DOI: https://doi.org/10.34862/rbm.2020.2.6

Julia Makuch
Uniwersytet Medyczny im. Piastów Śląskich we Wrocławiu
julka.makuch@gmail.com
https://orcid.org/0000-0003-4678-9564

Mateusz Guziak
Gdański Uniwersytet Medyczny
mateusz.guziak@gumed.edu.pl
https://orcid.org/0000-0002-5720-3410

Cyberbezpieczeństwo w sektorze ochrony zdrowia. Przypadek Polski na tle tendencji światowych

Abstrakt: Przedmiotem niniejszego artykułu jest próba usystematyzowania wiedzy o data breach występujących w ochronie zdrowia i fluktuacjach, jakim podlega ono w czasie. Omówione zostały standardy administrowania danymi medycznymi oraz najczęstsze przyczyny ich wycieku. Analizie poddana została literatura traktująca o cyberbezpieczeństwie sektora ochrony zdrowia. Cyberataki są obecnie bardziej wyrafinowane i lepiej finansowane, rośnie również ich liczba. Jedną z przyczyn jest wzrastającą wartość danych medycznych na czarnym rynku, natomiast w warunkach polskich jest to przede wszystkim niska świadomość zagrożeń, skutkująca lekceważącym podejściem do raportowania incydentów, niewystarczające kwalifikacje personelu medycznego w obrębie cyberhigieny oraz nieprzejrzystość polityki informacyjnej służb. W obliczu aktualnie występującej pandemii COVID-19 i coraz szybciej postępującej cyfryzacji branży medycznej, problem ten może dodatkowo narastać. Niezbędne jest nawiązanie dialogu między ekspertami od spraw cyberbezpieczeństwa a specjalistami związanymi z branżą medyczną.

Słowa kluczowe: cyberbezpieczeństwo, ochrona zdrowia, dane wrażliwe, bezpieczeństwo informacji, elektroniczna dokumentacja medyczna.

Cybersecurity in Healthcare. Polish Case Against the World Trends

Abstract: The subject of this article is an attempt to systematize the knowledge about the data breach phenomenon and its fluctuations in time. Medical data administration standards and the most common causes of their leakage were discussed. The literature on cybersecurity in the healthcare sector was analyzed. Cyberattacks are now more sophisticated and better financed, and their number is growing. One of the reasons is the increasing value of medical data on the

black market. At the same time, in Poland, the awareness of threats is primarily low, resulting in a disrespectful approach to reporting incidents, insufficient qualifications of medical personnel in the field of cyber hygiene, and the non-transparency of the information policy of the services. In the face of the current COVID-19 pandemic and the increasingly faster digitisation of the medical industry, this problem may increase further. It is necessary to establish a dialogue between cybersecurity experts and specialists related to the medical industry.

Keywords: cybersecurity, healthcare, sensitive data, information security, electronic health records.

Wstęp

Wieloaspektowa problematyka, jaką stanowi cyberbezpieczeństwo, coraz częściej poruszana jest w kontekście wielu branż, jednak wciąż wyjątkowo rzadko mówi się o nim w obrębie sektora ochrony zdrowia. Czasy papierowej dokumentacji medycznej powoli odchodzą w zapomnienie, jednocześnie ustępując miejsce elektronicznej dokumentacji medycznej (EDM). Wraz z rozwojem technologii i urządzeń medycznych, rozwija się również ich wzajemna komunikacja oraz interoperacyjność i, choć przeważnie działają one niezależnie, wiele jest podłączonych do jednej sieci w obrębie podmiotu świadczącego usługi lecznicze. Obecnie, zgodnie z danymi pochodzącymi z północnoamerykańskich szpitali, na jedno łóżko chorego przypada od 10 do 15 zintegrowanych urządzeń podpiętych do sieci (Walker, 2017). Są to jedynie niektóre z powodów, dla których dane wrażliwe pochodzące z sektora ochrony zdrowia stanowią obecnie nawet 30% wszystkich danych, a ich ilość wzrasta wykładniczo wraz ze wzrastającym ryzykiem zagrożeń dla ich bezpieczeństwa, integralności i poufności (Hoffman, 2020). Są to niezwykle intymne i wrażliwe informacje dotyczące m.in. aktualnych chorób, przebytych operacji, przyjmowanych leków, nałogów, czy także członków rodziny, a nawet sytuacji socjoekonomicznej pacjenta (Najbuk, Kaźmierczyk, Dziomdziora i Marczuk, 2017). Warunki te stanowią zatem niezwykle ambitne wyzwanie dla wszystkich osób zarówno odpowiedzialnych pośrednio i bezpośrednio za podmioty zajmujące się opieką zdrowotną, jak i tych odpowiadających holistycznie za cały system ochrony zdrowia i jego administrację.

Najbardziej aktualne artykuły poruszające tematykę cyberbezpieczeństwa wskazują, iż branża opieki zdrowotnej pozostaje daleko w tyle pod względem jego implementacji (Kruse, Frederick, Jacobson i Monticone, 2017). Podczas gdy inne sektory infrastruktury krytycznej również są celami cyberataków, powagę problemu w sektorze medycznym istotnie podnoszą potencjalne konsekwencje,

które wykraczają poza straty finansowe czy naruszenie prywatności danych pacjentów (Gordon, Fairhall i Landman, 2017; Jarrett, 2017; Kramer, Fu, 2017; Perakslis, 2014). Co więcej, niezwykle ważne jest to, że cyberataki w tym sektorze mogą wiązać się z bezpośrednim zagrożeniem dla zdrowia i życia pacjentów – przykładem mogą być tu medialne przypadki *ransomware*[1], takie jak *WannaCry*, *NotPetya* czy incydenty, które miały miejsce w polskiej cyberprzestrzeni, jakim był na przykład wyciek danych pacjentów z Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Kole, czy liczne informacje załączone w publicznie dostępnym katalogu systemu stosowanego do obsługi placówek opieki zdrowotnej (Clarke i Youngstein, 2017; Gordon *et al.*, 2017; Majdan, 2017). Dodatkowo, zgodnie z raportem *ENISA* incydenty w obszarze ochrony zdrowia mogą mieć bardzo duży wpływ na całe społeczeństwo (Liveri, Sarri i Skouloudi, 2015).

Biorąc pod uwagę rosnące znaczenie cyberbezpieczeństwa dla prawidłowego funkcjonowania sektora opieki zdrowotnej, niezbędne staje się kompleksowe opracowanie problematyki poruszanej w literaturze z pogranicza medycyny i cyberbezpieczeństwa. Wierzymy, że współpraca obu tych sektorów może przynieść wymierne korzyści wszystkim zainteresowanym. Oczekiwać można, że kooperacja ta wzmocni nie tylko kompatybilność rozwiązań z potrzebami sektora ochrony zdrowia, ale również zwiększy popyt na nie. Jednocześnie warto pamiętać, że dane medyczne i ich bezpieczeństwo dotyczą każdego obywatela, a w konsekwencji troska o te dane leży w interesie każdego z nas.

Bezpieczeństwo ma ogromne znaczenie dla społeczeństwa – zarówno na szczeblu indywidualnym, jak i zbiorowym. Problematyka dotycząca bezpieczeństwa ma charakter interdyscyplinarny, stąd trudno wyodrębnić wspólne dla wielu dyscyplin kryteria i wprowadzić jednolitą typologię bezpieczeństwa. Zarówno cyberbezpieczeństwo, jak i ochrona zdrowia stanowią odrębne dziedziny traktujące o bezpieczeństwie. Spotykają się one w tym artykule, w którym przedstawiamy przegląd literatury, skupiając się szczególnie na cyberbezpieczeństwie jako ogóle technik, procesów i praktyk stosowanych w celu ochrony sieci informatycznych, urządzeń, programów i danych w obrębie sektora bezpieczeństwa, jakim jest ochrona zdrowia.

Do przygotowania przeglądu literatury przeszukano bazę danych PubMed,

[1] *Ransomware* – definiowane jako kategoria złośliwego oprogramowania, które po uruchomieniu wyłącza funkcjonalności komputera (0'Gorman i McDonald, 2012).

wykorzystując terminy *cybersecurity* lub *databreach* i *healthcare* lub *medical data*. Aby zmaksymalizować liczbę uzyskanych danych, autorzy przeszukali ręcznie bibliografie wyszukanych artykułów. Wykorzystano jedynie artykuły wydane w latach 2010–2020. W celu wzbogacenia artykułu do wybranej literatury dołączono liczne raporty stworzone w ostatnich latach przez instytucje podejmujące problematykę cyberbezpieczeństwa.

Problematyka cyberbezpieczeństwa

Falessi (2012) analizując narodowe strategie dotyczące cyberbezpieczeństwa (CS – *cyber security*) państw członkowskich Unii Europejskiej, zaznaczył, że nie ma powszechnej ani prostej definicji CS (Falessi, Gavrila, Klejnstrup i Moulinos, 2012). Termin cyberbezpieczeństwa jest powszechnie używany zamiennie z terminem bezpieczeństwa informacji (IS – *information security*). Według niektórych naukowców CS uznawana jest za gałąź IS, która koncentruje się bardziej na integralności i dostępności aniżeli poufności danych, tak jak ma to miejsce w przypadku IS (Wamala, 2011). Inni uznają, że CS wykracza poza granice tradycyjnego IS i obejmuje nie tylko ochronę zasobów informacyjnych, ale także ochronę innych aktywów, w tym zasobów ludzkich, które dodatkowo przyjmują wymiar potencjalnego celu cyberataków (von Solms i van Niekerk, 2013), co w kontekście sektora ochrony zdrowia ma szczególne znaczenie. Ataki na sektor ochrony zdrowia mogą bowiem przybierać charakter terroryzmu nie tylko systemowego, ale również wymierzonego bezpośrednio w pacjenta, stanowiąc bezpośrednie zagrożenie dla jego zdrowia i/lub życia.

Wśród najbardziej aktualnych doniesień znaleźć można nową, ulepszoną definicję cyberbezpieczeństwa, opartą na zestawieniu dotychczas stosowanych definicji oraz ich leksykalnej i semantycznej analizie. Określa ona CS jako *podejście i działania związane z procesami zarządzania ryzykiem bezpieczeństwa stosowane przez organizacje i państwa w celu ochrony poufności integralności i dostępność danych i zasobów wykorzystywanych w cyberprzestrzeni. Koncepcja obejmuje wytyczne, zasady i zbiory zabezpieczeń, technologii, narzędzi i szkoleń, aby zapewnić najlepszą ochronę stanu środowiska cybernetycznego i jego użytkowników* (Schatz, Bashroush, Wall, 2017, s. 64). Warto zwrócić uwagę na jej holistyczny charakter i podkreślenie ochrony końcowego użytkownika cyberprzestrzeni.

Cyfryzacja i cyberbezpieczeństwo w ochronie zdrowia

Cyfryzacja ochrony zdrowia istotnie postępuje. Współdzielone systemy czy bazy danych podmiotów leczniczych oraz obsługa danych przez zewnętrzne firmy wiążą się z potencjalnymi zagrożeniami i atakami na sieci informatyczne, urządzenia, programy i dane wykorzystywane przez podmioty lecznicze (Jalali i Kaiser, 2018). Już w 2009 roku w Stanach Zjednoczonych w ramach programu *Obamacare* uchwalono HITECH Act (*Health Information Technology for Economic and Clinical Health Act*), który ma za zadanie promować i poszerzać wdrażanie technologii informacyjnych w opiece zdrowotnej, w tym cyfryzację dokumentacji medycznej w celu usprawnienia oraz poprawy jakości i bezpieczeństwa prowadzonej opieki medycznej (HealthIT.gov, b/d).

W Polsce cyfryzacja sektora branży zdrowotnej trwa od wielu lat. Proces legislacji rozpoczął się od wprowadzenia pojęcia elektronicznej dokumentacji medycznej przez ustawę o systemie informacji w ochronie zdrowia z 2011 roku (Dz. U. 2011, poz. 657). Wprowadzenie informatyzacji w codzienną pracę szpitali i innych placówek medycznych znacząco wzrosło wraz z wprowadzeniem obowiązkowej elektronicznej dokumentacji medycznej (po 31 grudnia 2017 roku), e-zwolnień (grudzień 2018 roku) oraz e-recept (styczeń 2020 roku). W coraz większej liczbie ośrodków pacjenci mają dostęp do chirurgii robotowej, a także rośnie istotnie dostępność i powszechność urządzeń oraz aplikacji wspierających leczenie przewlekłe i regularną ocenę stanu zdrowia. Szczególną rolę można przypisać także aktualnie trwającej pandemii wirusa SARS-CoV-2 – praktycznie z dnia na dzień rozpoczęło się powszechne udzielanie porad medycznych telefonicznie i internetowo, a wiele placówek służby zdrowia na czas pandemii całkowicie przeszło na zdalny tryb pracy.

Pandemia COVID-19 wywiera olbrzymi wpływ nie tylko na funkcjonowanie podmiotów z zakresu ochrony zdrowia, ale też na działalność wielu przedsiębiorstw, wymuszając masową pracę zdalną i zwiększając zapotrzebowanie na usługi wideokonferencyjne, aplikacje w chmurze i zasoby sieciowe. W tegorocznym dokumencie IBM Security zatytułowanym *Raport z badania kosztów naruszeń ochrony danych 2020* znajdujemy ciekawe dane wynikające z odpowiedzi uczestników badania na pytania dotyczące potencjalnego wpływu pandemii COVID-19 na koszty naruszeń ochrony danych. Z raportu wynika, że aż 54% organizacji nakazało pracę zdalną w reakcji na epidemię. Według

76% uczestników ankiety praca zdalna wydłuży czas potrzebny na rozpoznanie i powstrzymanie naruszenia ochrony danych, a 70% spośród nich uważa, że praca zdalna zwiększy koszty naruszeń ochrony danych (IBM, 2020). Podobnych zmian powinniśmy spodziewać się też w sektorze ochrony zdrowia – implementacja pytań z przytoczonego badania w grupie składającej się wyłącznie z pracowników placówek świadczących usługi medyczne mogłaby dostarczyć niezwykle ciekawych wyników.

Według Becker's Hospital Review, na podstawie analizy Ponemon Institute, naruszenia danych generują dla branży ochrony zdrowia koszty około 5,6 mld dolarów rocznie w samych Stanach Zjednoczonych (Grealish, 2016), a zgodnie z *Report Breach Barometer: Year in Review* w 2016 roku dochodziło do co najmniej jednego naruszenia danych zdrowotnych dziennie, które łącznie miały wpływ na ponad 27 mln dokumentów (Protenus, 2017).

Liczne badania wskazują, że duża część zagrożeń bezpieczeństwa danych wrażliwych związanych jest z nieprawidłowym postępowaniem personelu pracującego z tymi danymi – załączaniem ich w wiadomościach e-mailowych, wynoszeniem dokumentacji poza miejsce opieki czy przesyłaniem dokumentacji na prywatne urządzenia mobilne (Jiang, Bai, 2019; Liu, Musen, Chou, 2015). Co więcej, posiadanie przez personel sektora ochrony zdrowia świadomości wagi problematyki cyberbezpieczeństwa wydaje się szczególnie istotna w obliczu informacji, że kadry medyczne coraz częściej padają ofiarą celowanych ataków typu e-mail *phishing*[2] (Gordon *et al.*, 2019). Źródła jednoznacznie wskazują najczęściej spotykane zagrożenia dla bezpieczeństwa danych w sektorze medycznym w Stanach Zjednoczonych. Są to przede wszystkim kradzież lub zgubienie urządzeń, incydenty hakerskie, nieuprawniony dostęp lub nieprawidłowe załączenie do wiadomości czy niewłaściwa utylizacja danych (Jiang i Bai, 2019; Seh *et al.*, 2020).

Według Federalnego Biura Śledczego (*Federal Bureau of Investigation*, FBI) ataki na opiekę zdrowotną dotyczą najczęściej kradzieży danych uwierzytelniających pracowników sektora przy użyciu złośliwego oprogramowania, w tym trojanów, oraz infiltracji sieci podmiotów świadczących usługi medyczne. Dodatkowo, potencjalne zagrożenia wynikają ze słabych wewnętrznych procedur

[2] *Phishing* – definiowany jako cyberoszustwo, w ramach którego przestępca uzyskuje informacje od zaatakowanego użytkownika poprzez podszywanie się pod zaufane jednostki (Lastdrager, 2014).

bezpieczeństwa dotyczących ochrony danych podczas wykorzystania oprogramowania w podmiotach oraz zewnętrznych przy outsourcingu usług przechowywania danych pacjentów (Hoffman, 2020).

Co więcej, media coraz częściej donoszą, iż branża opieki zdrowotnej jest jednym z najbardziej pożądanych celów obieranych przez cyberprzestępców ze względu na czarnorynkową wartość tych danych, które przy kompletnych bazach są warte nawet 10 razy więcej niż informacje z karty kredytowej danej osoby (Humer i Finkle, 2014; Murray, 2019; Stack, 2017).

Według raportu firmy Corvus (b/d) *ransomware* nadal pozostaje jednym z największych cyberzagrożeń dla sektora opieki zdrowotnej. Jedynie w okresie między czwartym kwartałem 2018 roku a tożsamym okresem roku 2019 udokumentowano 350-procentowy wzrost liczby ataków typu *ransomware* na podmioty medyczne (Corvus Insurance, b/d). Istotny jest fakt, że przedstawiciele sektora opieki zdrowotnej są skłonni do płacenia okupu, ponieważ konsekwencje związane z zakłóceniem ciągłości świadczenia usług medycznych lub utrata danych pacjentów mogą osiągnąć znacznie wyższy wymiar szkodliwości. Szacuje się, że 23% podmiotów z branży opieki zdrowotnej dokonało jakiejś formy płatności na rzecz okupu z powodu ataku typu *ransomware* (Zurkus, 2018).

Ponadto, nawiązując do raportu KPM *Health care and cyber security: Increasing Threats Require Increased Capabilities*, kolejnymi powodami podatności sektora zdrowia na cyberzagrożenia, poza wspomnianą wcześniej postępującą cyfryzacją, jest stosowanie przestarzałych aplikacji do sporządzania EDM i aplikacji klinicznych, które nie zostały zaprojektowane do bezpiecznego działania w aktualnym środowisku sieciowym. Kolejną przyczyną okazuje się niejednorodny charakter systemów i aplikacji sieciowych oraz wykorzystywanie urządzeń z obsługą sieci w tej samej sieci co infrastruktura krytyczna podmiotu (KPMG, 2015).

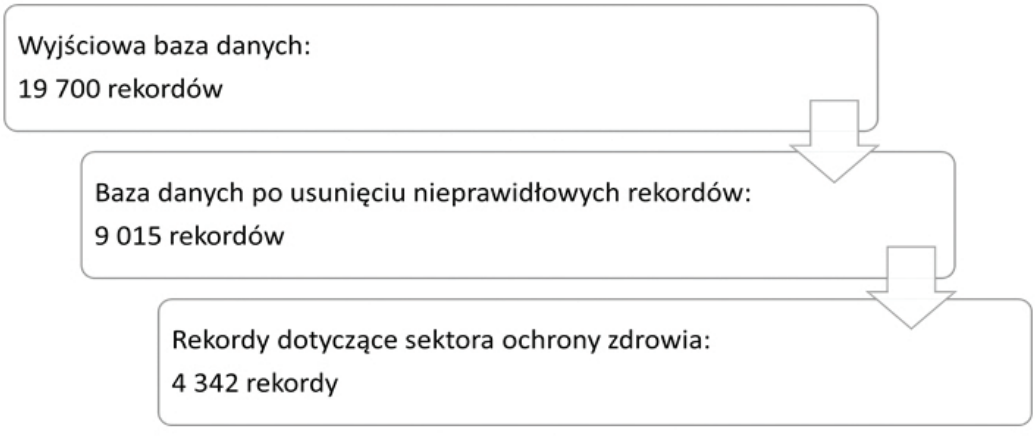
Ze względu na fakt, że dane medyczne są często warte więcej niż te, dotyczące tożsamości czy instrumentów finansowych, nacisk na bezpieczeństwo tych danych powinien być jednym z priorytetów systemów ochrony zdrowia (Kruse *et al.*, 2017). Jak pokazały wspomniane ataki z Wielkiej Brytanii czy Stanów Zjednoczonych, wzrost intensywności ataków typu *ransomware* na szpitale może doprowadzić do wstrzymania funkcjonowania całych systemów opieki zdrowotnej oraz znaczących skutków finansowych i zdrowotnych dla społeczeństwa (Deane-McKenna, 2017).

Dyrektywa NIS zakłada poszerzenie współpracy państw członkowskich w kwestii cyberbezpieczeństwa. Jednym z sektorów objętych dyrektywą jest sektor e-zdrowia obejmujący zagadnienia przetwarzania elektronicznej dokumentacji medycznej (Parlament Europejski i Rada Unii Europejskiej, 2016).

Analiza bazy danych *Chronology of Data Breaches*

W celu pogłębionej analizy problemu wykorzystaliśmy publicznie dostępną bazę danych *Chronology of Data Breaches* autorstwa *Privacy Rights Clearinghouse* (Privacy Rights Clearinghouse, b/d). Składa się ona z danych zebranych głównie na podstawie informacji udostępnianych przez prokuratorów generalnych oraz departament zdrowia i opieki społecznej Stanów Zjednoczonych. Oryginalnie zawiera 19700 rekordów, z czego – z powodu niepoprawnego wypełnienia pewnej ich części – w analizie wykorzystano 9015. Wyizolowane rekordy zostały uszeregowane według roku ich zgłoszenia (warto zauważyć, że rok zgłoszenia nie w każdym przypadku odpowiada momentowi wystąpienia zdarzenia).

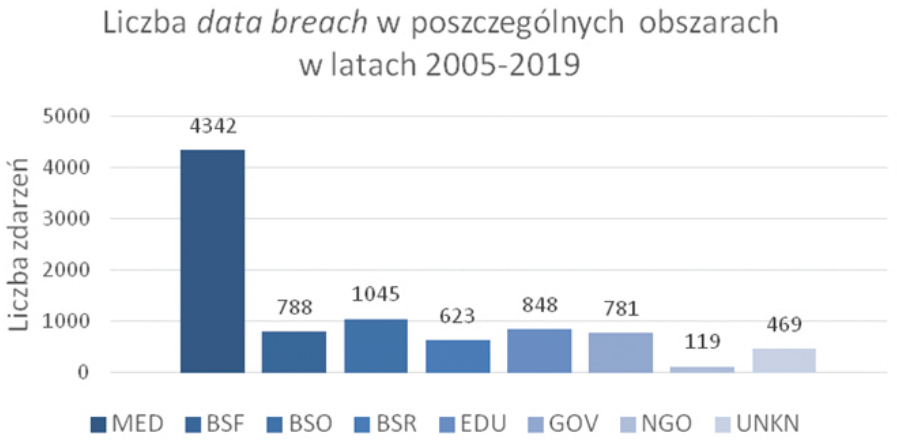
Schemat 1: Liczba rekordów wykorzystanych w analizie.



Źródło: analiza własna.

W latach 2005–2019 znacząca część zgłoszonych incydentów związanych z bezpieczeństwem danych miała miejsce w sektorze medycznym; zaraportowane zostały 4342 zdarzenia, co stanowi 48,16% wszystkich incydentów przekazanych do wiedzy publicznej.

Wykres 1: Liczba zagrożeń bezpieczeństwa danych (data breach) w poszczególnych obszarach w latach 2005–2019.

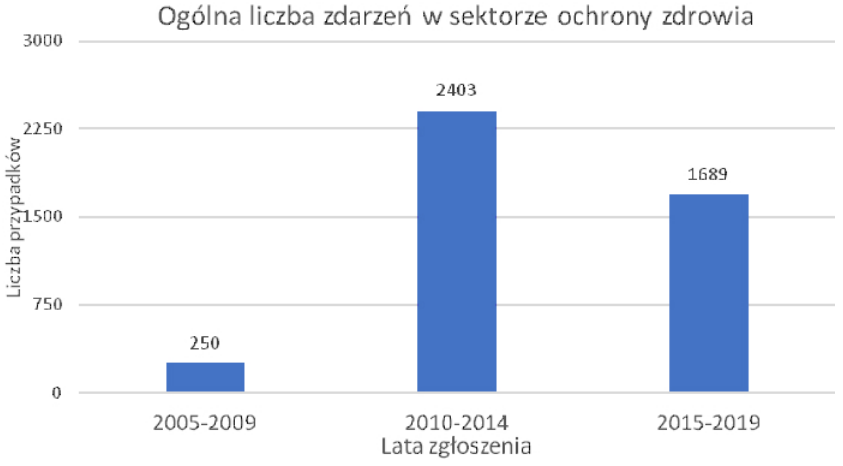


Legenda: EDU: organizacje edukacyjne; BSF: biznes–finanse; BSO: przedsiębiorstwa – inne; BSR: biznes–handel detaliczny (obejmuje sprzedaż detaliczną online); MED: dostawcy usług opieki zdrowotnej; GOV: instytucje rządowe i obronne; NGO: organizacje pozarządowe; UNKN: nieznane.

Źródło: analiza własna.

Choć częstość występowania zdarzeń związanych z naruszeniem bezpieczeństwa danych w sektorze medycznym ulegała znaczącym zmianom na przestrzeni lat, to jednak wykazywała stałą tendencję wzrostową.

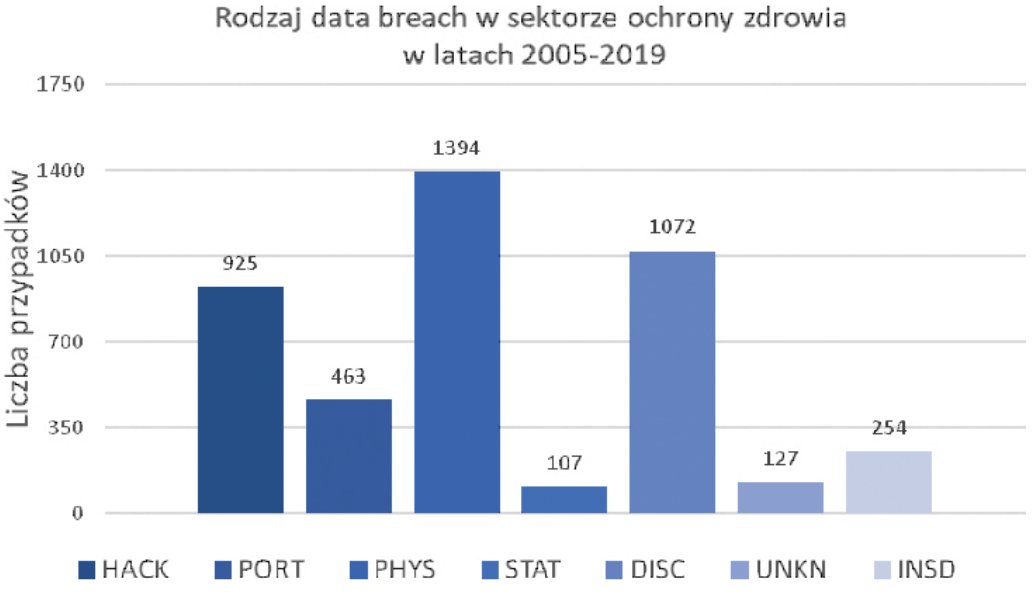
Wykres 2: Ogólna liczba zdarzeń w sektorze ochrony zdrowia w poszczególnych 5-letnich okresach.



Źródło: analiza własna.

Na podstawie naszej analizy danych zawartych w bazie wynika, że w sektorze medycznym USA do najczęstszych przyczyn *data breach* należą: (1) fizyczne (zgubienie, wyrzucenie lub skradzenie dokumentów papierowych), (2) zhakowanie przez podmiot zewnętrzny lub zainfekowanie złośliwym oprogramowaniem, (3) niezamierzone ujawnienie nieobejmujące hakowania, umyślnego naruszenia lub fizycznej utraty (publikowane publicznie, niewłaściwie przetwarzane lub wysyłane do niewłaściwej strony poprzez publikację online, wysyłanie e-mailem, wysyłanie pocztą lub wysyłanie faksem) oraz (4) urządzenie przenośne (zgubiony, wyrzucony lub skradziony laptop, PDA, smartfon, pendrive, płyty CD, dysk twardy, taśma z danymi itp.).

Wykres 3: Rodzaj zagrożenia dla bezpieczeństwa danych w sektorze ochrony zdrowia w latach 2005-2019.

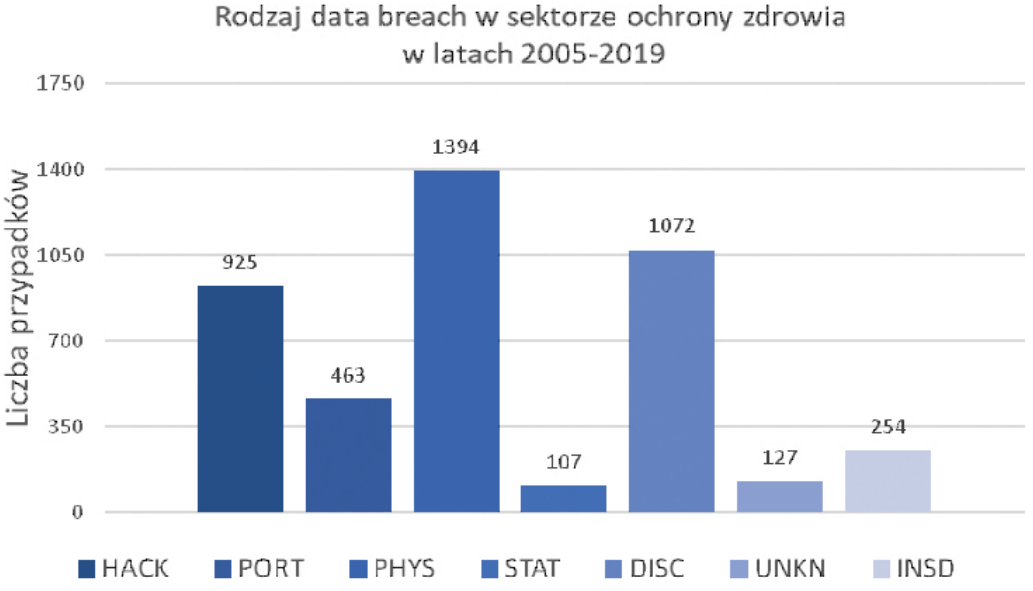


Legenda: DISC: niezamierzone ujawnienie; HACK: hakowanie lub złośliwe oprogramowanie; INSD: ataki „od środka"; PHYS: uszkodzenie fizyczne, kradzież lub utrata dokumentów papierowych; PORT: uszkodzenie urządzenia przenośnego, takie jak zgubienie lub kradzież; STAT: utrata komputera stacjonarnego; UNKN: nieznane.

Źródło: analiza własna.

W poszczególnych 5-letnich przedziałach zauważyć można znaczną tendencję wzrostową takich przyczyn, jak hakowanie oraz niezamierzone ujawnienie.

Wykres 4: Liczba przypadków *data breach* w zależności od lat zgłoszenia.



Legenda: DISC: niezamierzone ujawnienie; HACK: hakowanie lub złośliwe oprogramowanie; INSD: ataki "od środka"; PHYS: uszkodzenie fizyczne, kradzież lub utrata dokumentów papierowych; PORT: uszkodzenie urządzenia przenośnego, takie jak zgubienie lub kradzież; STAT: utrata komputera stacjonarnego; UNKN: nieznane.

Źródło: analiza własna.

Stan cyberbezpieczeństwa podmiotów medycznych w Polsce

Przeanalizowana przez nas baza danych jasno wskazuje, że na rynku zagranicznym coraz większe zagrożenie dla bezpieczeństwa danych w sektorze medycznym stanowią cyberprzestępcy oraz – przytaczane w licznych publikacjach (Gordon *et al.*, 2019; Jiang, Bai, 2019) – nieprawidłowe przesyłanie i udostępnianie danych medycznych przez sam personel podmiotów medycznych. Ze względu na brak oficjalnych baz i analiz zgłaszanych do CERT Polska[3] zdarzeń, nie możemy ekstrapolować tych wyników bezpośrednio na realia naszego kraju. W publicznie dostępnych raportach CERT Polska podaje jedynie, że w 2019 roku obsłużyła 53 incydenty w sektorze ochrony zdrowia, co stanowiło 0,8% wszystkich zdarzeń, jednocześnie podkreślając, że w poprzednim roku można było zaobserwować

[3] CERT Polska to zespół powołany do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet; działa od 1996 roku.

znaczący wzrost infekcji typu *ransomware* (NASK PIB/CERT Polska, 2019). Brakuje dostępnych analiz zarówno przyczyn naruszeń bezpieczeństwa danych, jak i ilości rekordów, których te naruszenia dotyczyły.

Z powodu braku wyczerpujących zestawień dotyczących bezpośrednio zagrożeń bezpieczeństwa danych, ocenę stanu polskiego rynku danych medycznych można przeprowadzić na podstawie kontroli Naczelnej Izby Kontroli *Wdrożenie przez podmioty lecznicze regulacji dotyczących ochrony danych osobowych* (NIK, 2019), przeprowadzonej w dniach 25 maja 2018 r. – 23 kwietnia 2019 r., tj. po wprowadzeniu obowiązkowej elektronicznej dokumentacji medycznej w placówkach medycznych. Wyniki tej kontroli wykazały liczne nieprawidłowości w zakresie zabezpieczenia i dostępu do danych wrażliwych:

- aż w 21% (n=5) placówek zauważono, że kopia zapasowa danych była przechowywana na nośnikach, których dotyczyła ta kopia.
- 46% (n=11) podmiotów przekazało zgłoszenia serwisowe do *helpdesków*[4] zawierające dane osobowe pacjentów, a także ich dane medyczne. Informacje te nie były niezbędne do rozwiązania usterek, możliwe było wykorzystanie automatycznie nadanego, zanonimizowanego ID pacjenta.
- 75% (n=18) szpitali nie stosowało odpowiednich środków zabezpieczenia elektronicznej dokumentacji medycznej.
- w 30% (n=7) placówek część komputerów nie była chroniona przez oprogramowanie antywirusowe lub nie posiadały one aktualnych baz sygnatur wirusów.

Kolejne nieprawidłowości wykazano w zakresie tworzenia i aktualizacji haseł, stosowaniu tej samej pary login-hasło przez dużą część personelu, a nawet braku uwierzytelniania użytkownika przy włączaniu urządzenia. Raport donosi też o bardzo licznych przypadkach nadania uprawnień do przeglądu danych medycznych osobom, których zakres obowiązków nie wymagał dostępu do takich informacji. Co więcej, pojawiały się też informacje o wykorzystywaniu oprogramowania niewspieranego technicznie przez producenta, przypadkach nieprawidłowego udostępniania dokumentacji medycznej czy opóźnieniach w odbieraniu byłym pracownikom uprawnień do systemów informatycznych.

[4] *Helpdesk* – usługa odpowiedzialna za przyjmowanie zgłoszeń od użytkowników oraz ich rozwiązanie lub przekazanie.

Podobna kontrola NIK dotycząca tworzenia i udostępniania dokumentacji medycznej miała miejsce w 2016 roku. Pomimo że kontrola obejmowała okres sprzed wprowadzenia obowiązkowej EDM, warto zwrócić uwagę na kwestię zabezpieczenia danych pacjentów w tamtym okresie. W 11 z 24 skontrolowanych placówek dokumentacja medyczna nie była odpowiednio zabezpieczona przed zniszczeniem, uszkodzeniem, utratą czy nawet dostępem osób nieuprawnionych (NIK, 2016). W tym okresie niewiele ponad 40% szpitali było zinformatyzowanych (CSIOZ/Rynek Zdrowia, 2017), a 46% zbadanych podmiotów nie zapewniało podstawowych zasad bezpieczeństwa dokumentacji medycznej (NIK, 2016).

Co ciekawe, kontrola z 2016 roku wskazała, że jedynie niewielka część szpitali rozpoczęła migrację do EDM (n=2). W toku kontroli tych podmiotów nie stwierdzono istotnych nieprawidłowości w zabezpieczeniu i przechowywaniu EDM, natomiast takie nieprawidłowości zanotowano już w 75% podmiotów kontrolowanych w 2019 roku, po wprowadzeniu obowiązkowej EDM (NIK, 2016).

Pomimo braku publicznie dostępnych analiz polskiego rynku cyberbezpieczeństwa w sektorze ochrony zdrowia, problem podnoszony jest przez różne organizacje państwowe (Centrum Systemów Informacyjnych Ochrony Zdrowia, 2017; NASK PIB/CERT Polska, 2019), czy organizacje pozarządowe (Regional Cyber Labs, 2020). Może to sugerować, że pomimo nieprawidłowości w ochronie danych pacjentów problem ten albo nie dotyka jeszcze licznych podmiotów medycznych, albo – zakładając podobną częstość zdarzeń jak w krajach zachodnich – nie wszystkie zdarzenia są zgłaszane oficjalnym komórkom państwowym powołanym w celu ich zwalczania i badania, tj. CERT Polska.

Nieliczne organizacje podejmują problematykę cyberbezpieczeństwa w medycynie w ramach swoich działań popularyzujących. Jedną z nich jest fundacja The Bridge, która w 2020 roku rozpoczęła szereg takich działań, obejmujących różne sektory, w tym także medyczny. Wśród działań popularyzatorskich znalazły się kampania społecznościowa"*Don't click on sh*t* uczulająca internautów na niebezpieczeństwo związane z *phishingiem*, a także stworzenie studenckiego raportu *Nowe otwarcie w edukacji o cyberbezpieczeństwie 2020–2021*. Autorzy części medycznej uzyskali interesujące dane dotyczące postaw studentów kierunków medycznych polskich uczelni medycznych:

- 87,4% (n=166) respondentów uważa, że tematyka cyberbezpieczeństwa powinna być poruszana w toku studiów,

- jedynie u 18,4% (n=35) respondentów tematyka ta została poruszona w czasie zajęć (Makuch, Guziak, Karolak i Korczak, 2020).

Dane te wskazują na to, że pokolenie kształcące się na przyszłe kadry medyczne potencjalnie stanowi grupę, która w szczególności skorzystałaby ze szkoleń z zakresu cyberhigieny i szeroko rozumianego cyberbezpieczeństwa. To, w połączeniu z faktem, że najczęstsze zagrożenie bezpieczeństwa danych w tym sektorze wiąże się zazwyczaj z działaniami personelu, może stanowić skuteczne rozwiązanie umożliwiające znaczące ograniczenie takich incydentów w przyszłości.

Podsumowanie

Celem cyfryzacji w sektorze ochrony zdrowia jest nie tylko zwiększenie efektywności i usprawnienie diagnostyki oraz procesu terapeutycznego zespołowi medycznemu, ale także ułatwienie pacjentom kontaktu i interakcji z samym systemem. Jednocześnie, wraz z rozwojem technologii, cyberprzestępcy coraz częściej wykorzystują ludzkie niedociągnięcia, a także słabości istniejącej infrastruktury, aby dokonać kradzieży danych wrażliwych. Cyberataki są obecnie bardziej wyrafinowane i lepiej finansowane z powodu wzrastającej wartości danych medycznych na czarnym rynku. Wraz z pojawieniem się na świecie pandemii SARS-CoV-2 i przyspieszenia cyfryzacji tych możliwości przybywa.

Prawidłowe funkcjonowanie wykorzystywanych w opiece zdrowotnej technologii odgrywa kluczową rolę dla zdrowia całego społeczeństwa. Choć głównym zadaniem sektora pozostaje opieka nad pacjentem, równolegle dużo uwagi powinno się poświęcać infrastrukturze, w szczególności tej informacyjnej, ze względu na jej bezpośredni wpływ na realizację tego zadania, oraz ogromne ilości cennych, wrażliwych danych, które ta infrastruktura obsługuje.

Niezbędne jest nawiązanie dialogu między ekspertami od spraw cyberbezpieczeństwa a specjalistami związanymi z branżą medyczną. Ważna jest też aktywizacja pacjentów, którzy powinni czynnie uczestniczyć w ochronie swoich danych dotyczących zdrowia, ponieważ numer ubezpieczenia społecznego czy dokumentacja medyczna nie ulegają przedawnieniu i zostają z pacjentem na całe życie.

Z powodu zbyt skąpych danych dotyczących polskiego rynku cyberbezpieczeństwa w ochronie zdrowia w przyszłości niezbędne będzie przeprowadzenie szeroko zakrojonych badań w temacie. Ważna byłaby ocena

świadomości personelu medycznego i administracyjnego, a także ocena ich codziennych zachowań w tym zakresie.

Bibliografia

Centrum Systemów Informacyjnych Ochrony Zdrowia. (2017). *Rekomendacje Centrum Systemów Informacyjnych Ochrony Zdrowia w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej.* Warszawa: Centrum Systemów Informacyjnych Ochrony Zdrowia. Dostęp: https://cez.gov.pl/fileadmin/user_upload/rekomendacje_csioz_bezpieczenstwo_wrzesien2017_59cd1e951e9ba.pdf [15.09.2020].

Clarke, R. i Youngstein, T. (2017). Cyberattack on Britain's National Health Service — A Wake-up Call for Modern Medicine. *New England Journal of Medicine*, *377*(5), 409–411. DOI: https://doi.org/10.1056/NEJMp1706754

Corvus Insurance. (b/d). *Security Report. Health Care – Hospitals, Providers and more*. Boston: Corvus Insurance Holdings. Dostęp: https://info.corvusinsurance.com/hubfs/Security%20Report%202.2%20-%20Health%20Care%20.pdf [14.09.2020].

CSIOZ/Rynek Zdrowia. (2017, 6 czerwca). Radziwiłł: niewiele ponad 40 procent szpitali jest zinformatyzowanych. *Rynek Zdrowia*. Dostęp: https://www.rynekzdrowia.pl/Technologie-informacyjne/Radziwill-niewiele-ponad-40-procent-szpitali-jest-zinformatyzowanych,173509,7.html [27.10.2020].

Deane-McKenna, C. (2017, 13 maja). NHS ransomware cyber-attack was preventable. *The conversation.com*. Dostęp: https://theconversation.com/nhs-ransomware-cyber-attack-was-preventable-77674 [27.10.2020].

Falessi, N., Gavrila, R., Klejnstrup, M.R. i Moulinos, K. (2012). *National Cyber Security Strategies Practical Guide on Development and Execution*. Heraklion: European Network and Information Security Agency. Dostęp: https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide [28.10.2020].

Gordon, W.J., Fairhall, A. i Landman, A. (2017). Threats to Information Security – Public Health Implications. *The New England Journal Of Medicine*, *377*(8), 707–709. DOI: https://doi.org/10.1056/NEJMp1707212

Gordon, W.J., Wright, A., Aiyagari, R., Corbo, L., Glynn, R. J., Kadakia, J. i Landman, A. (2019). Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. *JAMA Network Open*, *2*(3). DOI: https://doi.org/10.1001/jamanetworkopen.2019.0393

Grealish, G. (2016, 20 czerwca). The top 5 cybersecurity threats hospitals need to watch for. *Becker Hospital Review*. Dostęp: https://www.beckershospitalreview.com/healthcare-information-technology/the-top-5-cybersecurity-threats-hospitals-need-to-watch-for.html [06.09.2020].

HealthIT.gov. (b/d). *Laws, Regulation, and Policy.* Dostęp: https://www.healthit.gov/topic/laws-regulation-and-policy [06.09.2020].

Hoffman, S.A.E. (2020). Cybersecurity Threats in Healthcare Organizations: Exposing Vulnerabilities in the Healthcare Information Infrastructure. *Information Security: Emerging Voices*, *24*(1). Dostęp: https://worldlibraries.dom.edu/index.php/worldlib/article/view/588 [06.09.2020].

Humer, C. i Finkle, J. (2014, 24 września). Your medical record is worth more to hackers than your credit card. *Reuters*. Dostęp: https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924 [09.09.2020].

IBM. (2020). *Raport z badania kosztów naruszeń ochrony danych w 2020 roku*. Dostęp : https://www.ibm.com/pl-pl/security/data-breach [27.10.2020].

Jalali, M.S. i Kaiser, J.P. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *Journal of Medical Internet Research*, *20*(5). DOI: https://doi.org/10.2196/10059

Jarrett, M.P. (2017). Cybersecurity – A Serious Patient Care Concern. *JAMA*, *318*(14). DOI: https://doi.org/10.1001/jama.2017.11986

Jiang, J. (Xuefeng) i Bai, G. (2019). Evaluation of Causes of Protected Health Information Breaches. *JAMA Internal Medicine*, *179*(2), 265–267. DOI: https://doi.org/10.1001/jamainternmed.2018.5295

KPMG. (2015). *Health care and cyber security: increasing threats require increased capabilities*. Dostęp: https://assets.kpmg/content/dam/kpmg/pdf/2015/09/cyber-health-care-survey-kpmg-2015.pdf [13.09.2020].

Kramer, D.B. i Fu, K. (2017). Cybersecurity Concerns and Medical Devices: Lessons From a Pacemaker Advisory. *JAMA*, *318*(21), 2077–2078. DOI: https://doi.org/10.1001/jama.2017.15692

Kruse, C.S., Frederick, B., Jacobson, T. i Monticone, D.K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1–10. DOI: https://doi.org/10.3233/THC-161263

Lastdrager, E.E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, 9. DOI: https://doi.org/10.1186/s40163-014-0009-y

Liu, V., Musen, M.A. i Chou, T. (2015). Data Breaches of Protected Health Information in the United States. *JAMA*, *313*(14). DOI: https://doi.org/10.1001/jama.2015.2252

Liveri, D., Sarri, A. i Skouloudi, C. (2015). *Security and Resilience in eHealth Security Challenges and Risks*. Heraklion: European Network and Information Security Agency. DOI: http://doi.org/10.2824/217830

Majdan, K. (2017, 12 czerwca). Nazwiska, numery PESEL i ubezpieczeń, historia badań. Duży wyciek danych z polskiego szpitala. *Business Insider*. Dostęp: https://businessinsider.com.pl/technologie/nowe-technologie/spzoz-w-kole-wyciek-danych-pacjentow/dbk7zzf [06.09.2020].

Makuch, J., Guziak, M., Karolak, N. i Korczak, M. (2020). Medycyna. W: *Raport: Nowe otwarcie w edukacji o cyberbezpieczeństwie 2020–2021*. Warszawa: The Bridge Foundation. Dostęp: https://98145a31-5189-415e-8474-41672cd6acb7.filesusr.com/ugd/2b3cfe_872f87ae3dd44675be1b7c7c75077e4f.pdf [27.10.2020].

Murray, K. (2019, 24 października). Why Healthcare Organizations are Easy Targets for Cybercrime. *Webroot.com*. Dostęp: https://www.webroot.com/blog/2019/10/24/why-healthcare-organizations-are-easy-targets-for-cybercrime/ [09.09.2020].

Najbuk, P., Kaźmierczyk, P., Dziomdziora, W. i Marczuk, P. (2017). *Cyberbezpieczeństwo w sektorze ochrony zdrowia*. Warszawa : DZP & Microsoft. Dostęp: https://www.dzp.pl/files/shares/Publikacje/Cyberbezpieczen%CC%81stwo%20w%20sektorze%20oz.pdf [15.10.2020].

NASK PIB/CERT Polska. (2019). *Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2019 z działaności CERT Polska.* Dostęp: https://www.nask.pl/pl/raporty/raporty/3873,Raport-CERT-2019.html [27.10.2020].

NIK. (2016). Tworzenie i udostępnianie dokumentacji medycznej. Informacja o wynikach kontroli nr 199/2015/P/15/061/KZD. Dostęp: https://www.nik.gov.pl/plik/id,10736,vp,13069.pdf [27.10.2020].

NIK. (2019). Wdrożenie przez podmioty lecznicze regulacji dotyczących ochrony danych osobowych. Informacja o wynikach kontroli nr 149/2019/P/19/063/LBI0. Dostęp: https://www.nik.gov.pl/plik/id,21467,vp,24109.pdf [27.10.2020].

O'Gorman, G. i McDonald, G. (2012). *Ransomware: A Growing Menace*. Dostęp: https://web.gccaz.edu/~davna92721/cis105/ransomware-a-growing-menace.pdf [27.10.2020]

Parlament Europejski i Rada Unii Europejskiej (2016). Dyrektywa Parlamentu Europejskiego i Rady UE nr 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. Unii Europejskiej L194 z 19.07.2016). Dostęp: http://data.europa.eu/eli/dir/2016/1148/oj [20.10.2020].

Perakslis, E.D. (2014). Cybersecurity in health care. *The New England Journal of Medicine*, *371*(5), 395–397. DOI: https://doi.org/10.1056/NEJMp1404358

Privacy Rights Clearinghouse. (b/d). *Data Breaches*. Dostęp: https://privacyrights.org/data-breaches [27.10.2020].

Protenus. (2017). *Breach barometer report: Year in review (2016)*. Baltimore: Protenus Inc. & DataBreaches.net. Dostęp: https://cdn2.hubspot.net/hubfs/2331613/Breach_Barometer/2016/2016%20Year%20in%20Review/Protenus%20Breach%20Barometer-2016%20Year%20in%20Review-%20final%20version.pdf [29.09.2020].

Regional Cyber Labs. (2020). *Raport: Nowe otwarcie w edukacji o cyberbezpieczeństwie 2020–2021*. Warszawa: Bridge Foundation. The Bridge Foundation. Dostęp: https://98145a31-5189-415e-8474-41672cd6acb7.filesusr.com/ugd/2b3cfe_872f87ae3dd44675be1b7c7c75077e4f.pdf [27.10.2020].

Schatz, D., Bashroush, R. i Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *The Journal of Digital Forensics, Security and Law*, *12*(2), 53–74. DOI: https://doi.org/10.15394/jdfsl.2017.1476

Seh, A.H., Zarour, M., Alenezi, M., Sarkar, A.K., Agrawal, A., Kumar, R. i Ahmad Khan, R. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare*, *8*(2). DOI: https://doi.org/10.3390/healthcare8020133

Stack, B. (2017, 6 grudnia). Here's How Much Your Personal Information Is Selling for on the Dark Web. *Experian.com*. Dostęp: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ [09.09.2020].

Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, (Dz. U. 2011, nr 113, poz. 657 ze zm.).

von Solms, R. i van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. DOI: https://doi.org/10.1016/J.COSE.2013.04.004

Walker, T. (2017, 10 grudnia). Interoperability a must for hospitals, but it comes with risks. *Managed Healthcare Executive*. Dostęp: https://www.managedhealthcareexecutive.com/view/interoperability-must-hospitals-it-comes-risks [27.10.2020].

Wamala, F. (2011). *The ITU National Cybersecurity Strategy Guide*. Geneva: International Telecommunication Union. Dostęp: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf [06.09.2020]

Zurkus, K. (2018, 10 maj). Healthcare Prone to Attack, Still Unprepared. *Infosecurity Magazine*. Dostęp: https://www.infosecurity-magazine.com/news/healthcare-prone-to-attack-still/ [09.09.2020].