PUODO wskazuje błędy w zabezpieczeniu danych pacjentów i nakłada karę. Przestroga dla jednostek ochrony zdrowi

Kategoria: Polityka Zdrowotna
Opublikowano: piątek, 30, sierpień 2024 13:49
Adrian Pokrywczyński

Dane pacjentów są szczególnie wrażliwym zasobem. Przykład pewnego zakładu opieki zdrowotnej jest przestrogą dla publicznych placówek zdrowia przed lekceważeniem kwestii zabezpieczenia danych.

Jak poinformował w swoim komunikacie, Prezes Urzędu Ochrony Danych Osobowych nałożył na pewien Samodzielny Publiczny Zespół Opieki Zdrowotnej karę 40 tys. złotych. W wyniku ataku hakerskiego placówka straciła bowiem dostęp do danych pacjentów i pracowników. Wcześniej nie przeprowadziła analizy ryzyka dla danych osobowych, a działania naprawcze podjęła dopiero po fakcie.

Stan faktyczny: do ataku hakerskiego doszło w lutym 2022 r. Złośliwe oprogramowanie typu „ransomware" zaszyfrowało dane osobowe 30 tys. pacjentów i ponad tysiąca pracowników. ZOZ zawiadomił o tym UODO i Policję. Uznał jednak, że atak nie był poważny, bo dane nie wyciekły – stały się tylko niedostępne (zewnętrzny ekspert wskazał, że danych nie da się odszyfrować – atakujący uzależnili odszyfrowanie danych od zapłacenia okupu w kryptowalucie).

Jak wskazał PUODO:

- na zagrożenie dla danych osobowych ZOZ zareagował dopiero po ataku. Wtedy wezwał ekspertów, którzy wskazali luki w zabezpieczeniach i zarekomendowali zmiany. Odbyły się też szkolenia dla pracowników dotyczące bezpieczeństwa systemów informatycznych i danych.
- ZOZ nie miał dokumentów potwierdzających sporządzenie i aktualizowanie analizy ryzyka dla danych osobowych. Bezpieczeństwo danych powierzono informatykowi, który na bieżąco analizował m.in. podatności, zagrożenia, możliwe skutki naruszenia oraz środki bezpieczeństwa mające na celu zapewnienie poufności, integralności i dostępności przetwarzanych danych osobowych. To w żaden sposób nie mogło zapewnić należytej kontroli nad bezpieczeństwem danych.

W efekcie, przyjęte w ZOZ procedury nie były adekwatne do ryzyk dla danych osobowych. Wykazał to przeprowadzony już po ataku audyt.

Jak wskazano w komunikacie, nie mając analizy ryzyka ZOZ popełnił błędy także po incydencie – zgłosił swój problem UODO i Policji, ale pominął problem osób, których dane dotyczyły. Nie powiadomił ich, że stracił kontrolę nad danymi takimi jak: imię i nazwisko, imiona rodziców, datę urodzenia, numer rachunku bankowego, adres zamieszkania lub pobytu, nr PESEL, nazwę użytkownika i/lub hasło, dane dotyczące zarobków lub posiadanego majątku, nazwisko rodowe matki, serię i numer dowodu osobistego, numer telefonu oraz dane dotyczące zdrowia.

ZOZ błędnie uważał, że powiadamiać zainteresowanych nie musi, bo dane nie zostały wykradzione, tylko nie ma do nich dostępu. Jak jednak zauważa organ z dokonanych ustaleń wynika jednak jedynie, że nie ma śladu wycieku danych. Nie jest to jednoznaczne z tym, że hakerzy tych danych sobie nie skopiowali.

Poza tym, gdyby ZOZ sporządził rzetelną analizę ryzyka dla danych, wiedziałby, że problemem jest nie tylko wyciek danych, ale i to, że pacjenci tracą dostęp do swoich danych dotyczących zdrowia. Takiego ryzyka nie można oceniać jako niskie. Według urzędników zajmujących się ochroną danych inna kwalifikacja ryzyka skłoniłaby ZOZ do wprowadzenia lepszych zabezpieczeń.

Jak poinformowano - oprócz kary finansowej Prezes UODO zalecił wdrożenie w terminie 30 dni odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania

danych w systemach informatycznych. Nakazał też powiadomić o zdarzeniu osoby, których dane dotyczą, wytłumaczyć im co się stało, przedstawić możliwe konsekwencje zdarzenia i wskazać, kto może udzielić w ZOZ więcej informacji na ten temat.

Opracowano na podstawie komunikatu Prezesa Urzędu Ochrony Danych Osobowych z dnia 26 sierpnia 2024 r.