KWARTALNIK NAUK O PRZEDSIĘBIORSTWIE

4/2024

**dr hab. Małgorzata Poniatowska-Jaksch, prof. SGH**
Szkoła Główna Handlowa w Warszawie
Kolegium Nauk o Przedsiębiorstwie
Instytut Rynków i Konkurencji
e-mail: mponia@sgh.waw.pl
ORCID: 0000-0001-5737-655X

# Ransomware w sektorze ochrony zdrowia – przyczyny, konsekwencje

## Ransomware in the healthcare sector – causes, consequences

**Słowa kluczowe:**
ransomware, platforma, sektor ochrony zdrowia, gospodarka cyfrowa

**Streszczenie:** Wraz z rozwojem gospodarki cyfrowej rośnie zagrożenie ze strony cyberprzestępczości. Szczególnie niebezpieczny jest atak złośliwym oprogramowaniem ransomware w modelu platformy cyfrowej – RaaS, w którym dostęp do usługi (wirusa lub wykradzionych danych) jest relatywnie łatwy, tani i nie wymaga specjalistycznej wiedzy. Zagrożenie atakiem ransomware nie omija także sektora ochrony zdrowia, w którym wskaźnik przeprowadzonych ataków, na tle innych sektorów, jest wysoki i wykazuje tendencję rosnącą. Celem artykułu jest identyfikacja, na podstawie raportów organizacji wyspecjalizowanych w zapewnieniu cyberbezpieczeństwa, przyczyn i konsekwencji tego ataku. Przyczyny to przede wszystkim bardzo duża liczba wrażliwych danych przechowywanych przez sektor ochrony zdrowia oraz niski poziom ich zabezpieczenia. Konsekwencje zaś mają wymiar finansowy (koszty usuwania ataku prawie w połowie pokrywają podmioty ochrony zdrowia) oraz społeczny – od utraty tożsamości pacjentów po błędy w sztuce medycznej z powodu utraty dokumentacji. W sytuacji wysokiego zagrożenia wyzwaniem staje się podniesienie cyberbezpieczeństwa sektora ochrony zdrowia, co jednak nie powinno dziać się kosztem społecznym, czyli spadkiem nakładów na ochronę zdrowia *sensu stricto*.

**Keywords:**
ransomware, platform, healthcare sector, digital economy

**Abstract:** The development of the digital economy has been accompanied by a growing threat of cybercrime. Particularly dangerous is the ransomware attack model utilising a digital platform – Ransomware as a Service (RaaS), where access to the service (malware or stolen data) is relatively easy, inexpensive, and does not require specialised knowledge. The ransomware threat also extends to the healthcare sector, where the rate of such attacks is high compared to other sectors

and continues to rise. This article aims to identify the causes and consequences of ransomware attacks in the healthcare sector, based on reports from organisations specialising in cybersecurity. The primary causes include the vast amount of sensitive data stored by the healthcare sector and the low level of data protection. The consequences are both financial (nearly half of the attack mitigation costs are borne by healthcare entities) and social – ranging from patient identity theft to medical malpractice due to the loss of documentation. In the face of this significant threat, the challenge lies in enhancing the cybersecurity of the healthcare sector without incurring social costs, such as a reduction in funding for core healthcare services.

**JEL:**
E26, I18, O17

## Wprowadzenie

W drugiej dekadzie XXI w. gospodarka cyfrowa dotyka każdego aspektu życia człowieka, nie omija też rozwoju cyberprzestępczości. Ta ostatnia wspomagana cyfrowymi technologiami jak: chmury obliczeniowe, algorytmy sztucznej inteligencji, blockchain czy też bitcoin funkcjonuje na cyfrowych platformach, zgodnie z zasadami e-modeli biznesu. Jednym z większych zagrożeń dla cyfrowego bezpieczeństwa jawi się ransomware [ENISA, 2022, s. 6]. Jest to program blokujący lub szyfrujący dostęp do plików znajdujących się na urządzeniu w celu wyłudzenia okupu. Płatności zazwyczaj żąda się za pośrednictwem anonimowej strony internetowej, zwykle w kryptowalucie. Określenie skali zjawiska jest bardzo trudne, gdyż znaczna większość organizacji, chroniąc reputację, nigdzie tego faktu nie zgłasza [ENISA, 2022, s. 3]. Niemniej jednak dane szacunkowe wskazują na wzrost zagrożenia w tym zakresie, zwłaszcza w sektorze ochrony zdrowia. Dane medyczne są od dziesięciu do dwudziestu razy cenniejsze niż dane kart kredytowych czy informacje bankowe, co sprawia, że opieka zdrowotna jest atrakcyjnym celem ataku dla cyberprzestępców [Market Research Future, 2024].

Stąd też celem artykułu jest identyfikacja przyczyn i konsekwencji ataków ransomware w sektorze ochrony zdrowia. Podstawą analizy są informacje i dane udostępniane przez organizacje wyspecjalizowane w ich ochronie w sieci jak: ENISA – agencja UE odpowiedzialna za zapewnienie wysokiego i efektywnego poziomu bezpieczeństwa w sieciach i systemach informatycznych UE, Sophos – brytyjskie przedsiębiorstwo informatyczne specjalizujące się w programach odpowiadających za bezpieczeństwo w sieci oraz Office of Information Security USA.

## Efekty sieciowe i ekosystem RaaS

W 2024 r. operatorzy oprogramowania ransomware to cyberprzestępcy coraz częściej korzystający w miejsce własnego programu z usług dostępnych w dark webie [eSentire, 2023]. Jedną z bardziej niebezpiecznych form tego oprogramowania jest RaaS (Ransomware as a Service). RaaS jest to technologiczna platforma (rodzaj sytemu informatycznego), na bazie której możliwe jest tworzenie i rozwój portfeli produktów oraz usług [Cusumano, 2012, s. 36]. RaaS to także zbiór zasobów cyfrowych, umożliwiający użytkownikom wykonywanie zadań i wchodzenie w różnego typu interakcje z innymi użytkownikami [Bonina i in., 2021, s. 869–902]. Tak postrzegane platformy cyfrowe tworzą wartość nie poprzez działania o charakterze liniowym – od nakładów do wyników, czyli tworząc tradycyjny łańcuch kreacji wartości, ale poprzez sieć wartości łącząc za pośrednictwem platformy cyfrowej różne strony rynku ukierunkowane na świadczenia usług [Täuscher, Laudien, 2018, s. 319–320]. Z perspektywy ekonomicznej jedną stroną RaaS tworzą dostawcy aktywów – operatorzy RaaS, z drugiej zaś konsumenci aktywów, czyli podmioty zaangażowane we wdrażanie złośliwego oprogramowania za pośrednictwem platformy cyfrowej. W modelu RaaS, tak jak we wszystkich innych platformach cyfrowych, kluczową rolę w rozwoju odgrywają efekty sieciowe [Hernandez-Castro i in., 2017, s. 1–14; Trischler i in., 2021]. Te ostatnie dzielimy na bezpośrednie i pośrednie. W pierwszym przypadku wynikają one ze wzrostu końcowej użyteczności dobra, a w drugim zaś ze wzrostu liczby podmiotów korzystających z usług świadczonych przez platformę. W przypadku RaaS w efekty bezpośrednie wpisuje się m.in. coraz bardziej kompleksowa usługa. RaaS zapewnia usługobiorcom już nie tylko sam kod dostępu i program – wirus, ale także monitoring przebiegu ataku, raporty zwierające obliczenia i prognozy rachunku zysków i strat itp. [Feilner, 2021]. Z kolei za efekty pośrednie w coraz większym stopniu odpowiedzialni są tzw. brokerzy. Brokerzy „dostępu" włamują się do sieci, w celu pozyskania kodu źródłowego złośliwego oprogramowania, który następnie sprzedają partnerom/operatorom. Ci z kolei mogą je dalej sprzedawać podmiotom stowarzyszonym, które uiszczają opłatę na rzecz operatorów ransomware. W RaaS spotykane są cztery modele przychodów: miesięczna subskrypcja, programy partnerskie – miesięczna stała opłata, której wysokość kalkulowana jest jako procent od zysków (najczęściej 20–30%), jednorazowa opłata licencyjna i procent od zysków [OIS, 2024, s. 11]. Warto w tym miejscu zaznaczyć, że ostatnio często spotykanym dodatkowym źródłem dochodu jest sprzedaż wykradzionych informacji podmiotom, które zaoferują najwyższą cenę. Jest to tzw. data brokering, który obejmuje także odsprzedaż uzyskanego dostępu do danych innym zainteresowanym w celu ich dodatkowego wykorzystania [ENISA, 2022, s. 16–18]. Jest to możliwe, gdyż korzystający z oprogramowania ransomware mają dostęp do licznych danych pochodzących od poprzednich ofiar, w tym także na temat ich „podatności" na zapłacenia okupu.

RaaS jest więc klasycznym rynkiem dwustronnym, którego celem jest zrównoważenie efektów sieciowych obu stron, tak aby byłe one korzystne dla wszystkich jego uczestników. Z teoretycznego punktu widzenia nie ma jednego uniwersalnego rozwiązania prowadzącego do generowania zrównoważonych efektów sieciowych. Każdy biznes oparty na efektach sieciowych charakteryzuje się odmiennym modelem biznesowym, własnymi odbiorcami, ekosystemem itp. [Bartels, Schmitt, 2022, s. 2–3]. W modelu RaaS głównym celem jest maksymalizacja zysku, a nie wzrost liczby podmiotów płacących okup [Hernandez-Castro i in., 2020, s. 12].

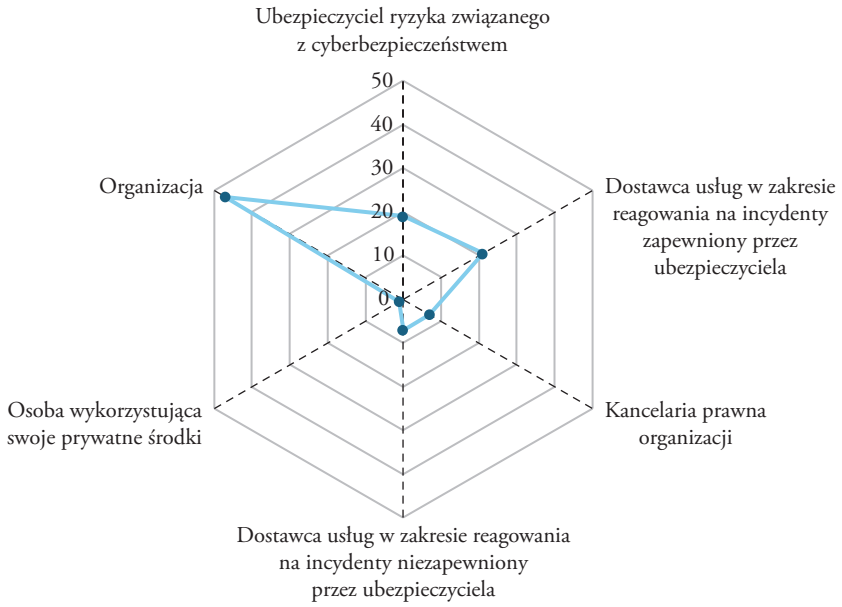
Platformy, wchodząc w interakcje z uczestnikami rynku, tworzą ekosystem biznesu [Ceccagnoli i in., 2011, s. 263–290]. Poza zbiorem podmiotów bezpośrednio zaangażowanych we wdrażanie oprogramowania ransomware (rdzeń platformy), szerszy ekosystem obejmuje dalszych graczy po stronie ofiary (peryferia platformy), które mogą czerpać zyski z ataków ransomware. Należą do nich [Clancy, 2021]:

a) firmy zajmujące się pomocom ofiarom ataku w zakresie reagowania na incydenty,
b) brokerzy oprogramowania ransomware, których działania obejmują m.in. negocjacje czy obsługę płatności w imieniu ofiary,
c) specjaliści ds. reagowania na tego rodzaju incydenty, w tym zarówno zewnętrzni, jak i zatrudnieni przez ubezpieczyciela cybernetycznego organizacji dotkniętej atakiem,
d) ubezpieczyciele,
e) prawnicy,
f) prywatne osoby/firmy, które udostępniają swoje zasoby finansowe, aby pomóc ofierze ataku w zapłaceniu okupu.

W przypadku sektora ochrony zdrowia głównym źródłem finansowania okupu jest sama organizacja, pokrywająca średnio niemal połowę (46%) płatności, spółka macierzysta organizacji i/lub organ zarządzający zazwyczaj zapewnia 18%, a 19% całkowitego finansowania płatności okupu pochodzi od dostawców ubezpieczeń lub za pośrednictwem wyznaczonego przez niego specjalisty ds. reagowania na incydenty (21%) (zob. rysunek 1).

W latach 20. XXI w. w sektorze zdrowia do najgroźniejszych grup RaaS należały [Hutchinson, 2024]: LockBi, BlackCat, znany również jako ALPHV lub Noberus oraz w nieco mniejszym stopniu Cl0p. Jednakże upadek dwóch pierwszych w 2024 r. [Coker, 2024], którzy odpowiadali łącznie za ponad 30% wszystkich zgłoszonych ataków przeprowadzonych na sektor ochrony zdrowia na całym świecie [OIS, 2024, s. 18] sprawił, że model RaaS i jego ekosystem ewoluuje. Wyraża się to przede wszystkim wzrostem liczby przemieszczeń partnerów oprogramowania pomiędzy różnymi operatorami RaaS, a tym samym zacieraniem się granic pomiędzy ich ekosystemami. Oznacza to, że ugrupowania ransomware są ze sobą luźno powiązane, a odpowiedzialność za przeprowadzenie ataku „rozmywa się".

**Rysunek 1. Transakcja okupu w sektorze ochrony zdrowia wg podmiotu dokonującego płatności**




Źródło: opracowanie własne na podstawie [Sophos, 2024, s. 13].

## Ataki ransomware w sektorze ochrony zdrowia

Ransomware od lat jest obecny w sektorze zdrowia. I tak pierwszy w historii wirus ransomware został stworzony w 1989 r. na Harvardzie przez Josepha L. Poppa nazywanego „ojcem oprogramowania ransomware", który rozesłał 20 tys. zainfekowanych dyskietek z napisem „AIDS Information – Introductory Diskettes" do uczestników międzynarodowej konferencji Światowej Organizacji Zdrowia na temat AIDS w Sztokholmie. Dyski zawierały złośliwy kod, który ukrywał katalogi plików, blokował ich nazwy, a w zamian za ich odzyskanie Autor zażądał od ofiar po 189 USD. Od tamtego czasu ransomware znacznie ewaluował, a przełomowym rokiem dla jego rozwoju było pojawienie się w 2008 r. bitcoina. Zdecentralizowana kryptowaluta zapewniła nowy, w większości anonimowy system przesyłania pieniędzy [Laszka i in., 2017, s. 2; OIS, 2024, s. 5–10].

Zagrożenie ransomware w sektorze ochrony zdrowia wzrosło w czasach pandemii COVID-19, czego wyrazem były przeprowadzane ataki na szpitale i laboratoria badawcze prowadzące prace nad szczepionką. W warunkach poczucia zagrożenia społecznego oraz przejścia na pracę „zdalną" przy użyciu słabo zabezpieczonych przez pracodawców informatycznych systemów domowych, skutecznymi technikami wykorzystywanymi

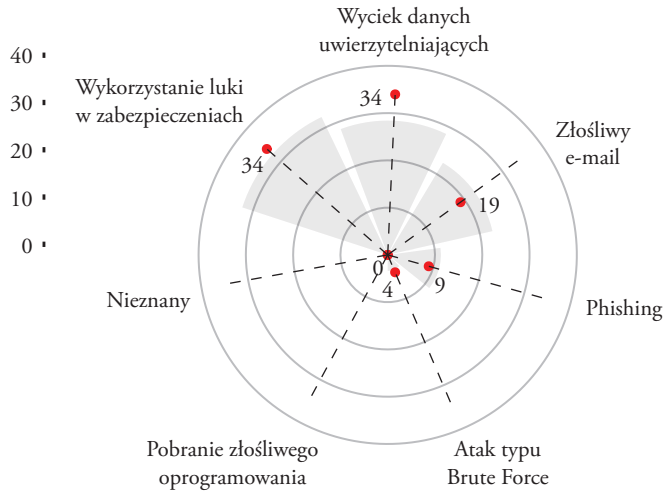
przez cyberprzestępców było podszywanie się pod Światową Organizację Zdrowia oraz Organizację Narodów Zjednoczonych. Wykorzystując programy komputerowe dedykowane pracy „na odległość" starano się nakłonić użytkowników do kliknięcia linków lub otwarcia zainfekowanych dokumentów. Dużymi ujawnionymi atakami ransomware zostały dotknięte Szpital Uniwersytecki w Brnie i Uniwersytet Kalifornijski w San Francisco, w których były prowadzone badania nad szczepionką przeciwko COVID-19. Z kolei grupa ransomware Maze opublikowała dane osobowe i medyczne tysięcy byłych pacjentów londyńskiej firmy, która przeprowadza testy na COVID-19. Natomiast w Kanadzie CryCryptor podszywał się pod aplikacje na urządzeniach z systemem Android, dedykowane śledzeniu kontaktów chorych na COVID-19 [Pranggono, Arabo, 2020, s. 5].

Po zakończeniu pandemii atrakcyjność sektora dla cyberprzestępców nie spadła. Organizacje opieki zdrowotnej przechowują bowiem cenne dane osobowe i informacje o stanie zdrowia swoich pacjentów. Elektroniczne rejestry dokumentacji medycznej zawierają dane, które są cennym „towarem" w dark webie od nazwisk, dat urodzenia i informacji o stanie zdrowia po numery ubezpieczenia społecznego, dane rozliczeniowe i ubezpieczeniowe. Szacuje się, że ponad 20% poufnych danych przechowywanych przez typowy podmiot opieki zdrowotnej jest zagrożonych atakiem ransomware, w porównaniu ze średnią wynoszącą 6% w innych sektorach gospodarczych [Olsen, 2024].

Wskaźnik ataków ransomware w opiece zdrowotnej wykazuje tendencję wzrostową. Na podstawie badań przeprowadzonych w 2024 r. przez Sophos szacuje się, że 67% organizacji opieki zdrowotnej zostało dotkniętych atakiem ransomware – dwukrotnie wyższy poziom niż w 2021 r. (34% zgłoszeń z zakresu cyberbezpieczeństwa wśród 5 tys. firm z 14 krajów, w tym 402 respondentów z sektora ochrony zdrowia). Warto zaznaczyć, że na tle innych sektorów gospodarczych, sektor ochrony zdrowia wyróżniał się w 2024 r. wysokim wskaźnikiem ataków ransomware, osiągając wraz sektorem energetycznym drugą lokatę pod tym względem wśród badanych sektorów, a wyższy poziom był typowy jedynie dla sektora organizacji rządowych (68%).

W 2024 r. najczęściej w atakach ransomware w ochronie zdrowia, podobnie jak w innych sektorach, wykorzystano: 1) luki w zabezpieczeniach, 2) „wyciek" danych uwierzytelniających (po ok. 34%), 3) złośliwe e-maile (19% ataków) (zob. rysunek 2). Te dwie pierwsze metody należały przeciętnie do najczęściej występujących na świecie przyczyn ataków ransomware (odpowiednio 32% i 29% ogółu). Co więcej, w 2024 r. sektor ochrony zdrowia odnotował jeden z najwyższych wskaźników naruszeń kopii zapasowych (95% podmiot opieki zdrowotnej, tj. nieznacznie powyżej średniej światowej wynoszącej 94%). Dwie trzecie prób naruszenia kopii w ochronie zdrowia okazało się skutecznymi, wyższe wskaźniki były charakterystyczne jedynie dla sektorów: energetycznego (79%) i edukacyjnego (71%).

**Rysunek 2. Podstawowa przyczyna ataku w sektorze zdrowia na tle pozostałych sektorów gospodarki w 2024 r.**




Źródło: opracowanie własne na podstawie [Sophos, 2024, s. 21].

Według badania Sophos niemal ¾ ataków ransomware w ochronie zdrowia w 2024 r., tj. powyżej średniej dla wszystkich sektorów (ok. 70%) skutkowało szyfrowaniem danych, co jest niemal identyczne ze wskaźnikiem szyfrowania zgłoszonym w 2023 r. Szyfrowaniu danych towarzyszyła ich kradzież (w 2024 r. 22% przypadków), w której przypadku odnotowano spadek w stosunku do 2023 r. (37% odnotowanych incydentów). Kradzież zwiększa na ogół zdolność atakujących do wyłudzania pieniędzy od swoich ofiar, a także umożliwia ich odsprzedaż w dark webie.

Chociaż 98% podmiotów opieki zdrowotnej odzyskało zaszyfrowane dane, to dokonywały tego w różny sposób, przy czym ponad połowa z nich zgłosiła korzystanie z więcej niż jednej metody, co stanowi trzykrotność tego wskaźnika zgłoszonego w 2023 r. I tak 73% przywróciło zaszyfrowane dane przy użyciu kopii zapasowych, 53% zapłaciło okup, a 29% skorzystało z innych środków, w tym m.in. poprzez współpracę z organami ścigania lub użycie kluczy deszyfrujących, które zostały już upublicznione. Dla porównania, przeciętnie na świecie w 68% użyto kopii zapasowych, a w 56% zapłacono okup [Sophos, 2024, s. 9].

Odpowiedzią na rosnące zagrożenie ransomware staje się zaangażowanie organów ścigania i instytucji rządowych w ich ograniczanie. Chociaż charakter i dostępność oficjalnego wsparcia w przypadku ataku ransomware różnią się w zależności od kraju, podobnie jak narzędzia do zgłaszania cyberataków, to niemal wszystkie zaatakowane przez ransomware podmioty opieki zdrowotnej, nawiązały z tego powodu kontakt z odpowiednimi organami państwowymi, a 76% z nich uznały ten kontakt za łatwy.

Niemal 61% podmiotów otrzymało porady dotyczące radzenia sobie z atakiem, 59% otrzymało pomoc w jego rozpoznaniu, a 41% otrzymało pomoc w odzyskaniu zaszyfrowanych podczas ataku danych.

## Przyczyny i konsekwencje

Przyczyny dużej aktywności cyberprzestępców w sektorze ochrony zdrowia są zróżnicowane i można je podzielić na cztery podstawowe grupy:

1. Wartość danych (jakościowa i ilościowa) przechowywanych w systemach opieki zdrowotnej. Dane nt. naszego stanu zdrowia są „bezcenne" i otrzymujemy je raz na całe życie. Co więcej, sektor zdrowia posiada bardzo dużą liczbę poufnych informacji na nasz temat. Szacuje się, że średniorocznie jest to 42 mln rekordów danych wrażliwych w porównaniu ze średnią światową wynoszącą 28 mln rekordów. Przewiduje się, że przepaść między sektorami w tym zakresie będzie wzrastać, gdyż organizacje opieki zdrowotnej gromadzą wrażliwe dane w szybszym tempie niż inne organizacje [Olsen, 2024].
2. Powszechne stosowanie starszych technologii niż w innych sektorach gospodarczych, a zwłaszcza w biznesie. Wiele placówek medycznych działa na przestarzałych urządzeniach, często z nieaktualnymi wersjami oprogramowania, bez odpowiednich środków bezpieczeństwa. Naruszenie pojedynczego starszego urządzenia/systemu może służyć jako „brama" dająca dostęp do danych wielu jednostek medycznych działających w szerszym systemie powiązań. Hakerzy coraz częściej obierają sobie za cel konkretny sprzęt medyczny lub inne urządzenia (np. drukarki) funkcjonujące w sieci poprzez wi-fi podmiotu ochrony zdrowia. Ryzyko wystąpienia takiego zdarzenia jest wysokie, ponieważ starsze systemy często nie są obsługiwane przez ich pierwotnych programistów, a tym samym często podmioty opieki zdrowotnej nie mają aktualnych zabezpieczeń [Hutchinson, 2024]. Jak już wspomniano, wg badań Spohos, ponad jedna trzecia (34%) ataków w tym sektorze zaczyna się właśnie od wykorzystania luk w zabezpieczeniach.
3. Elektroniczne systemy dokumentacji medycznej nie zostały zaplanowane z myślą o zagrożeniu cyberatakiem. Nowoczesne urządzenia medyczne, często działające w sieci, są bardzo korzystne dla sektora ochrony zdrowia, ale mają również wbudowane luki w zabezpieczeniach, których znajomości trudno oczekiwać od personelu medycznego. Cyfrowe przechowywanie danych umożliwia organizacjom opieki zdrowotnej szybką wymianę ważnych informacji między personelem, w tym ponad granicami krajowymi, co ułatwia szybszą, bardziej kompleksową i fachową opiekę nad pacjentem, ale wiąże się również z ryzykiem kradzieży informacji o pacjencie.

4. Outsourcing obsługi IT w sektorze zdrowia. Badania przeprowadzone w grupie przedsiębiorstw wykazały, że firmy, które zlecają jednostkom zewnętrznym obsługę IT, w tym też w zakresie zapewnienia bezpieczeństwa, są bardziej narażone na cyberatak. Wyniki tłumaczy się czynnikami behawioralnymi u podstaw, w których znajduje się „przeświadczenie", że płacenie za bezpieczeństwo w sieci niejako zwalnia nas z nadmiernej ostrożności i przewidywaniu niechcianych zdarzeń [Bekkers i in., 2023]. Z dużym prawdopodobieństwem można przyjąć, że z podobną sytuacją mamy do czynienia w publicznych jednostkach służby zdrowia, w których personel medyczny w jeszcze większym stopniu niż prywatni przedsiębiorcy, nie wiąże swoich obowiązków z zachowaniem wysokich standardów w zakresie cyberbezpieczeństwa.

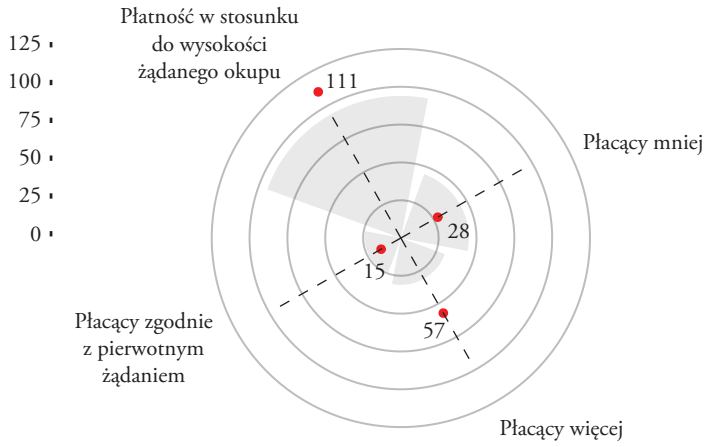
Rosnące zagrożenie atakami ransomware w sektorze ochrony zdrowia sprawia, że w raportach nt. cyberbezpieczeństwa podnoszony jest problem wynikających z tego tytułu konsekwencji. Najczęściej zwraca się uwagę na następujące kwestie [Thamer, Alubady, 2021, s. 215]:

a) straty finansowe,
b) utratę prywatności dokumentacji medycznej, a pośrednio ryzyko utraty tożsamości,
c) możliwość popełnienia błędu w sztuce lekarskiej spowodowanego brakiem wiarygodnej dokumentacji medycznej,
d) utratę zaufania i reputacji dla służby zdrowia.

Wiele z powyższych konsekwencji ma charakter niewymierny lub bardzo trudny do oszacowania. Stosunkowo najłatwiejsze do wykazania są straty finansowe, które można pośrednio wykazać poprzez nakłady podniesione na odzyskanie danych. Wysokie żądania okupu były charakterystyczne dla wszystkich sektorów, lecz średni poziom dla podmiotów ochrony zdrowia w 2024 r. wyniósł 4,9 mln USD, co stanowiło drugą najwyższą kwotę po sektorze organizacji rządowych (9,8 mln USD). Jednocześnie 65% żądań okupu w podmiotach opieki zdrowotnej obejmowało kwotę 1 mln USD lub wyższą, a 35% żądań kwotę 5 mln USD lub wyższą. Według badań Sophos [2024, s. 10] wyższe straty z tego tytułu odnotowały zwłaszcza podmioty, których kopie zapasowe zostały naruszone. Co więcej, w ich przypadku wiązało się to z wyższym poziomem żądanego okupu (średnio ponad trzy razy wyższym niż w przypadku tych, których kopie zapasowe nie zostały naruszone), większą skłonnością (ponad dwukrotnie) do zapłaty okupu, aby odzyskać zaszyfrowane dane (63% w porównaniu z 27%) i wyższymi całkowitymi kosztami ich odzyskiwania (dwukrotnie wyższa niż w przypadku tych, których kopie zapasowe nie zostały naruszone, tj. 750 tys. USD w porównaniu z 375 tys. USD).

Ochrona zdrowia, podobnie jak inne sektory o znaczącym udziale sektora publicznego, należy do grona sektorów o wysokim prawdopodobieństwie zapłaty wyższego okupu w stosunku do pierwotnego żądania, które odpowiednio wyniosło 4,4 mln USD w sektorze zdrowia wobec 6,6 mln USD w sektorach rządowych). Około 57% podmiotów opieki zdrowotnej zapłaciło więcej niż wynosiło początkowe żądanie okupu (zob. rysunek 3).

**Rysunek 3. Płatność okupu w stosunku do pierwotnego żądania według sektorów w 2024 r. (w %)**




Źródło: opracowanie własne na podstawie [Sophos, 2024, s. 26].

Płatności okupu to tylko jeden z elementów kosztów odzyskiwania danych w przypadku zdarzeń związanych z oprogramowaniem ransomware. Wyłączając wszelkie zapłacone okupy, w 2024 r. podmioty opieki zdrowotnej zgłosiły średni koszt odzyskiwania danych po ataku ransomware na poziomie 2,57 mln USD, co stanowi wzrost w porównaniu z 2,2 mln USD w 2023 r. Co więcej, koszty odzyskiwania danych w tym sektorze podwoiły się od 2021 r., w którym kształtowały się na poziomie 1,27 mln USD [Sophos, 2024, s. 14].

Rośnie też czas odzyskiwania danych po ataku ransomware, który to właśnie przekłada się na dodatkowe koszty. Przykładowo w 2024 r. w przypadku 22% ofiar ataków ransomware odzyskano w pełni dane w ciągu tygodnia lub krócej, co stanowi znaczny spadek sprawczości w tym zakresie w porównaniu z 2023 r., a zwłaszcza 2022 r., w których odsetek odzyskanych danych w ciągu tygodnia lub krótszym wyniósł odpowiednio 47% i 54%. To spowolnienie może oznaczać zwiększoną złożoność ataków, co pociąga za sobą z jednej strony wzrost nakładów i czasu na odzyskiwaniem danych a z drugiej wskazuje na rosnący brak przygotowania do odzyskiwania danych.

## Podsumowanie

Zagrożenie atakiem złośliwym oprogramowanie ransomware w drugiej dekadzie XXI w. należy do jednych z najgroźniejszych. Szczególnie niebezpieczną formą jest model platformy RaaS. Rosnąca liczba użytkowników platformy i zachodzące pomię-

dzy uczestnikami interakcje sprawiają, że dostęp do usługi (wirusa) jest przyjazny dla użytkownika a korzyści z ataku odnosi wiele organizacji w ekosystemie RaaS (efekty sieciowe), w tym też po stronie ofiary. Przedmiotem ataku coraz częściej staje się sektor ochrony zdrowia, sektor o dużej i rosnącej liczbie danych wrażliwych przechowywanych w przestarzałych, słabo zabezpieczonych systemach informatycznych opieki zdrowotnej. Sektor ochrony zdrowia nie jest bowiem w powszechnym odczuciu postrzegany jako atrakcyjny dla cyberprzestępców, o czym świadczą luki w zabezpieczeniach dokumentacji medycznej i sprzętu, czy powierzeniu bezpieczeństwa informatycznego podmiotom zewnętrznym bez właściwego przeszkolenia personelu medycznego. W wyniku ataku rosną finansowe koszty ich usuwania (prawie połowę ponoszą podmioty ochrony zdrowia), lecz najgroźniejsze szkody są o charakterze społecznym od utraty tożsamości pacjentów po błędy w sztuce medycznej z powodu utraty dokumentacji.

W sytuacji wysokiej atrakcyjności sektora ochrony zdrowia dla cyberprzestępców i tym samym wysokiego ryzyka ataku ransomware wyzwaniem staje się podniesienie jego poziomu cyberbezpieczeństwa, co jednak nie powinno dziać się kosztem społecznym, czyli spadkiem nakładów na ochronę zdrowia *sensu stricto*.

## Bibliografia


Bartels N., Schmitt A. [2022], *Developing network effects for digital platforms in two-sided markets – The NfX construction guide*, "Digital Business", vol. 2(2), 100044.

Bekkers L., van 't Hoff-de Goede S., Misana-ter Huurne E., van Houten Y., Spithoven R., Leukfeldt E.R. [2023], *Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model*, "Computers & Security", vol. 127, 103099.

Bonina C., Koskinen K., Eaton B., Gawer A. [2021], *Digital platforms for development: Foundations and research agenda*, "Information System Journal", vol. 31(6), s. 869–902.

Ceccagnoli M., Forman C., Huang P., Wu D.J. [2011], *Co-creation of Value in a Platform Ecosystem! The Case of Enterprise Software*, "MIS Quarterly", vol. 36(1), s. 263–290.

Clancy M. [2021], *Introducing the Ransomware Economy*, https://www.backblaze.com/blog/ransomware-economy/ (data dostępu: 10.09.2024).

Cocker J. [2024], *#Infosec2024: Ransomware Ecosystem Transformed, New Groups "Changing the Rules"*, Infosecurity Magazine, https://www.infosecurity-magazine.com/news/ransomware-transformed-new-groups/ (data dostępu: 10.10.2024).

Cusumano M.A. [2012], *Platforms Versus Products. Observations from the Literature and History*, w: Kahl S., Silverman B., Cusumano M.A. (red.), *Advances in strategic management*, Emerald Group Publishing, s. 35–67.

ENISA [2022], *Threat landscape for ransomware attacks*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks (data dostępu: 24.10.2024).

eSentire [2023], *Stop Ransomware Before It Spreads*, https://www.esentire.com/how-we-do-it/use-cases/ransomware?utm_source=pardot&utm_medium=email&utm_campaign=nurture&utm_content=ransomware-page&utm_medium=email&utm_source=pardot&utm_campaign=prospect_nurture (data dostępu: 24.10.2024).

Feilner M. [2021], "*Ransomware as a Service" as a Business Model: Why the Business of Extortion Flourishes*, Greenbone, https://www.greenbone.net/en/blog/ransomware-as-a-service/ (data dostępu: 10.10.2024).

Hernandez-Castro J., Cartwright A., Cartwright E. [2020], *An economic analysis of ransomware and its welfare consequences*, "Royal Society Open Science", vol. 7(3), 190023, https://pubmed.ncbi.nlm.nih.gov/32269778/ (data dostępu: 22.10.2024).

Hutchinson E. [2024], *Ransomware in the global healthcare industry*, Ciso Intelligent, https://www.intelligentciso.com/2024/08/16/ransomware-in-the-global-healthcare-industry/ (data dostępu: 12.10.2024).

Laszka A., Farhang S., Grossklags J. [2017], *On the Economics of Ransomware*, w: Rass S., An B., Kiekintveld C., Fang F., Schauer S. (red.), *Decision and Game Theory for Security: 8th International Conference*, GameSec, Vienna, Austria, October 23–25, Proceedings (s. 397–417), Springer International Publishing.

Market Research Future [2024], *Global Healthcare Cyber Security Market Overview Source*, https://www.marketresearchfuture.com/reports/healthcare-cyber-security-market-7612 (data dostępu: 24.10.2024).

OIS [2024], *Ransomware & Healthcare*, Office of Information Security, January 18, https://www.hhs.gov/sites/default/files/ransomware-healthcare.pdf (data dostępu: 10.10.2024).

Olsen E. [2024], *Ransomware attacks on healthcare impact nearly five times more sensitive data: report*, https://www.healthcaredive.com/news/healthcare-ransomware-sensitive-data-rubrik-zero-labs/714215/ (data dostepu: 9.10.2024).

Pranggono B., Arabo A. [2020], *Covid-19 pandemic cybersecurity issues*, "Internet Technology Letters", https://onlinelibrary.wiley.com/doi/pdf/10.1002/itl2.247 (data dostępu: 9.10.2024).

Sophos [2024], *The State of Ransomware in Healthcare 2024*, https://assets.sophos.com/X24WTUEQ/at/4bk9xt4h7gsm4xs6mfzh3k/sophos-state-of-ransomware-healthcare-2024.pdf (data dostepu: 9.10.2024).

Täuscher K., Laudien S.M. [2018], *Understanding platform business models: A mixed methods study of marketplaces*, "European Management Journal", vol. 36(3), s. 319–329.

Thamer N., Alubady R. [2021], *A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research*, 1st Babylon International Conference on Information Technology and Science (BICITS), Babil, Iraq, s. 210–216.

Trischler M., Meier P., Trabucchi D. [2021], *Digital platform tactics: How to implement platform strategy over time*, "Journal of Business Models", vol. 9, s. 67–76.