może działać przez kilka lat a o jej potrzebie urządzenie informuję operatora obsługującego system telemetryczny. W sytuacji zaś, gdy wymuszono by jej szybsze rozładowanie przy jednoczesnym zablokowaniu komunikacji z systemami dostawcy usługi jak i szpitala, wszczepione urządzenie przestanie prawidłowo funkcjonować, a by je wymienić potrzebna jest już operacja.
5) Dostęp do urządzenia poprzez wgranie złośliwego kodu do aktualizacji systemu, lub poprzez wtargnięcie do sieci lokalnej do której podłączone jest urządzenie [23] Taki wariant wydaje się dość mało prawdopodobny ze względu na to, że systemy firm dostarczających usługi są bardzo dobrze zabezpieczone.

Obecnie stosowane zabezpieczenia związane z cyberbezpieczeństwem kardiologicznych urządzeń wszczepialnych

W celu zweryfikowania sposobów zabezpieczenia systemów przez dostawców świadczących usługi związane z kardiologicznymi urządzeniami wszczepialnymi, wystosowaliśmy zapytanie do jednego z czołowych dostawców tego rodzaju sprzętu – firmy Biotronik. Wystosowaliśmy zapytanie o to, czy uży-

wają uwierzytelnienia wielopoziomowego w swoich produktach, a także jak wygląda polityka haseł i czy mają oni jakieś specjalne wymagania wobec klientów co do ich używania, co więcej poprosiliśmy o ustosunkowanie się do tego, czy przeprowadzają szkolenia dla klientów w tym lekarzy. Na zadane przez nas pytania otrzymaliśmy odpowiedzi, które prezentujemy poniżej:

1) Wdrożono uwierzytelnianie dwuskładnikowe (2FA) dla wszystkich klientów (szpitale), którzy mogą wprowadzić je dla swoich użytkowników. Proces autentyfikacji opiera się na haśle generowanym czasowo np. w formie kodu przy użyciu aplikacji Google Authenticator.
2) W kwestii polityki haseł wdrożone są procedury, które są aktualizowane zgodnie z aktualnymi trendami branżowymi. Firma zachęca klientów do tworzenia silnych i unikalnych haseł. (nie ma podanych szczegółów)
3) Firma oferuje szkolenia dla klientów w zakresie obsługi z obsługi systemu, w tym z zarządzania użytkownikami i kontami. Zaznaczono przy tym, że zakres szkolenia może się różnić w zależności od wymagań klienta i kraju.

Aby dowiedzieć się jak wygląda sytuacja w placówce, która wykorzystuje rozwiązania tej firmy, wystosowaliśmy zapytanie do jednego z wiodących polskich ośrodków leczenia chorób serca, gdzie pytaliśmy m.in. o szkolenia dla pracowników. Zapytaliśmy także o kwestie związane z potencjalnym zagrożeniem dla danych pacjentów, niemniej w związku z brakiem odpowiedzi placówki, z uwagi na dobro danych pacjenta nie opublikujemy reszty naszego zapytania.

Wybrane incydenty związane z cyberbezpieczeństwem kardiologicznych urządzeń wszczepialnych

Pomimo tego, że zdalnie sterowane kardiologiczne urządzenia wszczepialne obecnie należą do sprzętów, które ratują życie, nie oznacza to automatycznie, że nie mogą mu zaszkodzić. W przeszłości mieliśmy do czynienia z wykrytymi lukami w zabezpieczeniach takich urządzeń. W naszej pracy skupiliśmy się na kilku wybranych tak, by móc zobrazować do czego ewentualny (choć mało prawdopodobny) atak mógłby doprowadzić

1) W 2019 750 tys. rozruszników marki Biotronik było podatnych na atak poprzez luki w oprogramowaniu. Występowały one w protokole komunikacji Connexus i dotyczyły w sumie 16 modeli urządzeń. Jedna z luk pozwalała na odczytywanie danych z urządzenia, które było atakowane, druga zaś dotyczyła monitorowania danych pomiędzy dwoma skomunikowanymi ze sobą urządzeniami, w tym przypadku najczęściej chodziło o stymulator i monitor zdarzeń arytmicznych [16]. Co ciekawe Departament Bezpieczeństwa Krajowego USA przypisał podatnościom wskaźnik na poziomie 9,3/10 [17] co świadczy o poważnym traktowaniu tematu. Niemniej żaden z 750 tys narażonych na ryzyko rozruszników nie został zhackowany, a urządzenia zostały szybko zaktualizowane i należycie zabezpieczone.
2) Niepokojący raport z 2017 r. Buttsa i Riosa z Whitescope [18], który zawiera informację na temat ponad 8 tysięcy luk w 4 programatorach od 4 różnych producentów. Co ciekawe do swoich badań posłużyli się autentycznymi urządzeniami, które „rozłożyli" na części pierwsze. Analiza urządzeń wykazała ich dużą prymitywność w zakresie stosowanej technologii m.in. urządzenia funkcjonowały na starych systemach tj. Windows XP, a jedno z nich korzystało z OS/2 (system stworzony przez IBM i Microsoft w 1987roku). Stwierdzono także to, że producenci nie stosowali technik umożliwiających wsteczną inżynierię *firmware'u*, co więcej system plików nie był szyfrowany [19].
3) Na oficjalnej stronie FDA (U.S. Food and Drug Administration) zostały zamieszczone kolejne komunikaty dotyczące zagrożenia cyberbezpieczeństwa urządzeń wszczepialnych.
   A) List ostrzegawczy z dnia 12 kwietnia 2017r. dotyczący m.in. braku potwierdzenia zakończenia działań korygujących i zapobiegawczych, w tym pełnego zbadania pierwotnej przyczyny oraz określenia działań korygujących i zapobiegawczych ponownemu wystąpieniu potencjalnych luk w zabezpieczeniach cybernetycznych dotyczących nadajnika *Merlin@home* firmy St. Jude Medical (obecnie Abbott) [20]. Bezpośrednim powodem na wystosowanie wspomnianego pisma była publikacja raportu [12] z dnia 25 sierpnia 2016 roku przez Muddy Waters Research©.
   B) Komunikat z dnia 11 października 2018 r. dotyczący wykrycia luki w oprogramowaniu dwóch modeli programatorów firmy

Medtronic – *Carelink* oraz *Carelink Encore*. Tego samego dnia FDA zatwierdziło aktualizację oprogramowania firmy Medtronic jako działanie naprawcze firmy [21,22].

Wymienione wyżej incydenty z zakresu cyberbezpieczeństwa kardiologicznych urządzeń wszczepialnych pokazują, że urządzenia te były i nadal są narażone na ataki, niemniej dotychczas okazywały się nieatrakcyjnym celem dla cyberprzestępców, o czym świadczy brak ataków. Nie oznacza to jednak, że nie należy traktować tego zagrożenia poważnie. To, że obecnie nie ma popytu na ten rodzaj przestępczości nie oznacza tego, że należy pozostawiać otwarte drzwi dla potencjalnych sprawców. Sytuacyjne zapobieganie przestępczości w tym wypadku nie jest widoczne na pierwszy rzut oka ze względu na to, że nie doszło do czynów przestępczych o tym charakterze, w związku z czym nie da się obniżyć skali przestępczości, gdyż takowa nie istnieje. Nie prowadzi się także badań dotyczących kwestii udziału (lub braku udziału) urządzenia w mechanizmie zgonu pacjenta z implantowanym urządzeniem kardiologicznym. W Polsce nie wykonuje się także rutynowych odczytów danych z urządzenia u denata, gdy do śmierci pacjenta nie doszło w wyniku udziału osób trzecich. W przypadku jednak gdybyśmy zaprzestali działań mających na celu dalsze zapobieganie, czyny o tym charakterze mogłyby się pojawiać, co niosłoby za sobą poważne konsekwencje ze względu na specyfikę funkcjonowania tych urządzeń.

Trójstopniowy podział ról w zakresie cyberbezpieczeństwa kardiologicznych urządzeń wszczepialnych – filary zapewnienia bezpieczeństwa pacjentom

1. Rola lekarza

Najważniejszą i pierwszą linią obrony przed cyberatakami jest zapobieganie. Z tego powodu należy zwracać uwagę na używanie silnego, unikalnego i niedostępnego dla osób trzecich[24] hasła do programów przetwarzających dane pacjentów oraz używanie haseł do kodowanych maili służbowych, gdy wysyłane są dane medyczne pacjenta.

Rola lekarza powinna się sprowadzać do zapoznania pacjenta z tym, jak ma on korzystać z urządzenia w sposób bezpieczny, na co należy uważać i kiedy należy zgłosić się po pomoc z urządzeniem. Trzeba mieć na uwadze, że pacjent nie wybiera sobie choroby, stawiany jest on przed zaistniałym stanem rzeczy i nie do końca może wiedzieć nawet co się z nim dzieje, dlatego tak ważne jest to, by lekarz posiadał fachową wiedzę odnośnie do słabych stron urządzenia, które posiada pacjent, celem ostrzeżenia przed potencjalnymi zagrożeniami. Jeśli lekarz sam nie będzie wiedział co należy zrobić w sytuacji kryzysowej związanej z urządzeniem, nie można tego wymagać tym bardziej od pacjenta. Nie jest kwestią posiadanie wyspecjalizowanej wiedzy informatycznej, ale podstaw związanych z użytkowaniem tego urządzenia, a także ustaleniu awaryjnej drogi komunikacji, która może posłużyć w momencie awarii lub ataku na urządzenie. Dobrym przykładem tego w jaki sposób realizowane jest wprowadzenie w tematykę użytkowania urządzenia do telemonitoringu jest Śląskie Centrum Chorób Serca w Zabrzu. Nie robią oni go na oddziale po zabiegu pacjenta, ale później w poradni, gdzie co istotne na spotkanie zapraszany jest pacjent wraz z rodziną tak, by wiedza została przekazana kilku osobom. Należy mieć przy tym na uwadze, że dla chorego jest to ciężki czas, gdyż wiele się zmienia w jego życiu, stąd tak ważne by w tym procesie uczestniczyły inne osoby, by zminimalizować ryzyko wystąpienia późniejszych problemów [25].

Przydatnym narzędziem, które może pomóc lekarzowi w tym procesie jest lista kroków zaleconych przez FDA, które powinien podjąć lekarz celem zwiększenia cyberbezpieczeństwa urządzeń wszczepialnych swoich pacjentów [26,27].

Lekarz powinien:

1) Rozważyć w jakim zakresie cyberbezpieczeństwo łączy się z użytkowaniem urządzenia.
2) Posiadać spis połączonych urządzeń (dotyczy telemonitoringu).
3) Zastanowić się w jaki sposób lekarz oraz pacjent korzystają z tych urządzeń i jaki jest poziom ich bezpieczeństwa (np. za pomocą telefonu komórkowego).
4) Rozważyć zdrowie, prywatność i bezpieczeństwo związane z potencjalnym ryzykiem utraty kontroli nad urządzeniem.
5) Rozważyć w jaki sposób urządzenie uzyskuje połączenie (sieć GSM, sieć Wi-Fi, Bluetooth).
6) Dowiedzieć się od specjalistów czy firma posiada odpowiednie certyfikaty cyberbezpieczeństwa oraz odpowiednie rozwiązania problemów.
7) Ustalić co może się wydarzyć, gdy połączenie z urządzeniem zostanie zerwane (w przypadku telemonitoringu).

8) Jakie jest potencjalne ryzyko kliniczne dla pacjenta będącego użytkownikiem danego urządzenia.
9) Do kogo może się zgłosić, jeśli ma jakieś pytania.
10) Prowadzić aktualizację urządzeń po każdym piśmie wystosowanym przez firmę, reagować na wszelkie powiadomienia dotyczące konkretnych partii produktów oraz postępować zgodnie z wytycznymi towarzystw kardiologicznych.

Autorzy niniejszego artykułu uważają, iż instrukcja w obszerny i wyczerpujący sposób opisuje zalecenia postępowania lekarza. Niemniej w realiach dzisiejszej ochrony zdrowia oraz faktu przeładowania pracą personelu medycznego, niemożliwym może być zastosowanie jej w codziennej praktyce. Istnieje potrzeba podziału obowiązku przestrzegania zaleceń na cały zespół terapeutyczny oraz wyznaczenia przedstawiciela posiadającego kompetencje dotyczące cyberbezpieczeństwa ze strony producenta urządzeń na dany rejon geograficzny lub poszczególne jednostki medyczne.

2. Rola pacjenta

Przede wszystkim należy mieć na uwadze to, że zgoda na telemonitoring jest dobrowolna, to pacjent decyduje o tym, czy chce się poddać tej formie leczenia. Oczywiście powinien sugerować się zaleceniami lekarza, niemniej do niego należy ostatnie słowo. Podstawowym zadaniem pacjenta jest dbanie o to, by jego urządzenie transmitujące dane było stale podpięte pod źródło zasilania, a także dbanie o jego stan fizyczny, odpowiednie jego zabezpieczenie. Istotnym jest także to, by informował on personel medyczny o wszelkich widocznych odstępstwach od normy, jeśli chodzi o jego funkcjonowanie.

Do obowiązków pacjenta, którego urządzenie ma być podłączone do telemonitoringu należą[3]:
1) Sprawowanie fizycznej kontroli nad posiadaniem urządzenia.
2) Podłączanie urządzeń do źródeł, które są rekomendowane przez producenta.
3) Rejestracja urządzenia na stronie producenta przez pacjenta lub jego rodzinę.
4) Reagowanie na pojawiające się powiadomienia, problemy lub nietypowe zachowania urządzenia.

3. Rola producenta oprogramowania

Producent powinien przede wszystkim na etapie projektowania urządzenia wdrożyć odpowiednie działania względem cyberbezpieczeństwa, które obejmowałyby m.in. późniejszą łatwą możliwość wprowadzenia aktualizacji luk w oprogramowaniu[5]. System powinien także umożliwiać na wgląd do dziennika logowania tak, by w przyszłości można było nadzorować kto przegląda dane użytkowników. Ważnym jest także by o wszelkich zagrożeniach, czy też podatnościach informować odbiorców, nie ma nic gorszego niż ukrywanie prawdy[23]. Firmy tworzące tego rodzaju urządzenia powinny mieć także dobrze przygotowany plan działania na wypadek utraty danych swoich pacjentów np. w przypadku ataku *ransomware*, jest to o tyle ważne ze względu na to, że w momencie, gdy dojdzie do takiego incydentu działa się według określonych procedur, pozwala to na uniknięcie paniki i dalszego chaosu. Dobrą praktyką, której powinien poddawać się producent są regularne testy penetracyjne, pozwalające na wskazanie słabych stron i ich eliminacje [28].

Podsumowanie

Mimo zaistniałych naruszeń bezpieczeństwa, w sprawie których FDA wydało oświadczenia, nadal nie podano do informacji publicznej zarejestrowanych wydarzeń, które mogłyby mieć negatywny wpływ na zdrowie i bezpieczeństwo pacjentów[29]. *Hacking* urządzeń wszczepialnych nie stanowi obecnie poważnego problemu klinicznego na dużą skalę[3]. Przy braku udowodnionego klinicznie zagrożenia dla bezpieczeństwa pacjentów, warto brać pod uwagę klinicznie udowodnione korzyści wynikające z zastosowania kardiologicznych urządzeń wszczepialnych. Ze względu na to, iż żadne oprogramowanie ani sprzęt medyczny nie jest wolny od ryzyka, producenci stale powinni udoskonalać systemy nowych urządzeń oraz aktualizacje starszych, aby utrzymać wysoki poziom ochrony przed zagrożeniem cyberbezpieczeństwa[15]. Szczególnie ważnym tematem jest edukacja personelu medycznego w zakresie możliwości wystąpienia incydentów o charakterze cyberzagrożeń. Należy także zaznaczyć, że pomimo prób nawiązania kontaktu z dużym polskim ośrodkiem zajmującym się chorobami serca w sprawie związanej z potencjalnym zagrożeniem, autorzy nie otrzymali odpowiedzi, co budzi poważne zastrzeżenia jak i stwarza problemy przy tego rodzaju badaniach ze względu na brak chęci współpracy placówek w tym zakresie. Nawet najbardziej zaawansowany sprzęt czy system posiada słaby punkt, zazwyczaj jest to człowiek. Z tego powodu tak ważna jest edukacja w tym zakresie.

Konflikt interesów / Conflict of interest
Brak/None

ORCID
Katarzyna Knap 0000-0002-0404-9966
Szymon Nawrocki 0000-0002-7578-6947

Adres do korespondencji / Correspondence address
Katarzyna Knap
Wydział Lekarski, *Collegium Medicum* w Bydgoszczy,
Uniwersytet Mikołaja Kopernika w Toruniu
ul. Jagiellońska 13, 85-067 Bydgoszcz
☎ (+48 52) 585 33 96
321544@stud.umk.pl

Piśmiennictwo/References

1. U.S. Food and Drug Administration. Information on medical devices that incorporate radio frequency (RF) wireless technology [Internet]. [cytowane 24 marzec 2023]. Dostępne na: https://www.fda.gov/medical-devices/digital-health-center-excellence/wireless-medical-devices.
2. Landolina M, Perego GB, Lunati M, Curnis A, Guenzati G, Vicentini A, i in. Remote Monitoring Reduces Healthcare Use and Improves Quality of Care in Heart Failure Patients With Implantable Defibrillators. Circulation. 19 czerwiec 2012;125(24):2985–92.
3. Cybersecurity for Cardiac Implantable Electronic Devices: What Should You Know? - ScienceDirect [Internet]. [cytowane 24 marzec 2023]. Dostępne na: https://www.sciencedirect.com/science/article/pii/S0735109718302006?via%3Dihub.
4. Ricci RP, Morichelli L, Gargaro A, Laudadio MT, Santini M. Home Monitoring in Patients with Implantable Cardiac Devices: Is There a Potential Reduction of Stroke Risk? Results from a Computer Model Tested Through Monte Carlo Simulations. Journal of Cardiovascular Electrophysiology. 2009;20(11):1244-51.
5. Alexander B, Haseeb S, Baranchuk A. Are implanted electronic devices hackable? Trends in Cardiovascular Medicine. listopad 2019;29(8):476-80.
6. Banasiński C, Rojszczyk M, redaktorzy. Cyberbezpieczeństwo. Warszawa: Wolters Kluwer; 2020.
7. Medtronic©. EnPulse Pacemaker Programming Guide. s. 92.
8. Safavi-Naeini P, Saeed M. Pacemaker Troubleshooting: Common Clinical Scenarios. Texas Heart Institute Journal. 1 październik 2016;43(5):415-8.
9. Sinha SK, Chrispin J, Barth A, Rickard J "Jack", Spragg DD, Berger R, i in. Clinical recognition of pacemaker battery depletion and automatic reprogramming: SINHA ET AL . Pacing Clin Electrophysiol. sierpień 2017;40(8):969-74.
10. Biffi M, Bertini M, Ziacchi M, Gardini B, Mazzotti A, Massaro G, i in. Management of Phrenic Stimulation in CRT Patients over the Long Term: Still an Unmet Need ?: PHRENIC STIMULATION MANAGEMENT AT FOLLOW-UP. Pacing and Clinical Electrophysiology. październik 2011;34(10):1201-8.
11. Liu J, Wen L, Yao S, Zheng P, Zhao S, Yang J. Adverse clinical events caused by pacemaker battery depletion: two case reports. BMC Cardiovasc Disord. grudzień 2020;20(1):344.
12. MW is Short St. Jude Medical (STJ:US) [Internet]. Muddy Waters Research. 2016 [cytowane 24 marzec 2023]. Dostępne na: https://www.muddywatersresearch.com/research/stj/mw-is-short-stj/.
13. Lappegård KT, Moe F. Remote Monitoring of CIEDs—For Both Safety, Economy and Convenience? International Journal of Environmental Research and Public Health. styczeń 2022;19(1):312.
14. Andrzej Szczeklik, Piotr Gajewski. Choroby układu krążenia 6. Zaburzenia rytmu serca. W: Podręcznik Interna – Medycyna Praktyczna. s. 232-3.
15. Ransford B, Kramer DB, Foo Kune D, Auto de Medeiros J, Yan C, Xu W, i in. Cybersecurity and medical devices: A practical guide for cardiac electrophysiologists. Pacing Clin Electrophysiol. sierpień 2017;40(8):913-7.
16. Rymsza A. 750 tys. rozruszników serca podatnych na atak. Mają je także polscy pacjenci [Internet]. [cytowane 12 kwiecień 2023]. Dostępne na: https://www.dobreprogramy.pl/750-tys-rozrusznikow-serca-podatnych-na-atak-maja-je-takze-polscy-pacjenci,6628561882101889a
17. Cybersecurity and Infrastructure Security Agency. Medtronic Conexus Radio Frequency Telemetry Protocol (Update C).
18. WhiteScope IO. Understanding Pacemaker Systems Cybersecurity [Internet]. 2023. Dostępne na: http://blog.whitescope.io/2017/05/understanding-pacemaker-systems.html.
19. Maj M. Rozruszniki serca można zhackować. Także zdalnie. [Internet]. 2023. Dostępne na: https://niebezpiecznik.pl/post/rozruszniki-serca-mozna-zhackowac-takze-zdalnie/.
20. Abbott (St Jude Medical Inc.) - 519686 - 04/12/2017 [Internet]. U.S. Food and Drug Administration. FDA; 2020 [cytowane 23 marzec 2023]. Dostępne na: https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/abbott-st-jude-medical-inc-519686-04122017.
21. Wydział Świadczeń Opieki Zdrowotnej. Telemetryczny nadzór nad pacjentami z implantowanym automatycznym systemem do kardiowersji lub defibrylacji (ICD) lub układem resynchronizującym serce z funkcją defibrylacji (CRT-D). Raport w sprawie zasadności

zakwalifikowania świadczenia opieki zdrowotnej. [Internet]. Agencja Oceny Technologii Medycznych i Taryfikacji; 2018 paź. Report No.: WS.430.11.2018. Dostępne na: https://bipold.aotm.gov.pl/assets/files/zlecenia_mz/2018/173/RPT/2018.10.25_WS.430.11_RAPORT_Telemetryczny_nadzor_errata.pdf.

22. Commissioner O of the. FDA In Brief: FDA warns patients, providers about cybersecurity concerns with certain Medtronic implantable cardiac devices. FDA [Internet]. 20 grudzień 2019 [cytowane 24 marzec 2023]; Dostępne na: https://www.fda.gov/news-events/fda-brief/fda-brief-fda-warns-patients-providers-about-cybersecurity-concerns-certain-medtronic-implantable.
23. Kapoor A, Vora A, Yadav R. Cardiac devices and cyber attacks: How far are they real? How to overcome? Indian Heart Journal. listopad 2019;71(6):427–30.
24. Hassidim A, Korach T, Shreberk-Hassidim R, Thomaidou E, Uzefovsky F, Ayal S, i in. Prevalence of Sharing Access Credentials in Electronic Medical Records. Healthc Inform Res. 2017;23(3):176.
25. Akademia Pacjenta. Zdalne monitorowanie pacjentów z urządzeniami wszczepialnymi na przykładzie Śląskiego Centrum Chorób Serca w Zabrzu [Internet]. [cytowane 12 kwiecień 2023]. Dostępne na: https://akademiapacjenta.pl/2023/03/13/zdalne-monitorowanie-pacjentow-z-urzadzeniami-wszczepialnymi-na-przykladzie-slaskiego-centrum-chorob-serca-w-zabrzu/.
26. Cybersecurity Awareness for Connected Medical Devices [Internet]. Dostępne na: https://www.youtube.com/watch?v=TU1w6fQ-yf8.
27. Commissioner O of the. Medical Device Cybersecurity: What You Need to Know. FDA [Internet]. 2 kwiecień 2022 [cytowane 24 marzec 2023]; Dostępne na: https://www.fda.gov/consumers/consumer-updates/medical-device-cybersecurity-what-you-need-know.
28. Cloudflare. What is penetration testing? [Internet]. [cytowane 12 kwiecień 2023]. Dostępne na: https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/.
29. Alexander B, Haseeb S, Baranchuk A. Are implanted electronic devices hackable? Trends in Cardiovascular Medicine. listopad 2019;29(8):476-80.