Grudzień 2016

INSTYTUT KOŚCIUSZKI

BRIEF PROGRAMOWY INSTYTUTU KOŚCIUSZKI

Aaron Ostrovsky

Cyfryzacja sektora opieki medycznej – nowy front cyberbezpieczeństwa

autor

Aaron Ostrovsky – jest specjalistą ds. analiz systemów w jednym z nowojorskich szpitali. Aaron skończył studia licencjackie na kierunku Rusycystyka w Bates College i zdobył tytuł magistra historii Europy Środkowo-Wschodniej na Central European University. Ostrovsky posiada także tytuł magistra nauki o zdrowiu publicznym z George Washington University i certyfikat w zakresie technologii informacyjnych wykorzystywanych w opiece zdrowotnej. Aaron jest doktorantem na Rutgers University. W swoich badaniach skupia się na informatyce biomedycznej.

Wyzwania związane z cyberbezpieczeństwem zmieniły cyfrowy krajobraz, zmuszając wiele gałęzi przemysłu do oszacowania swoich możliwości w zakresie ochrony wrażliwych danych, ewaluacji nowych form technologii, a także implementowania środków bezpieczeństwa, które zapewnią bezpieczniejsze środowisko IT. Przemysł medyczny, zwłaszcza w Stanach Zjednoczonych, przeszedł ogromną zmianę. W ciągu ostatnich 10 lat zarówno gabinety lekarskie jak i szpitale wprowadziły Elektroniczną Dokumentację Medyczną (ang. *electronic health records* – EHR).

Dokument *Health Information Technology for Economic and Clinical Health* (HITECH) Act został uchwalony 17 lutego 2009 roku jako część amerykańskiej ustawy o odbudowie i reinwestycjach (ang. *American Recovery and Reinvestment Act – ARRA*). Jego główny cel to promowanie adaptowania technologii informacyjnych w sektorze opieki zdrowotnej. Dokument ma za zadanie ulepszenie świadczenia opieki medycznej w ogólnym rozumieniu oraz opieki nad pacjentami poprzez zaoferowanie zachęt finansowych dla dostawców usług zdrowotnych, którzy wykazują konstruktywne i znaczące metody (org. *meaningful use*) wykorzystywania EHR. Uprawomocniony przez HITECH urząd Narodowego Koordynatora ds. Technologii Informacyjnych w Sektorze Opieki Zdrowotnej (ang. *Office of the National Coordinator for Health Information Technology* – ONC) jest organem odpowiedzialnym za wdrożenie użycia rozwiązań IT do amerykańskiego systemu opieki zdrowotnej. Celem jest stymulacja wykorzystywania IT jako rozwiązań pozwalających na lepsze zarządzanie opieką nad pacjentami, redukcję błędów medycznych i usprawnienie przepływu informacji medycznej, a co za tym idzie, użytkowanie technologii w sposób konstruktywny i znaczący.

HITECH używając tego określenia wskazuje „wykorzystywanie certyfikowanej technologii EHR w konstruktywny i znaczący sposób; zapewnienie implementacji certyfikowanej technologii EHR tak, aby prowadziła ona do poprawy jakości opieki zdrowotnej; a także to, że użytkownik certyfikowanej

ISSN 1689-9873

technologii EHR musi dostarczyć do Ministra Zdrowia i Opieki Społecznej (ang. *Secretary of Health & Human Services* – HHS) informacji na temat jakości opieki i innych środków"[1]. Priorytetami konstruktywnego i znaczącego użycia i rezultatami polityki zdrowotnej są[2]:

- Poprawa jakości, wydajności, bezpieczeństwa i zmniejszanie różnic zdrowotnych;
- Poprawa kondycji zdrowotnej spoleczenstwa;
- Zapewnienie ochrony prywatności i bezpieczeństwa dla personalnych danych zdrowotnych;
- Poprawa koordynacji opieki zdrowotnej.

W celu ich osiągnięcia, konstruktywne i znaczące użycie zostało podzielone na kilka faz. Trzy główne etapy dotyczą: danych, zaawansowanych procesów klinicznych i udoskonalonych, spodziewanych rezultatów. Żeby zakwalifikować się do uzyskania zachęt finansowych, następujące kryteria konstruktywnego i znaczącego użytkowania muszą być spełnione:

1. Wykorzystywanie certyfikowanych EHR w konstruktywny i znaczący sposób, np. poprzez przepisywanie elektronicznych recept;

2. Wykorzystywanie certyfikowanych EHR przy elektronicznej wymianie informacji zdrowotnych, aby poprawić jakość opieki zdrowotnej;

3. Wykorzystywanie certyfikowanych technologii EHR do przesyłania wyników pomiarów jakości usług klinicznych.

Jako podstawowy akt prawodawczy, HITECH skierowany jest do federalnych programów i polityk IT w sektorze zdrowotnym. Dane Kongresowego Biura Budżetowego (ang. *The Congressional Budget Office* – CBO) pozwalają oszacować, że dzięki temu dokumentowi ok. 37.2 miliardów dolarów zostanie wydane na programy medyczne (Medicare i Medicaid) w latach 2009-2019[3]. W ramach HITECH przeznaczono 2 miliardy dolarów na sfinansowanie medycznej infrastruktury IT, centrów zasobów, programów zatrudnienia, programów prywatności i bezpieczeństwa oraz programów badawczych. Dodatkowo HITECH zapewnia granty dla poszczególnych stanów oferujących niskooprocentowane kredyty, które mają pomóc dostawcom w finansowaniu ich inicjatyw w zakresie medycznego IT. Około 1.985 miliarda dolarów ze wspominanych 2 miliardów zostało rozdystrybuowane od 1-ego marca 2013 r.[4] Premie Medicare dla tych dostawców lub szpitali, które zaadaptowały i korzystają z EHR, są fundowane dzięki HITECH. W planach jest zastąpienie finansowych zachęt karami dla tych podmiotów, które nie spełniają standardów konstruktywnego użytkowania. Ustawa określa dostawców Medicaid, którzy otrzymują od rządu pełne wsparcie finansowe na adaptacje certyfikowanego systemu EHR. Na ten moment, 12.7 miliarda dolarów zostało zapewnione ok. 388 593 szpitalom i dostawcom.[5]

Niestety, zwiększenie ilości zdigitalizowanych danych medycznych sprawiło, że sektor opieki zdrowotnej stał się celem cyberataków.

Niestety, zwiększenie ilości zdigitalizowaych danych medycznych sprawiło, że sektor opieki zdrowotnej stał się celem cyberataków. Grupa Robocza ds. Wymiany Danych Elektronicznych (ang. *Workgroup for Electronic Data Interchange* – WEDI) szacuje, że w latach 2010 – 2014 ok. 37 milionów danych zdrowotnych stało się celem cyberataków.[6] Poza wzrostem użycia EHR, inne technologie, jak np. urządzenia medyczne, stały się cennym źródłem danych o pacjentach.

Według Fortinet, firmy zajmującej się cyberbezpieczeństwem, w ciągu czterech pierwszych miesięcy 2015 roku zaobserwowano 93 ataki, które miały wpływ na ok. 99 milionów danych medycznych.[7] Niestety, ewolucja technologii w sektorze opieki zdrowotnej sprawiła, że sektor ten stał się cennym celem na cyberataków.

1 Meaningful Use (Internet) 2016,– Available from: http://www.cdc.gov/EHRmeaningfuluse/introduction.html

2 Ibid.

3 Senators Thune, Alexander, Roberts, Burr, Coburn, Enzi. Reboot: Re-Examining the Strategies Needed to Successfully Adopt Health IT. United States Senate, April 16th, 2013

4 Ibid.

5 Ibid.

6 WEDI, "WEDI Releases Perspectives on Cybersecurity in Healthcare Primer" (Internet) September 6th, 2016. Available from – http://www.wedi.org/news/press-releases/2015/06/22/wedi-releases-perspectives-on-cybersecurity-in-healthcare-primer

7 Ibid.

Cyberataki

Raport Ponemon Institute z 2016 roku przedstawia dane, według których ilość cyberataków w ciągu ostatnich pięciu lat niemal się podwoiła. Ponemon Institute szacuje, że złamanie ochrony baz danych kosztuje szpital ok. 2.1 miliona dolarów; natomiast na poziomie narodowym cyberataki, których celem były szpitale lub lekarze w Stanach, kosztują ok. 6 miliardów dolarów rocznie.[8] Amerykański system opieki zdrowotnej stał się kopalnią wrażliwych danych, które mogą zostać wykorzystane dla znacznych korzyści finansowych.

W 2013 roku wykonawczy wydawca *Healthcare Information and Management Systems Society* (HIMSS), Tom Sullivan, skomentował przejście od papierowej bazy danych do bazy elektronicznej: „jest trudniej ukraść miliony dokumentów papierowych niż elektronicznych. Ponieważ wzrastająca ilość EHR sprawia, że system opieki zdrowotnej staje się coraz bardziej zdigitalizowany, a wymiana informacji medycznych (ang. *health information exchanges* – HIE) i ubezpieczeń zdrowotnych jest normą, elektroniczne dane medyczne są często rozpowszechniane. Ich rosnąca liczba przechowywana jest w chmurze i innych centralnych repozytoriach, z których udostępnia się je licznym urządzeniom mobilnym; choć to już się zmienia. Dodatkowo, w sposób błyskawiczny następuje proliferacja urządzeń mobilnych, łatwych do zgubienia, często niekodowanych."[9]

Według raportu Breach Level Index z 2015 roku opublikowanego przez Gemalto, firmę zajmująca się bezpieczeństwem cyfrowym, sektor opieki zdrowotnej w USA doświadczył w pierwszej połowie 2015 roku 187 ataki na bazy danych, co jednocześnie stanowiło ok. 21.1% wszystkich ataków w 2015 roku. Według raportu, amerykański rząd i sektor opieki zdrowotnej ucierpiały najbardziej, a wspólnie stanowiły ok. 2/3 wszystkich ofiar wycieków danych.[10] Verizon Data Breach Raport (DBIR) z 2016 roku szacuje, że sektor opieki medycznej padł ofiarą ok. 166 incydentów narażających bezpieczeństwo w 2015 roku, a 115 z tych incydentów to potwierdzone przypadki utraty danych.[11] Mimo, że wspomniane raporty pozwalają na nakreślenie pewnego obrazu skali wycieku danych medycznych, wysoce prawdopodobnym jest, że ilość incydentów jest w rzeczywistości większa. Wynika to z braku wykrywalności niektórych ataków, a także niezgłaszania ich wystąpienia.

Od czerwca 2016 roku prawie 632 dostawców usług IT w sektorze zdrowia zaopatrzyło 337 432 lekarzy pierwszego kontaktu, pediatrów, specjalistów chirurgicznych[12] i medycznych, a także dentystów, w certyfikowane oprogramowania EHR w celu poprawienia opieki nad pacjentami. Sponsorowane przez rząd przejście na system elektroniczny w znaczący sposób przyczyniło się do poprawy opieki nad pacjentem, redukcji błędów i usprawnienia pracy. Jednakże, zmiana ta stworzyła też technologiczną zależność, która naraża wrażliwe dane na zagrożenia.

Według raportu Pricewaterhouse Coopers (PwC) z 2015 roku, do roku 2020 wartość produktów z dostępem do Internetu wzrośnie do ok. 285 miliardów dolarów.[13] Taka ekonomiczna perspektywa potencjalnie wpłynie na wzrost ryzyka ataków. W 2014 roku ok. 85% dużych organizacji związanych z opieką zdrowotną w rożnym stopniu doświadczyło poważnego naruszenia danych; ok. 18% tych naruszeń kosztowało ponad milion dolarów.[14] Emerytowany pułkownik armii amerykańskiej, Jeff Schilling, aktualnie CSO w Armor Inc., uważa, że ochrona danych medycznych „opiera się na architekturze sieci". Ponadto, Schilling stwierdził: „urządzenia medyczne powinny być odseparowane od pozostałych urządzeń w szpitalnych sieciach. W ich przypadku bowiem, jako jednym z nielicznych, dokonujący cyberataku może realnie

8 Pettypiece, Shannon "Rising Cyber Attacks Costing Health System $6 Billion Annually," *Bloomberg Technology*, May 7th, 2015. Available from – http://www.bloomberg.com/news/articles/2015-05-07/rising-cyber-attacks-costing-health-system-6-billion -annually

9 Sullivan, Tom. "Are providers ripe for massive medical records heist? *Government Health IT*, January 14th, 2013. Available from – http://www.healthcareitnews.com/news/are-providers-ripe-massive-medical-records-heist

10 Gemalto, "Findings from the Breach Level Index" (Internet) September 3rd, 2016. Available from – http://www.gemalto.com/press/Pages/Gemalto-Releases-Findings-of-First-Half-2015-Breach-Level-Index.aspx

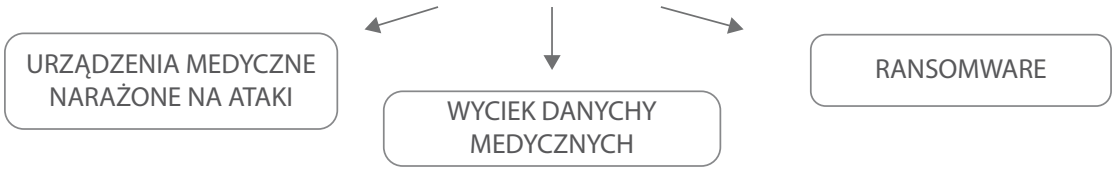
11 Verizon, "2016 Data Breach Investigations Report" September 17th, 2016. Available from – http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

12 The Office of the National Coordinator for Health Information Technology, Health IT Dashboard, 2016 September 3rd. Available from – http://dashboard.healthit.gov/quickstats/quickstats.php

13 PwC Cybersecurity Report (Internet) September 3rd, 2016. Available from – http://www.pwc.com/us/en/health-industries/top-health-industry-issues/cybersecurity.html

14 Ibid.

GŁÓWNE CYBERZAGROŻENIA W SEKTORZE OPIEKI ZDROWOTNEJ



kogoś skrzywdzić".[15] Dopiero w 2015 roku rząd wydał pierwsze oświadczenie ostrzegające przed zagrożeniami dotyczącymi urządzeń medycznych. 13 maja 2015 roku Agencja Żywności i Leków (ang. *U.S. Food and Drug Administration* – FDA) opublikowała komunikat na temat zagrożenia systemu pomp infuzyjnych Hospira LifeCare PCA3 and PCA5.[16] Billy Rios, badacz bezpieczeństwa, zidentyfikował zagrożenia w tych modelach pomp, które mogłyby stać się celem ataków poprzez zdalną infiltrację sieci szpitalnych. Podobne naruszenia bezpieczeństwa, wśród których znalazł się także nieautoryzowany zdalny dostęp, były powiązane z niewłaściwym użyciem takich protokołów jak: *hypertext transfer protocol* (HTTP), *anonymous file transfer protocol* (FTP), *exposed remote desktop protocol* (RDP), SSH, telnet, itd. Dodatkowo, błędy w kodach systemowych, aplikacjach i urządzeniach medycznych używanych przez instytucje opieki zdrowotnej mogą doprowadzić do złamania baz danych i innych zagrożeń spowodowanych przez takie eksploatacje systemów bezpieczeństwa jak: *buffer overflow, cross-site scripting* (XSS), *SQL injection*, i *cross-site request forgery* (CSRF).

Ataki na urządzenia medyczne nie są jedynym zagrożeniem, jakie stoi przed instytucjami opieki zdrowotnej. Ransomware, forma złośliwego oprogramowania zaprojektowana, aby ograniczyć dostęp użytkowników do ich systemów lub plików, uderzyła w sektor opieki zdrowotnej wyjątkowo mocno na przestrzeni kilku ostatnich lat. Ten typ malware'u zazwyczaj wysyłany jest za pomocą tzw. *phishingu*, którego intencją jest oszukanie niespodziewającego się ataku użytkownika i skłonienie go do otworzenia złośliwych załączników.17 Atakujący żąda zapłaty okupu za odblokowanie dostępu do danych i plików. Ransomware zaczął być tak poważnym zagrożeniem, że w marcu 2016 roku Departament Bezpieczeństwa Krajowego Stanów Zjednoczonych (ang. *U.S. Department of Homeland Security* – DHS) wystosował ostrzeżenie na temat proliferacji dwóch jego specyficznych wariantów – Locky i Samas – które za główny cel ataków obrały szpitale i instytucje opieki zdrowotnej.[18]

W maju 2016 roku szpital Kansas Heart padł ofiarą ataku Ransomware. Szpital zapłacił okup, jednak odmówił wpłacenia kolejnej kwoty. Był to drugi szpital, który publicznie przyznał się do zapłaty okupu. W lutym tego samego roku szpital Hollywood Presbyterian zapłacił hakerom 17 tysięcy dolarów.[19] Wiceprezes firmy Fortinet, Ryan Witt, stwierdził: „żądania okupów rosną, a problemem jest to, że organizacje je płacą. Ransomware stanie się jeszcze groźniejszy zanim ta tendencja zacznie się zmieniać… Naprawdę nie chcecie sobie wyobrażać zwrotu z inwestycji w zakresie tego rodzaju kryminalnej aktywności. Są to ogromne kwoty, a atakujący to wyrafinowani gracze, którzy wiedzą, na czym i gdzie można zarobić."[20]

15 Ibid.

16 U.S. Food & Drug, Medical Devices & Cyber Security (Internet) September 3rd, 2016. Available from – http://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm

17 United States Computer Emergency Readiness Team, Alert (TA16-091A) Ransomware and Recent Variants (Internet) September 3rd, 2016. Available from – https://www.us-cert.gov/ncas/alerts/TA16-091A

18 Gendre, Andrien. "Hospitals and Ransomware: Phishing and Healthcare," *VadeSecure*, April 21st, 2016. Available from – http://blog.vadesecure.com/en/hospitals-ransomware-phishing-healthcare/

19 Siwicki, Bill. "Ransomware attackers collect randsom from Kansas hospital, don't unlock all the data, then demand more money," *HealthcareIT News*, May 23rd 2016. Available from – http://www.healthcareitnews.com/news/kansas-hospital-hit-ransomware-pays-then-attackers-demand-second-ransom

20 Ibid

Ciągle zagrożenie cyberatakami wymaga, aby sektor opieki zdrowotnej stworzył nowe prewencyjne mechanizmy i standardy bezpieczeństwa, które będą chronić dane medyczne.

Cyberataki nie ograniczają się do szpitali i dostawców usług medycznych. Firmy ubezpieczeniowe także padły ofiarą tego typu ataków. 4 kwietnia 2014 Anthem Inc. publicznie przyznało, że dane dotyczące niemal 78.8 miliona obecnych i byłych członków i pracowników zostały zaatakowane. Ken Dort, specjalista ds. cyberbezpieczeństwa Drinker Biddle & Reath, uważa, że „ubezpieczyciele mają prawdopodobnie tak dużo przestarzałych systemów, że nie są w stanie ich zsynchronizować tak, jak powinni."[21] Długoterminowe skutki tych ataków jeszcze nie zostały w pełni rozpoznane. W podobnej sytuacji znalazła się 29 stycznia 2015 roku firma ubezpieczeniowa Premera Blue Cross z Pacific Northwest, która ujawniła, że prawie 11 milionów profili padło ofiarą cyberataków w konsekwencji nieautoryzowanego dostępu do ich systemów IT. W ramach uspokojenia klientów, Premera zobowiązała się do darmowego dwuletniego monitoringu kredytów i ubezpieczenia przed kradzieżą tożsamości dla tych klientów, którzy zostali dotknięci atakiem.[22] Pomimo tego, od czasu incydentu, Premera mierzy się z pozwami swoich klientów zgłaszających próby oszustwa.[23]

Mechanizmy obronne

Health Insurance Portability and Accountability Act (HIPAA), ustawa uchwalona w 1996 roku, służy obecnie jako narodowa regulacja standardów, jakie powinny zostać spełnione, aby chronić bezpieczeństwo i prywatność danych medycznych. Na podstawie drugiej części dokumentu, która skupia się na procedurach i standardach zapewniających bezpieczeństwo i prywatność określonych informacji medycznych, Departament Zdrowia i Opieki Społecznej Stanów Zjednoczonych (ang. *U.S. Department of Health and Human Services* – HHS), opublikował *HIPAA Privacy Rule* (Zasada Prywatności) i *HIPAA Security Rule* (Zasada Bezpieczeństwa). Mimo że nie jest to zdefiniowany model standardów bezpieczeństwa, wymagania HIPAA można zinterpretować w następujący sposób:[24]

- Szyfrowanie przesyłu danych – elektronicznie chronione dane medyczne (ang. *electronic protected health information* – ePHI) muszą być bezpiecznie przesyłane w bezpieczny zaszyfrowany sposób poprzez wykorzystanie SSL/TLS;
- Szyfrowane przechowywanie danych – regulacje HIPAA narzucają obowiązek szyfrowania danych archiwalnych (ang. *at rest*). Nie precyzują jednak, w jaki sposób instytucje mają definiować wewnętrzne procesy szyfrowania przechowywanych danych;
- Integralność – integralność danych jest zapewniona poprzez dbanie o ich spójność i precyzję. Dane nie mogą być zmienione przypadkowo bądź za pomocą złośliwego oprogramowania;
- Usuwanie – Jeśli zaistnieje taka potrzeba, dane podmiotów mogą być trwale usunięte. Dotyczy to także danych, które zostały zakwalifikowane do archiwizacji;
- Autoryzacja – dostęp do wrażliwych danych jest możliwy tylko dla autoryzowanego wcześniej personelu. Jak określa HIPAA, dostawcy hostingu muszą zgodzić się na partnerską umowę biznesową (ang. *Business Associate Agreement* – BAA);
- Backup – ePHI powinny być efektywnie zarchiwizowane, aby w przypadku sytuacji wyjątkowej ich odzyskanie było możliwe.

Tak zwana *Zasada Bezpieczeństwa* „ustanawia narodowe standardy dla ochrony elektronicznych personalnych danych medycznych, które są tworzone, odbierane, używane lub zarządzane przez objęte Porozumieniem podmioty. *Zasada Bezpieczeństwa* wymaga stosownych administracyjnych, fizycznych i technicznych zabezpieczeń, które zapewnią

21 Herman, Bob "Details of Anthem's massive cyberattack remain in the dark a year later," *Modern Healthcare*, March 30th, 2016. Available from – http://www.modernhealthcare.com/article/20160330/NEWS/160339997

22 Premera "Premera Blue Cross Announces Cyberattack, Offers Protection for Affected Individuals" (Internet) September 3rd, 2016. Available from – https://www.premera.com/wa/visitor/about-premera/press-releases/2015_03_17/

23 Garnick, Coral, "Premera negligent in data breach, 5 lawsuits claim," *The Seattle Times*, March 27th, 2015. Available from – http://www.seattletimes.com/seattle-news/premera-negligent-in-data-breach-5-lawsuits-claim/

24 Hosting Edge, "A proactive approach to cybersecurity in healthcare: Going beyond HIPAA compliance (Internet) September 5th, 2016 – Available from – https://www.edgehosting.com/blog/2015/11/a-proactive-approach-to-cybersecurity-in-healthcare-going-beyond-hipaa-compliance/

poufność, integralność i bezpieczeństwo elektronicznych chronionych informacji medycznych."[25]

Ta zasada wraz z *Zasadą Prywatności* regulują wykorzystywane ePHI, a także sposób, w jaki organizacje – „objęte Porozumieniem podmioty"* – posługują się wrażliwymi danymi. Poza ujętymi w *Zasadzie Bezpieczeństwa* administracyjnymi, technicznymi i fizycznymi wytycznymi dotyczącymi zabezpieczeń, wymagane jest przeprowadzenie analizy ryzyka, rozumianej jako jeden z procesów zarządzania bezpieczeństwem organizacji.

Zasada Bezpieczeństwa wymaga stosownych administracyjnych, fizycznych i technicznych zabezpieczeń, które zapewnią poufność, integralność i bezpieczeństwo elektronicznych chronionych informacji medycznych.

Pomimo istnienia tej linii obrony, nowsze technologie i metody infiltracji zmusiły amerykańskie agencje rządowe, takie jak Biuro Praw Obywatelskich (ang. *Office for Civil Rights* – OCR), do zmierzenia się z lukami w cyberbezpieczeństwie poprzez analizę zbieżności między Zasadą Bezpieczeństwa HIPAA oraz ramowym planem na rzecz cyberbezpieczeństwa (ang. *Cybersecurity Framework*) Narodowego Instytutu Standaryzacji i Technologii (ang. *National Institute of Standards and Technology* – NIST). NIST, nieregulacyjna agencja Departamentu Handlu Stanów Zjednoczonych (ang. U.S. *Department of Commerce*), „promuje amerykańskie innowacje i konkurencyjność w przemyśle poprzez poprawę wyników naukowych oraz standardów i technologii w taki sposób, aby zapewniły one bezpieczeństwo ekonomiczne i poprawiły jakość życia."[26] Znaczną częścią tej misji stanowi wypracowanie standardów i operowanie nimi. W lutym 2013 roku prezydent Barak Obama wystosował rozporządzenie (ang. *Executive Order 13636*), które wskazało potrzebę stworzenia ramowej polityki cyberbezpieczeństwa zawierającej „priorytetowe, elastyczne, powtarzalne, wydajne i opłacalne podejście do zarządzania ryzykiem w obszarze cyberbezpieczeństwa w kontekście procesów, informacji i systemów bezpośrednio związanych z dostarczaniem usług dla infrastruktury krytycznej"[27]. 12 lutego 2014 roku NIST, w odpowiedzi na potrzeby nakreślone w rozporządzeniu, opublikował ramowy plan na rzecz cyberbezpieczeństwa w celu wzmocnienia infrastruktury krytycznej.

Analiza porównawcza wykonana przez OCR służy jako środek prewencyjny, na podstawie którego mają być identyfikowane luki w bezpieczeństwie organizacji. Oba dokumenty, Zasada Bezpieczeństwa HIPAA i ramowy plan na rzecz cyberbezpieczeństwa NIST, zawierają wytyczne wspierające instytucje w ochronie danych medycznych. 18 grudnia 2015 roku prezydent Obama przyjął *Cybersecurity Information Sharing Act* (CISA). Ustawa ta ma na celu promowanie przepływu informacji dotyczących cyberzagrożeń pomiędzy sektorem prywatnym a rządem federalnym.[28] Zarówno HITECH jak i CISA wspierają implementację zapisów planu ramowego na rzecz cyberbezpieczeństwa NIST.

FDA wydała wytyczne dotyczące niebezpieczeństw w zakresie cyberbezpieczeństwa dla producentów urządzeń medycznych; Międzynarodowa Organizacja Normalizacyjna (ang. *International Organization for Standardization* – ISO) uchwaliła standard ISO 14971:2007 dotyczący zarządzania ryzykiem w obszarze urządzeń medycznych.[29] Instytucje opieki zdrowotnej powinny jednak pójść o krok dalej niż tego typu wytyczne i zapewnić bezpieczne środowisko funkcjonowania, stosując następujące działania[30]:

- Monitorować i kontrolować ruch w sieci, aby zabezpieczyć się przed nieautoryzowanym dostępem;
- Zainstalować oprogramowanie antywirusowe i umożliwić rutynowe kontrole konfiguracji zapór sieciowych;

25 HHS.gov, Health Information Privacy (Internet) September 5th, 2016. Available from – http://www.hhs.gov/hipaa/for-professionals/security/index.html

* Objęte Porozumieniem podmioty zdefiniowane przez HIPAA: banki informacji zdrowotnej, programy zdrowotne oraz personel medyczny, który elektronicznie przekazuje informacje medyczne (https://privacyruleandresearch.nih.gov/pr_06.asp).

26 NIST, NIST Mission, Vision, Core Competencies, and Core Values (Internet) September 5th, 2016. Available from – https://www.nist.gov/about-nist/our-organization/mission-vision-values

27 NIST, "Framework for Improving Critical Infrastructure Cybersecurity v1.0" *National Institute of Standards and Technology (NIST)*, Feb. 12th, 2014. Available from – https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

28 Norton Rose Fulbright, Data Protection Report (Internet) September 5th, 2016 – Available from – http://www.dataprotectionreport.com/2016/01/federal-cybersecurity-information-sharing-act-signed-into-law/

29 ISO, ISO 14971:2007 (Internet) September 6th, 2016. Available from – http://www.iso.org/iso/catalogue_detail?csnumber=38193

30 Deloitte Report Issue Brief, "Networked medical device cybersecurity and patient safety: Perspectives of healthcare information cybersecurity executives," *Deloitte*. Available from – http://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-lhsc-networked-medical-device.pdf

- Dzielić sieci, w ramach których przesyłane są wrażliwe dane, np. urządzenia medyczne podłączone do sieci;
- Przeprowadzać okresowe ewaluacje i testowe penetracje w celu wykrycia luk w zabezpieczeniach.

Technologie mobilne i rosnąca akceptacja dla wykorzystywania prywatnych urządzeń – *Bring Your Own Device* (BYOD) – wpłynęły na zmiany dotyczące tego, dla kogo dane są udostępniane, a także jak są użytkowane, przesyłane i przechowywane. *National Cybersecurity Center of Excellence* (NCCoE), jednostka NIST, opublikowało w 2015 roku dokument *NIST Cybersecurity Practice Guide SP 1800-1a*. Poradnik skupia się na tym, jak zabezpieczać dane elektroniczne na urządzeniach mobilnych i podpowiada, jak zachować bezpieczeństwo za pomocą różnych standardów cyber, projektów architektonicznych i technologii[31] Oprogramowanie zarządzania urządzeniami mobilnymi (ang. *Mobile Device Management* – MDM) zostało implementowane przez różne instytucje opieki medycznej, aby ulepszyć kontrolę, zarządzanie i bezpieczeństwo urządzeń mobilnych, które łączą się z siecią organizacji, by uzyskać dostęp do jej wewnętrznych zasobów i aplikacji.

Technologie mobile i rosnąca akceptacja dla wykorzystywania prywatnych urządzeń (BYOD) wpłynęły na zmiany dotyczące tego, dla kogo dane są udostępniane, a także jak są użytkowane, przesyłane i przechowywane.

Poza technologiami mobilnymi, zależności od rozwiązań podmiotów zewnętrznych i serwisów opartych na chmurze, w tym na modelu *oprogramowanie jako usługa* (ang. *Software as a Service – SaaS*), wzrosło w sposób dramatyczny w ciągu ostatnich kilku lat i może stać się źródłem nowego rodzaju ataków i włamań. Według raportu Q2 2015 opublikowanego przez Skyhigh Networks, około 928 opartych na chmurze usług jest przeciętnie użytkowanych przez organizacje opieki zdrowotnej.[32] Usługi w chmurze obejmują narzędzia współpracy, środowiska programistyczne, przekazywanie treści, *business intelligence*, itd. Raport Skyhigh sugeruje, że jedynie 7% z 928 usługodawców spełnia standardy bezpieczeństwa.[33] HIMSS oferuje pakiet narzędzi *cloud computing*, który zapewnia instytucjom opieki zdrowotnej środki – począwszy od porad w zarządzaniu ryzykiem po materiały edukacyjne – w celu ulepszenia funkcjonowania w chmurze.

Zależność od nowych technologii zmusiła działy bezpieczeństwa instytucji opieki medycznej do rewaluacji swoich ekosystemów w celu zapewnienia im odpowiedniej ochrony przed cyberatakami.

Poza federalnie narzucanymi regulacjami, instytucje opieki medycznej wciąż wychwytują luki w swoich strategiach bezpieczeństwa. Biorąc pod uwagę, że cyberzagrożenia stają się coraz częstszą rzeczywistością, organizacje podejmują coraz bardziej proaktywne działania, aby zabezpieczyć swoje dane. Wiceprzewodniczący ds. cyberbezpieczeństwa i misji specjalnych w Raytheon Intelligence, Jack Harrington, powiedział: „cyberbezpieczeństwo nie jest grą na zwłokę i organizacje, które nie posiadają odpowiednich ekspertyz i narzędzi niezbędnych do identyfikacji przeciwników i odpowiedzi na ich ataki muszą to zrozumieć… przestarzałe podejście polegało wyłącznie na technologii, która była w stanie wskazywać tylko znane zagrożenia"[34]. Ponadto, przewodniczący Raytheon Foreground Security, David Amalser, stwierdził, że „w dzisiejszych czasach zbyt wiele organizacji opiera swoją działalność na modelu reakcji i zautomatyzowanych narzędziach, które próbują wykryć zagrożenia poprzez analizę opartą na podpisie, regule lub środowisku testowym"[35].

Stosując minimalne standardy przewidziane w Zasadzie Bezpieczeństwa i Zasadzie Prywatności, organizacja w najlepszym wypadku będzie spełniać wymagania HIPAA, jednakże nie musi to oznaczać, że jej środowisko będzie bezpieczne; to w wielu przypadkach minimalny wysiłek na drodze do sprostania regulacjom federalnym.

31 NCCoE, Security Electronic Health Records on Mobile Devices Executive Summary (Internet) September 6th, 2016. Available from – https://nccoe.nist.gov/sites/default/files/library/sp1800/hit-ehr-nist-sp1800-1a-draft.pdf

32 Skyhigh Network, "Cloud Adoption & Risk in Healthcare Report" Q2 2015 published Q3 2015. Available from – http://info.skyhighnetworks.com/rs/274-AUP-214/images/WP-Cloud-Adoption-Report-Q2-2015-Healthcare.pdf

33 Ibid

34 Raytheon, "Business wait for damaging cyber attacks before taking action: study," *Raytheon* (Internet) September 5th, 2016 – Available from – http://raytheon.mediaroom.com/2016-06-06-Businesses-wait-for-damaging-cyber-attacks-before-taking-action-Study

35 Belliveau, Jacqueline "How a proactive approach improves healthcare cybersecurity," Health IT Security, June 6th, 2016. Available from – http://healthitsecurity.com/news/how-a-proactive-approach-improves-healthcare-cybersecurity

Zależność od nowych technologii zmusiła działy bezpieczeństwa instytucji opieki medycznej do re-ewaluacji swoich ekosystemów w celu zapewnienia im odpowiedniej ochrony przed cyberatakami. Zestaw narodowych i przemysłowych standardów, planów ramowych dotyczących cyberbezpieczeństwa, oprogramowania zabezpieczającego i alokacji funduszy na szkolenia w obszarze cyberbezpieczeństwa pomaga zmniejszyć zagrożenia, odstraszając atakujących.

Zestaw narodowych i przemysłowych standardów, planów ramowych dotyczących cyberbezpieczeństwa, oprogramowania zabezpieczającego i alokacji funduszy na szkolenia w obszarze cyberbezpieczeństwa pomaga zmniejszyć zagrożenia, odstraszając atakujących.

Wnioski

W tym roku Prezydent Obama stworzył Narodowy Plan Działania w obszarze Cyberbezpieczeństwa (ang. *Cybersecurity National Action Plan* – CNAP). Jego celem jest opracowanie długoterminowej strategii, która wzmocni świadomość i poprawi stan cyberbezpieczeństwa, zapewnienie i ochrona prywatności oraz autoryzacja agencji federalnych do wzmocnionej obrony ich bezpieczeństwa cyfrowego.[36] Plan Działania ma być także przypomnieniem, że cyberbezpieczeństwo i ochrona wrażliwych danych nie jest ograniczona do ochrony sektora opieki zdrowotnej, ale odnosi się do całego amerykańskiego środowiska cyfrowego. Odpowiedzialność spoczywa nie tylko na działach bezpieczeństwa, ale także na wszystkich użytkownikach systemów i urządzeń, które pozwalają na dostęp do wrażliwych danych medycznych. Obrazują to przykłady fizycznego bezpieczeństwa laptopów czy urządzeń mobilnych oraz hasła zabezpieczające i zmiana kultury bezpieczeństwa w zakładach pracy.

Zarówno rząd federalny jak i sektor prywatny zapewniły narzędzia pozwalające na lepsze funkcjonowanie i implementację zasad bezpieczeństwa, unormowały zasady bezpiecznej wymiany danych oraz ułatwiły dostęp do materiałów szkoleniowych w obszarze cyberbezpieczeństwa. Jednakże, kolejne kroki w stronę wypracowywania dojrzałych standardów i zachęcania instytucji opieki zdrowotnej do inwestowania w swoje programy bezpieczeństwa są niezbędne, aby wspierać ochronę tego sektora przed obecnymi i przyszłymi cyberatakami. Miejmy nadzieję, że istniejące narzędzia umożliwią sektorowi opieki zdrowotnej wyprzedzić zagrożenia i utrzymać poziom bezpieczeństwa i ochrony prywatności wymagany, aby amerykańskie dane medyczne były bezpieczne.

Podziękowania:

Chciałbym podziękować Michaelowi Czumakowi (CISO) za jego pomoc przy pisaniu tego artykułu.

36 General Services Administration (GSA), "Cybersecurity National Action Plan (CNAP) (Internet) September 6th, 2016. Available from – http://www.gsa.gov/portal/content/129694.

Biuro w Krakowie: ul. Feldmana 4/9, 31-130 Kraków, Polska, tel.: +48 12 632 97 24, www.ik.org.pl, e-mail: ik@ik.org.pl.

Dalsze informacje i komentarze: Joanna Świątkowska – joanna.swiatkowska@ik.org.pl – tel. +48 515 174 389.