https://doi.org/10.34862/rbm.2024.2.6
otrzymano: 04.IV.2024, zaakceptowano: 21.XII.2024

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

Kacper Ziarnik
Szpital Wojewódzki w Poznaniu
kacper.ziarnik@gmail.com
https://orcid.org/0009-0006-4676-3232

Przegląd naruszeń cyberbezpieczeństwa danych medycznych w polskim sektorze ochrony zdrowia w 2023 roku

Abstrakt: Elektroniczna Dokumentacja Medyczna (EDM) stała się domyślnym sposobem gromadzenia i przechowywania danych w sektorze ochrony zdrowia. Dane medyczne, agregowane w ten sposób są jednak szczególnie podatne na zagrożenia cybernetyczne, ostatnio szczególnie nasilone w obliczu wojny na Ukrainie. Stwarza to nowe wyzwania dla sektora ochrony zdrowia i wymaga wzmożonych środków zarówno w celu ochrony EDM, jak i cyberbezpieczeństwa całego sektora. W artykule dokonano przeglądu literatury oraz raportów instytucji rządowych i międzynarodowych w okresie 2013–2023. Przeszukano bazy danych PubMed i Google Scholar, w oparciu o terminy związane z cyberbezpieczeństwem sektora ochrony zdrowia i danymi medycznymi. Zebrane materiały poddane zostały analizie krytycznej. Dodatkowo przy użyciu Google Search dokonano przeglądu doniesień medialnych opisujących naruszenia cyberbezpieczeństwa polskiego systemu ochrony zdrowia w 2023 r. Autorzy wykazują, że w 2023 r. infrastruktura szpitalna w dalszym ciągu pozostawała podatna na cyberzagrożenia. Sektor ochrony zdrowia często był celem ataków cybernetycznych, a personel medyczny stał się ich celem głównym. Polskie instytucje medyczne odnotowały 405 incydentów zagrożeń cybernetycznych, a *ransomware* był najczęstszym typem ataku. Analiza incydentów wskazuje na znaczną różnorodność ataków. Do najbardziej znaczących zdarzeń w 2023 r. należały: atak na infrastrukturę serwerową Centrum Medycznego TW-DS. oraz atak *ransomware* na ALAB Laboratoria. Liczba incydentów zagrożeń cybernetycznych w sektorze

ochrony zdrowia utrzymuje się na wysokim poziomie. W obliczu wyzwań konieczne są skuteczne działania, aby zapewnić bezpieczeństwo danych pacjentów. Wskazujemy na znaczną rolę edukacji personelu w tym zakresie. Współpraca pomiędzy instytucjami medycznymi i ekspertami ds. cyberbezpieczeństwa wydaje się kluczowa dla zapewnienia skutecznej ochrony danych medycznych w erze rosnących zagrożeń cybernetycznych.

Słowa kluczowe: ochrona danych, cyberbezpieczeństwo, elektroniczna dokumentacja medyczna, ochrona zdrowia

A Review of Medical Data Security Breaches in the Polish Healthcare Sector in 2023

Abstract: Electronic Medical Records (EMR) have become the default method for collecting and storing data in the healthcare sector. However, medical data aggregated in this manner are particularly vulnerable to cyber threats, which have notably intensified in light of the war in Ukraine. This situation poses new challenges for the healthcare sector, necessitating enhanced measures to protect both EMR and the cybersecurity of the entire sector. This article reviews the literature and reports from government and international institutions covering the period from 2013 to 2023. Databases such as PubMed and Google Scholar were searched using terms related to healthcare sector cybersecurity and medical data. The materials were critically analysed. Additionally, a review of media reports describing cybersecurity breaches in the Polish healthcare system in 2023 was conducted using Google Search. The authors present that in 2023, hospital infrastructure remained susceptible to cyber threats. The healthcare sector frequently became the target of cyberattacks, with medical personnel being their primary focus. Polish medical institutions reported 405 incidents of cyber threats, with ransomware being the most common type of attack. The analysis of incidents highlighted a significant diversity of attacks. Among the most noteworthy incidents in 2023 were an attack on the server infrastructure of TW-MED Medical Center and a ransomware attack on ALAB Laboratories. The number of cybersecurity threat incidents in the healthcare sector remains high. In the face of these challenges, effective actions are necessary to ensure the safety of patient data. We emphasise the crucial role of staff education in this regard. Collaboration between medical institutions and cybersecurity experts appears essential for ensuring the effective protection of medical data in an era of increasing cyber threats.

Keywords: data protection, cybersecurity, electronical health records, healthcare

Wstęp

Jednym z kluczowych aspektów wdrażania technologii informacyjnych dla sektora ochrony zdrowia jest adaptacja Elektronicznej Dokumentacji Medycznej

(EDM) (ang. *electronic health record*, EHR) jako fundamentalnego narzędzia zarządzania danymi medycznymi (Milieu Ltd., 2014). EDM jest zorientowanym na pacjencie, aktualizowanym w czasie rzeczywistym elektronicznym dokumentem, do którego bezpośredni dostęp posiada wyłącznie autoryzowany personel medyczny (HealthIT.gov, b.d.). EDM zawiera dane demograficzne pacjenta, historię jego choroby, wcześniejszych wizyt, hospitalizacji, a także dane administracyjne i rozliczeniowe związane z otrzymaną opieką (Nancy i Maheswari, 2020; HealthIT.gov, 2019). W Polsce, w odpowiedzi na dynamiczny rozwój i zmieniające się potrzeby sektora ochrony zdrowia, wdrożono regulacje, wprowadzające obowiązek prowadzenia dokumentacji w formie EDM. Zgodnie z obowiązującym porządkiem prawnym, od 1 stycznia 2021 r. wszyscy dostawcy usług medycznych (lekarz, ośrodek medyczny, przychodnia zdrowia, klinika, sanatorium, szpital, centrum ambulatoryjne, ośrodek rehabilitacyjny i pracownicy powyższych instytucji (Ustawa, 2011) zobowiązani są do prowadzenia EDM zgodnie z rozporządzeniem z 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej (Rozporządzenie, 2020). W kontekście ochrony zdrowia EDM gromadzi wszelkie informacje, jakie podmiot leczniczy – samodzielny zakład opieki zdrowotnej, przedsiębiorca, a także instytut badawczy czy fundacja – uzyskuje bezpośrednio od pacjenta lub pośrednio, o jego osobie (Ustawa, 2011). W związku z powyższym, EDM zawiera i powiązuje personalia pacjenta z bardzo szczegółowymi informacjami odnośnie jego stanu zdrowia. W świetle aktualnie obowiązujących przepisów większość tych informacji stanowi dane wrażliwe i podlega szczególnej ochronie (OECD, 2013; Rozporządzenie, 2016).

Meglena Kuneva, europejska komisarz ds. ochrony konsumentów, jeszcze w 2009 r. podkreślała, że: „dane osobowe to nowa ropa w Internecie i nowa waluta cyfrowego świata" (ang. „*Personal data is the new oil of the internet and the new currency of the digital world*"), tym samym uznając kluczową rolę danych w gospodarce cyfrowej (Kuneva, 2009). W tym kontekście dane dotyczące stanu zdrowia są niezwykle cenne, a ich kompletność oraz poprawność stanowią bezwzględny warunek dla efektywnego funkcjonowania każdego podmiotu medycznego, a w konsekwencji prawidłowego funkcjonowania całego systemu ochrony zdrowia (Evans, 2018; Reddix-Smalls, 2012).

Wojna na Ukrainie stanowi istotne zagrożenie dla cyberbezpieczeństwa danych medycznych i sektora ochrony zdrowia w Polsce (Guziak i Bastrzyk, 2023). Powołując się na słowa wiceministra zdrowia Piotra Brombera, w ostatnim czasie

wzrosło prawdopodobieństwo ataków cybernetycznych i hakerskich na podmioty ochrony zdrowia (Ministerstwo Zdrowia, 2022). Co więcej, od lutego do grudnia 2022 r. polski system ochrony zdrowia przyjął dodatkowo ponad 350 tys. pacjentów z Ukrainy, generując tym samym znaczącą ilość nowej EDM (Solecka, 2023). W sferze cyber, sektor medyczny w Polsce stanął tym samym przed wyzwaniem zarówno utrzymania infrastruktury krytycznej w obliczu konfliktu zbrojnego toczonego bezpośrednio za wschodnią granicą państwa, ale także przetwarzania i zapewnienia bezpieczeństwa znacznie większej ilości danych.

Metody przeglądu i pojęcia z zakresu cyberbezpieczeństwa

Na potrzeby badania przeszukane zostały elektroniczne bazy danych PubMed i Google Schoolar z wykorzystaniem terminów: *cybersecurity and war*, *cybersecurity and Ukraine, patient data and war*, *electronic health record and war*. Wyniki obejmujące tytuły i treści artykułów ograniczono do prac opublikowanych w latach 2013–2023. Autorzy posłużyli się literaturą z zakresu: informatyki, kryptografii, prawa, etyki, socjotechniki oraz inżynierii oprogramowania. Dodatkowo, w celu maksymalizacji liczby uzyskanych materiałów związanych z tematyką badania, autorzy sprawdzali bibliografie wyszukanych artykułów. Ponadto, przegląd objął raporty opublikowane przez podmioty rządowe i międzynarodowe oraz publikacje o charakterze doniesień medialnych z instytucji takich jak: OECD, Ministerstwo Zdrowia, CERT Polska, CSIRT NASK i portal HealthIT.gov. Zebrane artykuły i raporty poddane zostały krytycznej analizie, dokonano syntezy i uogólnienia wynikających z nich wniosków.

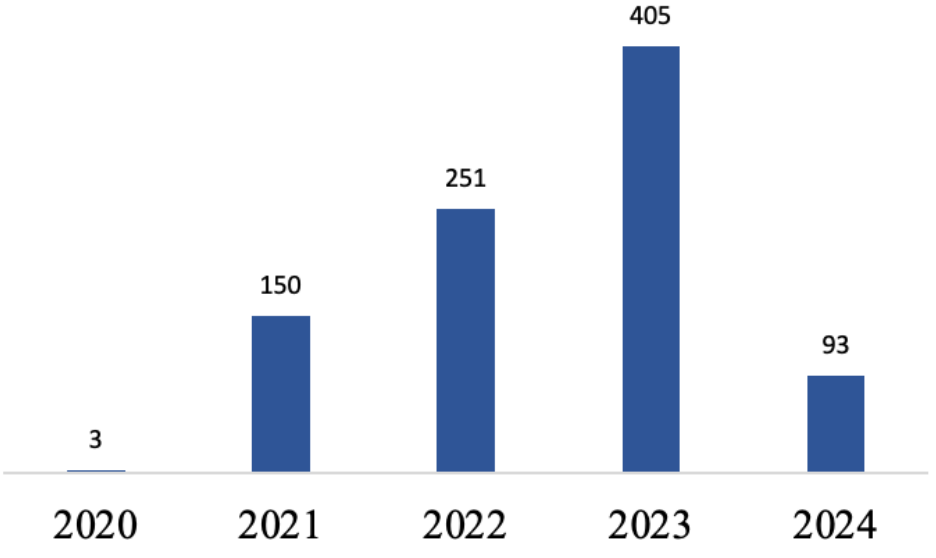
W niniejszym artykule przedstawiono przypadki ataków typu *ransomware* i *phishing*. *Ransomware* to rodzaj złośliwego oprogramowania, takiego jak wirusy czy trojany, które infekują komputer lub sieć, blokując dostęp do danych lub systemów. Najczęściej działanie *ransomware* polega na szyfrowaniu plików ofiary, co uniemożliwia ich odczytanie lub użycie, a następnie wymusza zapłatę okupu w zamian za klucz deszyfrujący. Z kolei *phishing* jest techniką wyłudzania poufnych informacji, takich jak dane logowania, numery kart kredytowych, hasła czy dane osobowe. Atakujący podszywają się pod zaufane instytucje lub osoby, wykorzystując fałszywe wiadomości e-mail, strony internetowe czy komunikaty, które przypominają oficjalne ogłoszenia, np. od banków, firm kurierskich czy

popularnych platform internetowych. Celem *phishingu* jest nakłonienie ofiary do ujawnienia danych osobowych lub kliknięcia w złośliwy link, co może prowadzić do infekcji urządzenia wirusem lub przejęcia kontroli nad jego systemem. W artykule wykorzystano również pojęcie oprogramowania złośliwego (*malware*), uwzględniającego trojany i wirusy oraz pojęcie oprogramowania szpiegującego, które mogą być użyte do kradzieży danych pacjentów lub zakłócenia pracy urządzeń medycznych – IoMT (Internet of Medical Things).

Cyberbezpieczeństwo sektora ochrony zdrowia w 2023 roku

Sektor ochrony zdrowia stanowi częsty cel ataków w ramach przestępczości cybernetycznej, zarówno w Polsce, jak i na świecie. Średni koszt naruszenia bezpieczeństwa danych osobowych w 2023 r. wyniósł 4,45 mln USD, co oznacza wzrost o 15% w ciągu ostatnich 3 lat (IBM Security, 2024).

Wykres 1. Incydenty z zakresu cyberbezpieczeństwa w sektorze ochrony zdrowia obsłużone przez CERT Polska w latach 2020-2024.



Dane dotyczące 2024 obejmują okres 01.01-07.03.2024.

Źródło: Opracowanie własne na podstawie danych CERT Polska.

Ze względu na dużą podatność, personel medyczny stanowi główny cel takich ataków (Makuch i Guziak, 2020). Niepokojący jest fakt, że aż 50% urządzeń szpitalnych podłączonych do Internetu jest podatnych na cyberataki, a 64% placówek opieki zdrowotnej wyraża obawy związane z bezpieczeństwem w tym obszarze (Diaz, 2022). Tylko 48% podmiotów ochrony zdrowia posiada opracowane procedury w postaci planu działania na wypadek wystąpienia zagrożenia cybernetycznego (Miliard, 2022).

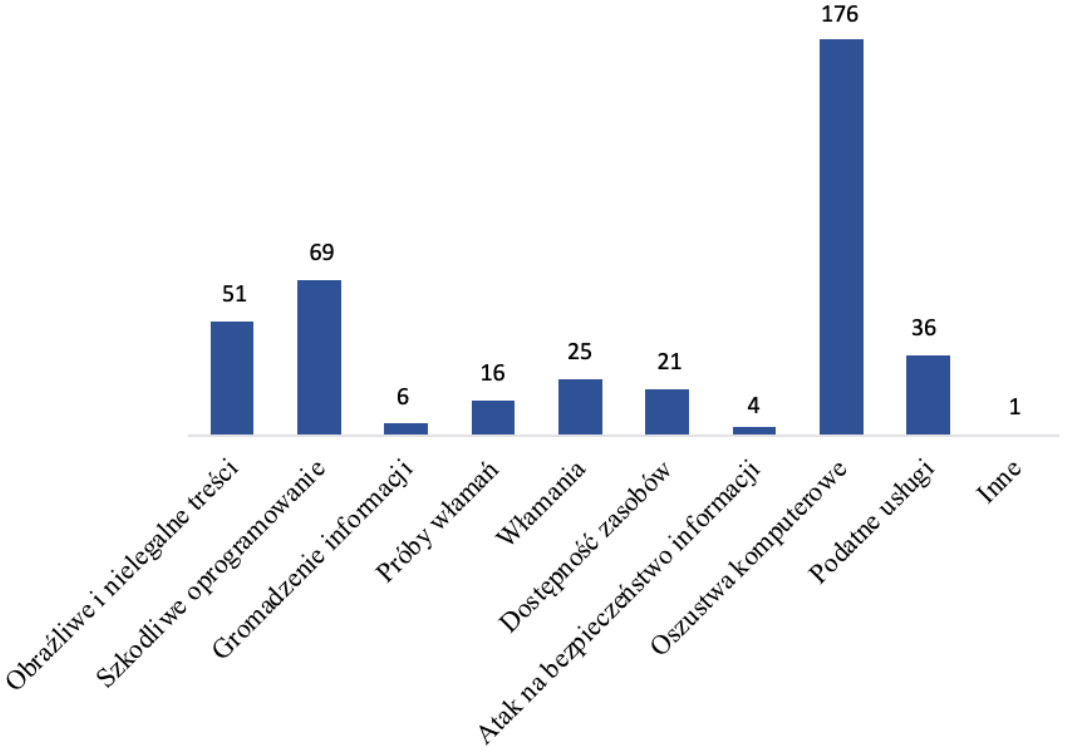
Warto podkreślić, że w Polsce od 2023 r. obowiązują uchwalone przez Radę Ministrów oraz Ministerstwo Cyfryzacji Narodowe Standardy Cyberbezpieczeństwa (NSC). Mimo wszelkich starań, tylko w sektorze ochrony zdrowia w 2023 r. zanotowano w Polsce 405 incydentów zagrożenia bezpieczeństwa cybernetycznego (wykres nr 1) (NSC, b.d.; CERT Polska, 2023).

Raport *ENISA Threat Landscape* 2023 ujawnia, że sektor medyczny najczęściej pada ofiarą ataków typu *ransomware,* które stanowią 54% wszystkich ataków (Lella i in., 2023).

Zagrożenia cyberbezpieczeństwa w sektorze ochrony zdrowia w 2023 roku

Obraz danych zagrożeń cyberbezpieczeństwa w 2023 r. (wykres 2) ukazuje różnorodność ataków, z oszustwami komputerowymi na czele – 176 zgłoszonych przypadków. Warto zauważyć, że 25 przypadków stanowiły włamania, co jednoznacznie pokazuje, że stosowane przez personel zabezpieczenia, nie były efektywne, a jednocześnie infrastruktura komputerowa w sektorze ochrony zdrowia pozostawała w kręgu zainteresowań hakerów. Nieautoryzowany dostęp do infrastruktury komputerowej naraża z kolei pacjentów na ryzyko utraty poufności ich dokumentacji medycznej. Analiza 176 przypadków oszustw komputerowych wskazuje, że metody, takie jak *phishing*, fałszywe e-maile czy ataki hakerskie są niezmiennie skuteczne. Podkreśla to potrzebę ciągłego rozwoju środków ochrony i edukacji w zakresie cyberbezpieczeństwa na różnych szczeblach kadry medycznej.

Wykres 2. Zagrożenia cyberbezpieczeństwa w sektorze ochrony zdrowia w Polsce w 2023 r.



Źródło: Opracowanie własne na podstawie danych CERT Polska.

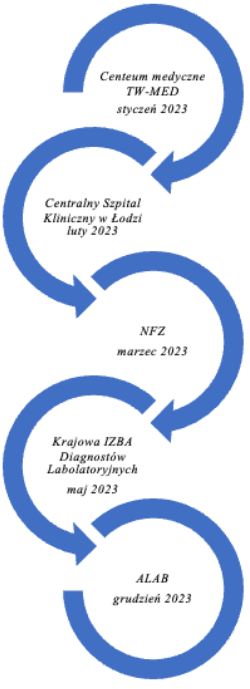
Krajobraz cyberataków na sektor ochrony zdrowia w Polsce

W niniejszej części artykułu, na podstawie przeglądu publikacji o charakterze doniesień medialnych, przedstawiamy incydenty, które w 2023 r. dotknęły infrastrukturę informatyczną polskiego sektora ochrony zdrowia. Zostały one zobrazowane na rysunku 1.

Na początku roku 2023 doszło do ataku hakerskiego na infrastrukturę serwerową Centrum Medycznego TW-MED, w wyniku, którego zaszyfrowane zostały zgromadzone na serwerze dane. Obejmowały one informacje o 50 tys. pacjentów z lat 2018–2023, w tym: imię i nazwisko, numer PESEL, dane kontaktowe, wyniki badań oraz dane dotyczące stanu zdrowia (Centrum Medyczne TW-MED, 2024). Kolejnym atakiem typu *ransomware* był cyberatak na Centralny Szpital

Kliniczny w Łodzi. Dnia 6 lutego 2023 r. pojawiły się problemy z infrastrukturą informatyczną szpitala. Według dyrekcji szpitala nie doszło jednak do wycieku danych pacjentów ani innych informacji wrażliwych. W celu zminimalizowania skutków ataku, zarząd szpitala podjął decyzję o całkowitym wyłączeniu systemów informatycznych szpitala. W konsekwencji cała dokumentacja medyczna była prowadzona w sposób tradycyjny, czyli formie papierowej. Wprowadzenie takich działań zabezpieczających utrudniały także diagnostykę pacjenta, badania obrazowe i laboratoryjne dostępne były jedynie na nośnikach zewnętrznych (Bohyńska, 2023).

Rys. 1. Cele ataków w sektorze ochrony zdrowia w Polsce w 2023 r. (chronologicznie).



Źródło: Opracowanie własne.

Analiza cyberzagrożeń wskazuje fałszywe e-maile jako szczególnie istotny problem dla bezpieczeństwa systemów IT placówek medycznych (NASK, 2023). W marcu 2023 r. na adresy e-mail pracowników sektora ochrony zdrowia w całej Polsce rozsyłane były wiadomości elektroniczne, w których nadawca podszywał się pod Narodowy Fundusz Zdrowia (NFZ), informował o rzekomym wycieku danych z serwerów NFZ. W załączniku wiadomości e-mail, atakujący umieścili

plik z listą owych skradzionych danych. W rzeczywistości e-mail okazał się złośliwym oprogramowaniem typu koń trojański, popularnie nazywany trojanem. NFZ nie odnotowało jednak żadnego wycieku danych (*Ktoś atakuje polskie placówki…*, 2023).

W maju 2023 r. Krajowa Izba Diagnostów Laboratoryjnych (KIDL) jako element niezbędny do stworzenia konta na platformie Izby oraz późniejszego logowania do serwisu żądała od członków ich numeru Prawa Wykonywania Zawodu Diagnosty Labolatoryjnego (PWZDL) oraz numeru PESEL. Numer PWZDL jest powszechnie dostępny na oficjalnej stronie KIDL, natomiast numer PESEL może być pozyskiwany z Krajowego Rejestru Sądowego (KRS) oraz z ksiąg wieczystych. Numer PESEL wymaga szczególnej ochrony, jednak w praktyce często tak nie jest. Przykładem mogą być, np. właściciele firm, czy urzędnicy dysponujący kwalifikowanym podpisem elektronicznym, ponieważ ich numery PESEL są łatwo dostępne w właściwościach podpisu (*Oszuści mogą*, 2021). Oznacza to, że w przypadku nieautoryzowanego dostępu do platformy KIDL, mogło dojść do uzyskania szeregu wrażliwych informacji (Maj, 2023). Opisana sytuacja powinna być przestrogą dla wszystkich organizacji, aby wystrzegać się stosowania numeru PESEL jako danych uwierzytelniających. Numer ten jest powszechnie dostępny i może służyć jako łatwe narzędzie do uzyskania kolejnych danych osobowych.

Przeprowadzony przez grupę hakerką RA World atak, którego celem stała się firma ALAB Laboratoria, zdecydowanie stanowi największy i najbardziej medialny atak odnotowany w 2023 r. W tym przypadku kolejny raz wykorzystano złośliwe oprogramowanie typu *ransomware*. Skradzione pliki zawierały ponad 54 tys. wyników badań oraz dane osobowe, w tym numery PESEL i adresy zamieszkania pacjentów, którzy przeprowadzili badania medyczne w sieci ALAB w latach 2015–2023. Dodatkowo, wyciekły dane pracowników i współpracowników firmy, informacje dotyczące nowych inwestycji, kosztów, faktur, analiz rynkowych oraz zdigitalizowane kopie akt papierowych. Całe archiwum kadrowe stanowiło ponad 27 GB danych (*Hakerzy ujawnili*, 2023). Szczególnie niepokojący jest fakt, że każdy katalog danych został pierwotnie oznaczony czterocyfrową nazwą, będącą początkiem numeru PESEL osoby poszkodowanej. Oznacza to, że w prosty sposób możliwa jest identyfikacja konkretnej osoby w udostępnionej bazie. Co więcej, sposób udostępnia danych pozwala na sprawdzenie informacji dotyczących pojedynczych osób bez konieczności pobierania dużej ilości danych z użyciem sieci TOR (*The Onion Router*).

W odpowiedzi na incydent, firma ALAB podjęła szereg działań mających na celu zminimalizowanie skutków wycieku danych. Pilnie wdrożono procedury bezpieczeństwa oraz komunikacji, aby zlikwidować efekty ataku i ocenić skalę szkód. Firma zgłosiła naruszenie do Prezesa Urzędu Ochrony Danych Osobowych oraz powiadomił odpowiednie instytucje, w tym CERT Polska, Ministerstwo Zdrowia i Centrum E-Zdrowia. Dodatkowo, złożono zawiadomienie o podejrzeniu przestępstwa do Centralnego Biura Zwalczania Cyberprzestępczości. CERT Polska, we współpracy z Centralnym Ośrodkiem Informatyki, udostępnił na stronie bezpiecznedane.gov.pl numery PESEL, które zostały ujawnione przez hakerów z grupy „RA World". Jednocześnie firma uruchomiła procedury audytów bezpieczeństwa danych, zarówno wewnętrznie, jak i zewnętrznie. Ponadto rozpoczęła monitoring sieci, aby zapobiec ewentualnemu upublicznieniu nielegalnie pozyskanych informacji.

Atak na firmę ALAB pokazuje, jak ważne są instytucje państwowe stojące na straży cyberbezpieczeństwa, takie jak NASK (Narodowy Instytut Akseleracji Sieci i Telekomunikacji). Jako Państwowy Instytut Badawczy, który pełni kluczową rolę w zapewnianiu bezpieczeństwa internetu w Polsce, zajmuje się, m.in. reagowaniem na incydenty cybernetyczne przez swoje Centrum Cyberbezpieczeństwa (w tym zespół CERT Polska). Koordynuje ono działania w obszarze ochrony sieci. Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa (Ustawa, 2018), NASK jest jednym z Zespołów Reagowania na Incydenty Komputerowe (CSIRT), a jego działalność obejmuje również obsługę zgłoszeń od operatorów usług kluczowych, dostawców usług cyfrowych, samorządów oraz użytkowników indywidualnych.

W obszarze nauki i innowacji, NASK prowadzi zaawansowane badania dotyczące bezpieczeństwa sieci teleinformatycznych, systemów IoT, a także biometrycznych metod weryfikacji tożsamości. Instytut łączy naukowe podejście do rozwiązywania problemów z praktycznymi potrzebami użytkowników, tworząc innowacyjne technologie w dziedzinach takich jak cyberbezpieczeństwo czy telekomunikacja (NASK, 2023).

Biorąc pod uwagę środki ochronne dla sektora medycznego, należy również wspomnieć o dokumencie pt. „Kodeks postępowania dla sektora ochrony zdrowia", przygotowanym przez Polską Federację Szpitali (przypis). Jest to zbiór zasad mających służyć podnoszeniu poziomu ochrony danych osobowych, zgodnie z RODO i ustawodawstwem krajowym (UODO, b.d.).

Dlaczego sektor ochrony zdrowia jest podatny na ataki hakerskie?

Rosnące wykorzystanie technologii informatycznych oraz związane z nimi sposoby gromadzenia i przetwarzanie danych tworzą kolejne wyzwania dla sektora ochrony zdrowia. Wrażliwe dane, które personel medyczny codziennie przetwarza, czyni go atrakcyjnym celem dla cyberprzestępców (Bentz i in., 2019). Hakerzy często wykorzystują brak świadomości personelu przy pomocy *phishingu*, aby uzyskać nieautoryzowany dostęp do systemów placówek medycznych (Aldawood i Skinner, 2020). Ochrona przed zagrożeniami cybernetycznymi w sektorze zdrowia wymaga uwzględnienia czynników związanych z dobrostanem psychicznym personelu. Pracownicy medyczni, obciążeni stresem mogą mieć obniżoną zdolność do reagowania na potencjalne zagrożenia, takie jak podejrzane e-maile czy próby *phishingu* (Braquehais i Vargas-Cáceres, 2023). Świadomość zagrożeń związanych z *phishingiem* jest tym samym niezbędna w kontekście cyberbezpieczeństwa. Pracownicy powinni być przeszkoleni w zakresie rozpoznawania podejrzanych wiadomości e-mail i linków, aby uniknąć sytuacji, w których poufne informacje zostają wykradzione lub zainstalowane zostaje złośliwe oprogramowanie. Niestety placówki medyczne nie oferują powszechnie szkoleń dla personelu w zakresie bezpiecznych praktyk technologicznych (Branch i in., 2019, s. 2016–2017).

Brak przygotowania do pracy zdalnej uwidocznił się zwłaszcza podczas pandemii COVID-19 (Burke i in., 2024). Szczególnie w tym okresie wysoka presja na sektor skutkowała szybką adaptacją rozwiązań technologicznych bez zapewnienia odpowiednich środków bezpieczeństwa, zwiększając tym samym podatność na incydenty cybernetyczne (Vilakazi i Adebesin, 2023). Jednym z fundamentalnych kroków w zapewnieniu bezpieczeństwa jest stosowanie silnych, unikalnych haseł logowania oraz wdrożenie dwuetapowego uwierzytelniania. Silne hasła są trudniejsze do odgadnięcia i znacznie utrudniają nieautoryzowany dostęp do systemów. Dwuetapowe uwierzytelnianie z kolei wprowadza dodatkową warstwę zabezpieczeń, która wymaga od użytkowników potwierdzenia tożsamości za pomocą drugiego urządzenia lub metody.

Raport Najwyższej Izby Kontroli (NIK) z 2019 r. wykazał, że w wielu placówkach medycznych zaniedbuje się te podstawowe praktyki, co skutkuje m.in. stosowaniem tych samych haseł przez różnych pracowników oraz brakiem wymogu

uwierzytelniania użytkowników podczas logowania do systemów (NIK, 2019). Kolejnym kluczowym elementem jest systematyczna aktualizacja systemów operacyjnych i oprogramowania. Producenci regularnie wydają poprawki, które usuwają wykryte luki bezpieczeństwa. Zaniedbanie tych aktualizacji może narazić placówki na ataki wykorzystujące znane już słabości. NIK wskazuje, że w wielu przypadkach używane są programy, które przestały być wspierane technicznie lub pochodzą z niepewnych źródeł, co stanowi poważne zagrożenie (NIK, 2019).

Należy również podkreślić, że w sektorze ochrony zdrowia problem cyberbezpieczeństwa nie ogranicza się jedynie do aparatury komputerowej. Firma TrapX w swoim raporcie z 2018 r. ujawniła, że zagrożenia dotyczą również sprzętu medycznego. Luki w zabezpieczeniach stwierdzono w przypadku sprzętu rentgenowskiego, systemów archiwizacji obrazów i komunikacji (PACS), w skanerach PET, tomografach komputerowych, rezonansach magnetycznych, a także pompach infuzyjnych, laserach medycznych oraz respiratorach (TrapX Research Labs, 2018).

Podsumowanie

Przedstawione dane i analizy wskazują na istotne wyzwania, z jakimi w zakresie cyberbezpieczeństwa boryka się sektor ochrony zdrowia. Liczba naruszeń z zakresu cyberbezpieczeństwa w sektorze ochrony zdrowia nadal jest znacząca i z roku na rok rośnie. Podkreśla to konieczność podjęcia skutecznych działań mających na celu ochronę integralności, dostępności i poufności danych medycznych. Niezwykle ważna jest edukacja kadry medycznej w zakresie cyberbezpieczeństwa. Nowoczesne strategie bezpieczeństwa winny być priorytetem dla zapewnienia ochrony danych pacjentów i pracowników sytemu ochrony zdrowia w cyberprzestrzeni, a współpraca pomiędzy instytucjami medycznymi, organami regulacyjnymi i ekspertami ds. cyberbezpieczeństwa wydaje się być w realizacji tego celu kluczowa.

Bibliografia

ALAB laboratoria. (2023, 27 listopada). *Komunikat: incydent naruszenia bezpieczeństwa danych osobowych.* https://www.alablaboratoria.pl/19811-komunikat-incydent-naruszenia-bezpieczenstwa-danych-osobowych

Aldawood, H., & Skinner, G. (2020). Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools, and Solutions. *IEEE Access*, *8*, pp. 67321-67329. https://doi.org/10.1109/ACCESS.2020.2983280

Bentz, L., Pirard, P., Motreff, Y., Vandentorren, S., Baubet, T., Fabre, R., Touboul Lundgren, P., & Pradier, C. (2019). Health outcomes of the July 14, 2016 Nice terror attack among hospital-based professionals and students: the «ECHOS de Nice» health survey protocol. *BMC Public Health*, *19*(1), 1163. https://doi.org/10.1186/s12889-019-7489-3

Bochyńska, N. (2023, 9 lutego). *Cyberatak na Centralny Szpital Kliniczny w Łodzi [AKTUALIZACJA].* https://cyberdefence24.pl/cyberbezpieczenstwo/cyberatak-na-centralny-szpital-kliniczny-w-lodzi-aktualizacja

Branch, L., Eller, W., Bias, T., Mccawley, M., Myers, D., Gerber, B., & Bassler, J. (2019). Trends in Malware Attacks against United States Healthcare Organizations, 2016-2017. *Global Biosecurity*, *1*, 15. https://doi.org/10.31646/gbio.7

Braquehais, M. D., & Vargas-Cáceres, S. (2023). Psychiatric Issues Among Health Professionals. *The Medical Clinics of North America*, *107*(1), 131–142. https://doi.org/10.1016/j.mcna.2022.04.004

Burke, W., Stranieri, A., Oseni, T., & Gondal, I. (2024). The need for cybersecurity self-evaluation in healthcare. *BMC Medical Informatics and Decision Making*, *24*(1), 133. https://doi.org/10.1186/s12911-024-02551-x

Centrum Medyczne TW-MED. (2024, 8 kwietnia). *Komunikat o naruszeniu ochrony danych osobowych w Centrum Medycznym TW-MED.* http://www.tw-med.pl/?page_id=717

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008

Croke, L. (2020). Protecting your organization from e-mail phishing and ransomware attacks. *AORN Journal*, *112*(4), P10–P12. https://doi.org/10.1002/aorn.13229

Diaz, N. (2022, 21 stycznia). 50% of internet-connected hospital devices vulnerable to cyberattacks. Direct line between hospital cyberattacks and patient mortality, report shows. *The Becker's Hospital Review.* https://www.beckershospitalreview.com/cybersecurity/50-of-internet-connected-hospital-devices-vulnerable-to-cyberattacks.html

Evans, M. (2018, 12 marca). Why Data Is The Most Important Currency Used In Commerce Today. *Forbes.* https://www.forbes.com/sites/michelleevans1/2018/03/12/why-data-is-the-most-important-currency-used-in-commerce-today/

Guziak, M., & Bastrzyk, Z. (2023). Sektor ochrony zdrowia w obliczu konfliktu zbrojnego. *Rocznik Bezpieczeństwa Międzynarodowego*, *17*(1), 33–50. https://doi.org/10.34862/rbm.2023.1.3

Hakerzy ujawnili kolejną część danych wykradzionych z ALAB Laboratoria – sprawdź czy Twoje dane zostały upublicznione. (2023, 12 grudnia). Baza wiedzy. Pobrano 1 marzec 2024, z https://www.gov.pl/web/baza-wiedzy/hakerzy-ujawnili-kolejna-czesc-danych-wykradzionych-z-alab-laboratoria--sprawdz-czy-twoje-dane-zostaly-upublicznione

HealthIT.gov. (b. d.). *Electronic Health Record (EHR).The Basics.* https://www.healthit.gov/faq/what-information-does-electronic-health-record-ehr-contain

HealthIT.gov. (2019, 10 sierpnia). *What Are Electronic Health Record (EHR)?* https://www.healthit.gov/faq/what-electronic-health-record-ehr

IBM Security. (2024). *Cost of a Data Breach Report 2023*. Pobrano 1 marzec 2024, z https://tiny.pl/53jpyr42

Instytut. (b.d.). Pobrano 22 grudzień 2024, z https://nask.pl/instytut/

Ktoś atakuje polskie placówki ochrony zdrowia "na wyciek z NFZ". (2023, 20 marca). NieBezpiecznik.pl. https://niebezpiecznik.pl/post/ktos-atakuje-polskie-placowki-ochrony-zdrowia-na-wyciek-z-nfz/

Kuneva, M. (2009, 31 marca). *Meglena Kuneva - European Consumer Commissioner - Keynote Speech - Roundtable on Online Data Collection, Targeting and Profiling.* [Tekst]. European Commission. Pobrano 15 marzec 2024, z https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156

Lella, I., Ciobanu, C., Tsekmezoglou, E., Theocharidou, M., Magonara, E., Malatras, A., & Svetozarov Naydenov, R. (Eds.) (2023). *ENISA threat landscape 2023: July 2022 to June 2023.* European Union Agency for Cybersecurity. Publications Office of the EU. https://data.europa.eu/doi/10.2824/782573

Maj, M. (2023, 12 czerwca). Jak można było podejrzeć dane osobowe diagnostów? I dlaczego PESEL to zawsze kiepskie hasło…. *NieBezpiecznik.pl.* https://niebezpiecznik.pl/post/logowanie-po-peselu-to-zlo-jak-izba-diagnostow-zespula-proces-aktualizacji-danych/

Makuch, J., & Guziak, M. (2020). Cyberbezpieczeństwo sektora ochrony zdrowia. Przypadek Polski na tle tendencji światowych. *Rocznik Bezpieczeństwa Międzynarodowego*, *14*(2), 86–102. https://doi.org/10.34862/rbm.2020.2.6

Miliard, M. (2022, wrzesień 9). Direct line between hospital cyberattacks and patient mortality, report shows. *Healthcare IT News.* https://www.healthcareitnews.com/news/direct-line-between-hospital-cyberattacks-and-patient-mortality-report-shows

Milieu Ltd. (2014, 23 lipca). *Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services. Final report and recommendations*. https://health.ec.europa.eu/document/download/3eb04ec0-b-1c3-4e01-8ffb-46765744c049_en?filename=laws_report_recommendations_en.pdf

Ministerstwo Zdrowia. (2022, 26 października). *Ponad 260 mln zł z Ministerstwa Zdrowia na cyberbezpieczeństwo w szpitalach*. https://www.gov.pl/web/zdrowie/ponad-260-mln-zl-z-ministerstwa-zdrowia-na-cyberbezpieczenstwo-w-szpitalach

Najwyższa Izba Kontroli [NIK]. (2019). *Wdrożenie przez podmioty lecznicze regulacji dotyczących ochrony danych osobowych.* Informacja o wynikach kontroli (P/19/063). https://bip.nik.gov.pl/kontrole/P/19/063/

Nancy, M., & Maheswari, R. (2020). A Review on Unstructured Data in Medical Data. *Journal of Critical Reviews,* 7(13), 2202-2208.

Narodowe Standardy Cyberbezpieczeństwa [NSC]. (b.d.). Baza wiedzy. Pobrano 1 marzec 2024, z https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber

NASK. (2023, 5 czerwca). *Raport roczny z działalności CERT Polska 2022*. https://nask.pl/magazyn/raport-roczny-z-dzialalnosci-cert-polska-w-2022-roku/

OECD. (1980/2013). *OECD Privacy Guidelines* (OECD/LEGAL/0188). Pobrano 15 marzec 2024, z https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm

Oszuści mogą zdobyć PESEL legalnie. (2021, 6 kwietnia). https://www.ey.com/pl_pl/serwis-audytorow-sledczych/2021/03/oszusci-moga-zdobyc-pesel-legalnie

Otwarte Dane. (2024, 3 stycznia). *Statystyki obsłużonych incydentów przez zespół CERT Polska – 01.01.2023-28.12.2023.* https://dane.gov.pl/pl/dataset/1992/resource/53602,statystyki-obsuzonych-incydentow-przez-zespo-cert-polska-01012023-28122023/table

Reddix-Smalls, B. (2012). Credit Scoring and Trade Secrecy: An Algorithmic Quagmire or How the Lack of Transparency in Complex Financial Models Scuttled the Finance Market. *Business Law Journal*, *12*. https://blj.ucdavis.edu/archives/12/1/credit-scoring-and-trade-secrecy-algorithmic-quagmire-or-how-lack-transparency

Rozporządzenie. (2016). *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*. Dz. U. UE L 119/1 z 4.5.2016. http://data.europa.eu/eli/reg/2016/679/oj

Rozporządzenie. (2020). Rozporządzenie z 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania. Dz. U. 2020, poz. 666 ze zm. https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20200000666

Solecka, M. (2023, 23 lutego). Uchodźcy w systemie czy poza nim? *Medycyna Praktyczna*. http://www.mp.pl/social/article/317681

TrapX Research Labs. (2018). *MEDJACK.4 Medical Device Hijacking*. https://www.trustdimension.com/wp-content/uploads/2015/02/MedJack.4-ilovepdf-compressed.pdf

UODO. (b.d.). *Zatwierdzone kodeksy postępowania*. Urząd Ochrony Danych Osobowych. Pobrano 22 grudzień 2024, z https://uodo.gov.pl/pl/426/1110

Ustawa. (2011). *Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej*. Dz. U. 2011, nr 112, poz. 654 ze zm. https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20111120654

Ustawa. (2018). *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,* Dz. U. 2018, poz. 1560 ze zm. https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560

Vilakazi, K., & Adebesin, F. (2023, 26 maja). *A systematic literature review on cybersecurity threats to healthcare data and mitigation strategies*. https://doi.org/10.29007/hf15