Cyberbezpieczeństwo aparatury medycznej jako wspólne zadanie inżynierów klinicznych i specjalistów IT

Ewa Zalewska

Instytut Biocybernetyki i Inżynierii Biomedycznej im. M. Nałęcza, Polska Akademia Nauk, ul. Księcia Trojdena 4, 02-109 Warszawa,
e-mail: ewa.zalewska@ibib.waw.pl

W ślad za publikacją *Informatyzacja i cyfryzacja w ochronie zdrowia musi być prowadzona z udziałem inżynierów klinicznych* [9], wskazującą na znaczenie, jakie ma współdziałanie specjalistów IT i inżynierów klinicznych dla funkcjonalności i bezpieczeństwa działania sieci informatycznych w ochronie zdrowia, niniejsza publikacja sygnalizuje istotę i specyfikę problemu, jakim jest cyberbezpieczeństwo w odniesieniu do sieci medycznych.

Aparatura medyczna stała się skomputeryzowana zarówno w zakresie swoistych funkcji diagnostycznych czy terapeutycznych, jak i wyposażona w rozwiązania informatyczne łączące urządzenia medyczne z lokalną siecią informatyczną (LAN) lub Internetem, umożliwiające komunikację, transmisję i archiwizację danych medycznych, ale także zdalny nadzór i serwis.

Informatyzacja i cyfryzacja ochrony zdrowia ma na celu usprawnienie administracji, archiwizacji i organizacji pracy, ale także podniesienie jakości usług medycznych i efektów leczenia [2]. W sieciach z aparaturą medyczną stosowana jest technologia IoT (Internet of Things), która w zastosowaniu do aparatury medycznej nazywana jest IoMT (Internet of Medical Things) [5]. IoMT to rozległa sieć urządzeń medycznych, czujników, oprogramowania i systemów technologicznych, które współpracują ze sobą w celu zintegrowanej opieki nad pacjentem. Pomostem łączącym cyfryzację w obszarze administracji z technologią IoMT w medycynie jest wprowadzenie elektronicznej dokumentacji medycznej (EHR – Electronic Health Record, EDM – Elektroniczna Dokumentacja Medyczna) integrującej informacje medyczne pacjenta [1].

Systemy informatyczne w ochronie zdrowia, które obejmują również aparaturę medyczną, wymagają specjalistycznej wiedzy z dziedziny inżynierii klinicznej zarówno na etapie projektowania, jak i eksploatacji. WHO wydało rekomendacje zatrudniania w procesie informatyzacji w ochronie zdrowia specjalistów w dziedzinie inżynierii klinicznej [6, 7]. Inżynierowie kliniczni są odpowiedzialni za wdrażanie technologii medycznej, podczas gdy specjaliści IT zarządzają infrastrukturą wspierającą tę technologię. Włączanie do EHR danych i zapisów wyników badań bezpośrednio z aparatów medycznych jest obszarem działania zastrzeżonym dla kompetencji inżynierów klinicznych, którzy mają unikatową wiedzę o metodach pomiarowych, formatach danych i ich archiwizacji, interfejsach i oprogramowaniu aparatury medycznej, w zakresie których nie ma dotychczas standaryzacji.

Zapewnienie bezpieczeństwa danych i aparatury medycznej w sieciach informatycznych wymaga współdziałania specjalistów IT i inżynierów klinicznych. Dokument IEC 80001-1:2010 [3] określa role, obowiązki i działania niezbędne do zarządzania

ryzykiem sieci informatycznych, do których dołączona jest aparatura medyczna w odniesieniu do bezpieczeństwa systemu i danych oraz efektywności funkcjonowania [4].

Aparaty medyczne, które są elementami IoMT, najczęściej komunikują się przez sieć na podstawie protokołu IP, który jest protokołem ogólnego zastosowania, co może powodować problemy związane z kompatybilnością oprogramowania, interfejsów, monitorowaniem bezprzewodowym i coraz większą ilością danych przekazywanych z aparatury medycznej bezpośrednio do EHR.

Na przykład komunikowanie się systemów placówek medycznych: przychodni i szpitali z systemami, z których korzystają lekarze pierwszego kontaktu przez Internet, może powodować narażenie na zagrożenia cybernetyczne, ponieważ przesyłanie danych ogólnodostępną siecią wprowadza dodatkowe wektory ataku. Niezaszyfrowane lub zaszyfrowane przestarzałymi algorytmami dane przesyłane przez Internet mogą zostać skopiowane lub zmienione, a źle skonfigurowane lub nieuaktualniane systemy mogą stać się celem zautomatyzowanych ataków. Takim spektakularnym atakiem był atak ransomware o nazwie WannaCry w 2017 roku, który zainfekował i zaszyfrował dane w ponad 70 tysiącach urządzeń medycznych należących do National Health Service w Anglii i Szkocji [11, 12]. Raporty National Audit Office i parlamentu wykazały, że większość (ponad 90%) zainfekowanych komputerów działało pod kontrolą Windows 7, ale bez uaktualnień. Od tego czasu podobne ataki stają się coraz częstsze, według raportu firmy Comparitech, zajmującej się cyberbezpieczeństwem, w 2020 roku miały miejsce 92 ataki ransomware, które dotknęły łącznie ponad 600 różnych szpitali, klinik i organizacji oraz dotyczyły ponad 18 milionów rekordów pacjentów. Szkody oszacowano na prawie 21 miliardów dolarów [13]. Pomimo tego niewielki procent firm i instytucji medycznych podjęło jakiekolwiek kroki, by zminimalizować zagrożenie. Według badania przeprowadzonego przez Irdeto, holenderską firmę zajmującą się cyfrowym bezpieczeństwem, tylko 13% liderów IoMT ocenia, że ich firmy są przygotowane do łagodzenia przyszłych zagrożeń, 70% uważa, że są tylko częściowo przygotowane, a 17%, że są zupełnie nieprzygotowane [14]. Przyczyną takiego stanu rzeczy jest niewystarczający zakres wiedzy i słabe zrozumienie zagadnień cyberbezpieczeństwa przez kadrę zarządzającą placówkami medycznymi, personel medyczny, techników obsługujących aparaturę medyczną, a także inżynierów bez wymaganego przygotowania specjalistycznego w dziedzinie inżynierii klinicznej, oraz słabe zrozumienie specyfiki danych medycznych i różnic między danymi przesyłanymi przez typowe urządzenia sieciowe a danymi z urządzeń medycznych.

Dołączenie do sieci IT aparatury medycznej stawia nowe wyzwania w zakresie bezpieczeństwa danych, ale także spełnienia wymagań bezpieczeństwa aparatury medycznej. Oprócz bezpieczeństwa informatycznego dotyczącego oprogramowania i danych, kluczowym jest bezpieczeństwo aparatury medycznej, a w konsekwencji bezpieczeństwo pacjenta i personelu medycznego. Inżynierowie kliniczni mają kompetencje oceny, jaki wpływ na bezpieczeństwo pacjenta i personelu medycznego może mieć dołączenie aparatu do sieci i urządzeń IT. Dotyczy to bezpieczeństwa elektrycznego i transmisji danych, ale także możliwych zakłóceń pomiaru i wpływu na funkcjonowanie aparatury. Wymaga to przeprowadzenia analizy ryzyka i podejmowania decyzji z uwzględnieniem wymagań procedur medycznych i bezpieczeństwa.

Specyfika zagadnień cyberbezpieczeństwa sieci informatycznych w ochronie zdrowia to dwie kluczowe funkcje: ochrona dokumentacji pacjentów i danych medycznych oraz zapewnienie prawidłowego funkcjonowania aparatury medycznej. Nieskuteczne zabezpieczenie naraża pacjentów na dostęp do ich danych osobowych i medycznych, ale też na znacznie poważniejsze zagrożenie, jakim może być przejęcie przez osoby nieuprawnione (hakerów) kontroli nad urządzeniami medycznymi. O ile pierwszy problem może być rozwiązany z zastosowaniem standardowych procedur i leży w zakresie kompetencji specjalistów IT, to zabezpieczenie aparatury medycznej w sieci wymaga kompetencji inżynierów klinicznych w zakresie opracowywania strategii zarządzania ryzykiem dla urządzeń, oprogramowania i sieci.

Istotnym zadaniem inżynierów klinicznych w zakresie cyberbezpieczeństwa jest prowadzenie konsekwentnych działań w celu wymiany aparatury medycznej z oprogramowaniem, które nie spełnia wymaganych standardów inżynierii klinicznej, w tym standardów bezpieczeństwa, np. nieprofesjonalne oprogramowanie, niestandardowy interfejs lub brak możliwości aktualizacji. Problem nie może być rozwiązywany jednostkowo, tylko systemowo wg opracowanej strategii. Każdy aparat medyczny ma swój własny cykl życia od zdefiniowania potrzeb, planowania zakupu, poprzez eksploatację aż do utylizacji. Do wyłącznych kompetencji inżynierów klinicznych należy nadzór nad wszystkimi etapami cyklu życia aparatury, w tym ewentualne podjęcie decyzji o wcześniejszej wymianie ze względu na zapewnienie cyberbezpieczeństwa.

Inżynierowie kliniczni mogą wzmocnić cyberbezpieczeństwo poprzez stopniowe wycofywanie starszych systemów i usprawnianie technologii sieciowej. Zastąpienie starszego systemu nowym sprzętem medycznym wymaga kompetencji umożliwiających dobre zrozumienie funkcjonalności aktualnie wykorzystywanego aparatu i przygotowanie kompatybilnych rozwiązań, a następnie we współpracy z działem IT opracowanie niezbędnej infrastruktury do kompleksowego i bezpiecznego wsparcia sieciowego, planu wdrożenia, a w efekcie strategicznego harmonogramu zastępowania starszych systemów nową technologią.

Problem cyberbezpieczeństwa staje się coraz trudniejszy i wymaga wdrażania nowych rozwiązań w związku z rozwojem obszaru usług medycznych świadczonych poza placówkami medycznymi w systemie telemedycyny, w którym dopuszczone jest również korzystanie z pomiarów przy użyciu urządzeń niebędących wyrobami medycznymi, ale będących w powszechnym użyciu takich jak np. aplikacje na telefony czy zegarki umożliwiające

pomiary parametrów życiowych, z których niektóre uzyskują już certyfikację, np. oprogramowanie do analizy EKG [15]. Z pewnością będzie rozwijał się obszar mHealth (mobile health), co będzie wymagało nowych rozwiązań w systemach informatycznych, EHR, związanych nie tylko z rejestracją wyników, ale również zdalnym nadzorem korzystania z tych urządzeń [8]. Ocena możliwości wykorzystania tych danych, również pod względem cyberbezpieczeństwa, wymaga kompetencji inżynierów klinicznych. W raporcie WHO z 2017 roku [10] pozytywnie oceniono działalność inżynierów klinicznych w zakresie włączenia tych nowych metod i urządzeń do informatycznych systemów medycznych.

Specyfika wymagań cyberbezpieczeństwa w systemach ochrony zdrowia wymaga oddzielnej ścieżki rozwoju prowadzonej przez zespoły specjalistów IT i inżynierów klinicznych, którzy ponoszą wspólną odpowiedzialność za tworzenie i utrzymywanie sieci informatycznych wspomagających stosowanie środków technicznych i technologii medycznych w ochronie zdrowia.

Piśmiennictwo

1. Global Observatory for eHealth – WHO, 2016. Third Global Survey on eHealth – 2015. March, Retrieved from: http://www.who.int/goe/survey/2015survey/en/.
2. D.U. Himmelstein, A.Wright, S. Woolhandler: *Hospital computing and the costs and quality of care: a national study*, Am J Med., 123, 2010, 40e6.
3. IEC 80001-1:2010: Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities.
4. A. Subhan: *ISO/IEC 80001 (Risk Management of Medical Devices on a Network)*, Journal of Clinical Engineering, 41(3), 2016, 117-118. DOI: 10.1097/JCE.0000000000000165.
5. https://econsultancy.com/internet-of-things-healthcare/
6. WHO, 2005. "eHealth", Ninth plenary meeting, The Fifty-eighth World Health Assembly, Committee A, seventh report WHA58.28. Retrieved from: www.who.int/healthacademy/media/WHA58-28-en.pdf?ua=1.
7. WHO, 2007. "Health technologies", Eleventh plenary meeting, The Sixtieth World Health Assembly, Agenda item 12.19 WHA60.29. Retrieved from: http://www.who.int/medical_devices/resolution_wha60_29-en1.pdf.
8. WHO, 2011. mHealth: New Horizons for Health through Mobile Technologies: Second Global Survey on eHealth. WHOI, Geneva.
9. E. Zalewska: *Informatyzacja i cyfryzacja w ochronie zdrowia musi być prowadzona z udziałem inżynierów klinicznych*, Inżynier i Fizyk Medyczny, 10(1), 2021, 51-53.
10. https://www.who.int/medical_devices/global_forum/2nd-gfmd_report.pdf
11. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf
12. https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/787/787.pdf
13. https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/#How_much_did_these_ransomware_attacks_cost_healthcare_organizations_in_2020
14. https://go.irdeto.com/report-the-business-value-of-cybersecurity-in-medtech/
15. https://www.accessdata.fda.gov/cdrh_docs/reviews/DEN180044.pdf