**Anthem godzi się na 16 milionów dolarów grzywny**

**Drugi co do wielkości ubezpieczyciel zdrowotny w USA, Anthem, przekaże 16 milionów dolarów Urzędowi ds. Praw Obywatelskich w amerykańskim Departamencie Zdrowia i Opieki Społecznej.**

Jest to konsekwencja naruszenia elektronicznie chronionych informacji zdrowotnych (ePHI – ang. electronic protected health information) dotyczących blisko 80 milionów osób. Anthem wprowadzi także plan działań naprawczych, obejmujący gruntowną analizę ryzyka i stałe raportowanie.

Realizacja planu będzie nadzorowana przez rząd, co ma zapewnić jego zgodność z Ustawą o Swobodzie Przenoszenia Ubezpieczeń i Odpowiedzialności (HIPPA – ang. Health Insurance Portability and Accountability Act). Ustalona kwota jest najwyższą z tych, jakie kiedykolwiek wpłynęły do Urzędu ds. Praw Obywatelskich w konsekwencji naruszenia prawa do prywatności.

„Największe w historii USA naruszenie danych zdrowotnych bezwzględnie zasługuje na najwyższy w historii wymiar grzywny”

– [powiedział](https://healthitsecurity.com/news/anthem-to-pay-record-16m-for-hipaa-violations-exposing-79m-records) Roger Severino, dyrektor Urzędu ds. Praw Obywatelskich.

Wydany przez HIPAA, z myślą o ochronie danych pacjentów, zestaw [wytycznych](https://digitalguardian.com/blog/what-hipaa-compliance) dotyczących prywatności i bezpieczeństwa, uznawany jest za standard przemysłowy. Podmioty administrujące dokumentacją medyczną o krytycznym znaczeniu, takie jak Anthem, muszą spełniać standardy HIPAA pod względem bezpieczeństwa fizycznego i sieciowego oraz bezpiecznego przetwarzania. Dochodzenie przeprowadzone przez Urząd ds. Praw Obywatelskich wykazało, że Anthem nie podjął odpowiednich środków zabezpieczających dokumentację medyczną.

*„Niestety, firmie Anthem nie udało się wprowadzić odpowiednich środków umożliwiających wykrycie ingerencji hakerów, którzy uzyskali dostęp do jej systemu, umożliwiający zbieranie haseł i kradzież prywatnych informacji.*

*Wiadomo, że duże instytucje opieki zdrowotnej są dla hakerów atrakcyjnym celem. Dlatego oczekuje się, że będą one przestrzegały skutecznej polityki ochrony haseł oraz monitorowały i raportowały incydenty bezpieczeństwa, wykorzystując najnowsze dostępne środki”*

– powiedział Severino.

W roku wystąpienia zdarzenia (2015), incydent został opisany przez dyrektora generalnego firmy jako „bardzo wyrafinowany atak cybernetyczny”. Po przeprowadzeniu zmasowanego ataku, hakerom udało się przeniknąć do systemu informatycznego firmy i wykraść prywatne dane współpracowników i pacjentów, w tym ich adresy, identyfikatory medyczne, numery ubezpieczenia społecznego i dane o dochodach. Ujawnione mogły również zostać dane dotyczące zatrudnienia. Naruszenie dotknęło klientów Anthem Blue Cross, Anthem Blue Cross and Blue Shield, Blue Cross and Blue Shield of Georgia, Empire Blue Cross and Blue Shield, Amerigroup, Caremore, Unicare, Healthlink i DeCare.

Po złożonym w zeszłym roku przez zainteresowanych klientów pozwie, Anhthem wypłacił 115 milionów dolarów odszkodowania, celem pokrycia kosztów postępowania sądowego, dwóch lat monitorowania postępowań kredytowych i wykorzystania tożsamości, a także celem zwrotu kosztów, na jakie mogły zostać narażone ofiary (np. poniesionych na skutek fałszywych zeznań podatkowych).

*„Było to jedno z największych naruszeń danych klientów firmy ubezpieczeniowej.*

*Obowiązkiem ubezpieczycieli jest dbanie o zdrowie i tajemnicę finansową klientów. Komisja kontrolna nakazała firmie Anthem podjęcie szeregu kroków, mających na celu poprawę bezpieczeństwa cybernetycznego i zapewnienie ochrony kredytowej klientom dotkniętym incydentem. Komisja nasza ze znacznym stopniem pewności stwierdziła, że w tym przypadku przestępca działał w imieniu obcego rządu”*

– [powiedział](https://healthitsecurity.com/news/judge-gives-final-ok-to-115m-anthem-data-breach-settlement) Dave Jones, członek Komisji ds. Ubezpieczeń.

*„Przypadek firmy Anthem potwierdza, że bez względu na to, jak duże jest przedsiębiorstwo, zawsze może ono paść ofiarą ataku wykorzystującego phishingową wiadomość e-mail. Tym razem jeden moment nieuwagi i jeden złośliwy e-mil wystarczyły, by umożliwić hakerom włamanie się do infrastruktury IT firmy”* *Dariusz Woźniak, inżynier techniczny Bitdefender z firmy Marken* .