

# Ataki na placówki medyczne – najnowsze przykłady i sposoby na ochronę danych

17.04.2025

Digitalizacja organizacji opieki zdrowotnej zrewolucjonizowała sposób gromadzenia, przechowywania i zarządzania danymi pacjentów. Jednakże wprowadza ona również wiele wyzwań, szczególnie związanych z bezpieczeństwem tych danych. W niniejszym artykule omówiono kwestie związane z bezpieczeństwem danych medycznych oraz ich znaczeniem, zwracając uwagę na kluczowe wyzwania i najlepsze praktyki w zakresie ochrony organizacji opieki zdrowotnej przed rozwijającymi się zagrożeniami cybernetycznymi.

## **Czym jest bezpieczeństwo danych medycznych?**

Bezpieczeństwo danych opieki zdrowotnej ma na celu ochronę poufnych informacji o pacjentach i powiązanych danych przed nieautoryzowanym dostępem, ujawnieniem, zmianą lub zniszczeniem. Łączy różne praktyki i

technologie w celu zabezpieczenia elektronicznej dokumentacji medycznej (EHR), historii medycznych i innych poufnych informacji przechowywanych w systemach opieki zdrowotnej.

## **Dlaczego bezpieczeństwo danych medycznych jest tak ważne?**

Bezpieczeństwo danych w opiece zdrowotnej jest krytyczne ze względu na wrażliwy charakter informacji i poważne konsekwencje ich ujawnienia. Zgodnie z raportem IBM Security Cost of a Data Breach Report z 2024 r. organizacje opieki zdrowotnej poniosły najwyższy średni koszt naruszenia danych po raz 14. z rzędu, wynoszący 9,77 mln USD. Zgodnie z HIPAA liczba zgłoszonych naruszeń danych w opiece zdrowotnej w USA wzrosła z 200 do 725 incydentów w latach 2011–2023. Poniższe przykłady z życia wzięte dodatkowo podkreślają konieczność wdrożenia silnych środków bezpieczeństwa danych w organizacjach opieki zdrowotnej.

Ubiegły rok był najgorszy w historii pod względem naruszeń danych w opiece zdrowotnej. Do 19 marca 2025 r. do OCR zgłoszono 734 duże naruszenia danych, co stanowi spadek procentowy o 1,74% w porównaniu z 747 dużymi naruszeniami danych w opiece zdrowotnej zgłoszonymi w 2023 r. Mimo niewielkiego spadku liczby incydentów, 2024 r. przyniósł bezprecedensowy wzrost liczby naruszonych rekordów danych medycznych – aż do 276 775 457, co odpowiada 81,38% populacji USA.

Jednak, jak wygląda sytuacja w Polsce? Tomasz Jeruzalski, dyrektor Pionu Eksploatacji Systemów Teleinformatycznych w Centrum e-

Zdrowia, zaznaczył, że rok 2025 będzie przełomowy dla kwestii związanych z bezpieczeństwem cyfrowym. Powodem jest m.in. planowana nowelizacja ustawy o Krajowym Systemie Cyberbezpieczeństwa, która ma na celu wdrożenie unijnej dyrektywy NIS2. Projekt ustawy ma zostać przyjęty jeszcze w pierwszym kwartale 2025 roku. Jeruzalski zwrócił uwagę, że zmiany te będą miały duże znaczenie także dla sektora ochrony zdrowia.

Jak pokazują analizy Centrum e-Zdrowia, poziom zabezpieczeń jest bardzo zróżnicowany. Co więcej, dane z ostatnich lat są niepokojące – liczba incydentów cybernetycznych w placówkach medycznych rośnie w szybkim tempie. W 2022 roku zarejestrowano 251 przypadków ataków, w 2023 już 405, natomiast w 2024 liczba ta przekroczyła tysiąc – dokładnie 1028 zdarzeń.

Najczęściej dochodziło do oszustw komputerowych, których było 374. Nie brakowało jednak również wycieków danych uwierzytelniających czy przypadków, w których wykorzystywano luki w usługach. Szczególnie niepokojący jest wzrost liczby ataków typu ransomware, które mogą sparaliżować pracę całych szpitali – z 317 przypadków w 2023 roku do aż 506 w 2024.

### **W jaki sposób cyberprzestępcy pozyskują dane medyczne?**

Czynnik ludzki Błąd ludzki pozostaje jednym z najważniejszych czynników przyczyniających się do naruszeń danych. Pomimo wdrożenia zaawansowanych technologii bezpieczeństwa pracownicy mogą nieumyślnie ujawnić poufne informacje za pomocą różnych środków, w

tym:

Ataków phishingowych, w których cyberprzestępcy nakłaniają użytkowników do ujawnienia danych logowania.

Stosowaniu słabych haseł lub używania tych samych haseł na wielu kontach.

Nieprzestrzeganiu odpowiednich protokołów bezpieczeństwa danych, prowadzących do przypadkowego ujawnienia poufnych danych pacjentów.

## **Szybkie wdrażanie technologii**

Szybkie przyjęcie chmury obliczeniowej, mobilnych aplikacji medycznych i Internetu Rzeczy Medycznych (IoMT) zwiększyło powierzchnię ataku dla organizacji opieki zdrowotnej. Urządzenia IoMT są na przykład coraz częściej podłączane do sieci szpitalnych w celu zdalnego monitorowania i diagnostyki. Jednak urządzenia te często nie mają takiego samego oprogramowania do ochrony danych opieki zdrowotnej, jak tradycyjne systemy IT, co czyni je kuszącymi celami dla cyberprzestępców.

## **Ewolucja zagrożeń cybernetycznych**

Cyberprzestępcy nie polegają już wyłącznie na tradycyjnych wektorach ataków, takich jak złośliwe oprogramowanie lub ransomware. Mogą na przykład atakować pracowników za pomocą ataków phishingowych

wspomaganych sztuczną inteligencją. Innym poważnym zagrożeniem w ostatnich latach jest korzystanie z platform ransomware-as-a-service (RaaS), na których hakerzy wynajmują swoje narzędzia ransomware innym przestępcom, ułatwiając w ten sposób przeprowadzanie ataków ransomware. Ataki te często prowadzą do utraty danych, przerwania ratujących życie zabiegów medycznych i strat finansowych.

## **Najlepsze praktyki zabezpieczania i ochrony danych dotyczących opieki zdrowotnej**

Poniższe najlepsze praktyki pomogą Ci chronić dane dotyczące opieki zdrowotnej i przygotować się na audyty zgodności:

### **Opracuj i utrzymuj solidne zasady bezpieczeństwa**

Dobrze zdefiniowana polityka bezpieczeństwa powinna być podstawą strategii ochrony danych, ponieważ pomaga łagodzić ryzyko poprzez określenie sposobu obsługi danych, zmniejszając w ten sposób potencjalne naruszenia danych.

Rozważ utworzenie szczegółowych zasad, które określają protokoły bezpieczeństwa, definiują obowiązki personelu ds. bezpieczeństwa i ustanawiają procesy zarządzania poufnymi danymi. Zasady te powinny być zgodne z odpowiednimi normami prawnymi dotyczącymi ochrony danych pacjentów.

### **Kształć i szkol pracowników**

Błąd ludzki nadal jest jedną z głównych przyczyn naruszeń danych w opiece zdrowotnej, co sprawia, że szkolenie pracowników jest niezbędne dla każdej organizacji. Powinieneś przeprowadzać regularne szkolenia z zakresu świadomości cyberbezpieczeństwa dla wszystkich pracowników, ze szczególnym uwzględnieniem identyfikowania i reagowania na próby phishingu, zabezpieczania urządzeń i przestrzegania właściwych procedur obsługi danych. Możesz również użyć symulacji phishingu, aby przetestować i zidentyfikować osoby, które mają trudności z rozpoznawaniem prób phishingu i potrzebują dodatkowego szkolenia.

### **Szyfruj i twórz kopie zapasowe danych**

Wszystkie dane pacjentów, niezależnie od tego, czy są przechowywane, czy przesyłane, powinny być szyfrowane przy użyciu standardowych algorytmów szyfrowania. Zapewnia to, że nawet jeśli dane zostaną przechwycone lub udostępnione złośliwym podmiotom, pozostaną nieczytelne bez kluczy deszyfrujących. Oprócz szyfrowania, musisz wykonywać kopie zapasowe, aby zabezpieczyć swoją organizację przed utratą danych. Ważne jest, aby wykonywać kopie zapasowe często i przechowywać dane w bezpieczny sposób, najlepiej poza siedzibą firmy lub w bezpiecznym środowisku chmury.

### **Wdrożenie silnych kontroli dostępu**

Stosuj podejście bezpieczeństwa zero trust, w którym nikt nie jest domyślnie zaufany, a wszystkie tożsamości są weryfikowane w celu zminimalizowania narażenia danych i nieautoryzowanego dostępu.

Możesz również trzymać się zasady najmniejszych uprawnień, która zapewnia, że użytkownicy otrzymują dostęp tylko do informacji, których potrzebują do wykonywania swoich funkcji zawodowych.

Dodatkowo rozważ wymuszenie obowiązkowego uwierzytelniania wieloskładnikowego (MFA) dla wszystkich użytkowników uzyskujących dostęp do poufnych danych. To doda dodatkową warstwę bezpieczeństwa, gwarantując, że nawet jeśli cyberprzestępcy ukradną dane logowania, nie będą mogli łatwo uzyskać dostępu do Twoich krytycznych systemów.

### **Zarządzaj ryzykiem stron trzecich**

Naruszenie na poziomie dostawcy może poważnie wpłynąć na Twoją organizację – zgodnie z ustawą HIPAA możesz zostać ukarany grzywną za nieodpowiednie zabezpieczenie danych, jeśli naruszenie ze strony osób trzecich ujawni PHI Twoich pacjentów, klientów lub personelu. Dlatego tak ważne jest, aby zagrożenia ze strony osób trzecich były pod kontrolą. Musisz dokładnie sprawdzać i monitorować wszystkich swoich dostawców, upewniając się, że przestrzegają najnowszych standardów bezpieczeństwa.

### **Przeprowadzaj regularne oceny ryzyka**

Przeprowadzaj regularne oceny ryzyka i testy penetracyjne, aby zidentyfikować potencjalne luki w zabezpieczeniach, zanim zostaną wykorzystane. Ocena ryzyka dostarcza cennych informacji na temat

obszarów, które wymagają wzmocnionych środków bezpieczeństwa, podczas gdy testy penetracyjne symulują rzeczywiste ataki, aby ocenić skuteczność Twoich zabezpieczeń.

## **Stwórz plan reagowania na incydenty**

Nawet przy najlepszych środkach zapobiegawczych, naruszenia nadal mogą się zdarzyć, co sprawia, że dobrze udokumentowany i wykonalny plan reagowania na incydenty (IRP) jest niezbędny. Utwórz IRP, który określa jasne kroki wykrywania, ograniczania, eliminowania i odzyskiwania po naruszeniu danych. Twój plan reagowania na incydenty powinien również obejmować strategię komunikacji mającą na celu powiadomienie osób poszkodowanych i organów regulacyjnych zgodnie z obowiązującymi przepisami i ustawami, takimi jak HIPAA i RODO.

## **Używaj dedykowanego oprogramowania do cyberbezpieczeństwa**

„Wdrożenie solidnego oprogramowania do cyberbezpieczeństwa jest kluczowym krokiem w ochronie systemów opieki zdrowotnej przed rozwijającymi się cyberzagrożeniami. Współczesne systemy antywirusowe mogą pomóc w automatyzacji zadań bezpieczeństwa, monitorowaniu aktywności użytkowników, zarządzaniu dostępem do krytycznych danych oraz wyświetlają alerty w czasie rzeczywistym w przypadku potencjalnych incydentów bezpieczeństwa” – mówi Arkadiusz Kraszewski z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło: <https://bitdefender.pl/ataki-na-placowki-medyczne-najnowsze-przyklady-i-sposoby-na-ochrone-danych/>

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.

Data udostępnienia: 17.04.2025

Z pozdrowieniami Piotr Rozmiarek

E-mail: [piotr.r@marken.com.pl](mailto:piotr.r@marken.com.pl) | Tel. bezpośredni: 570 400 019

### Informacje o firmie Bitdefender

Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.