

Warszawa, dn. 22 października 2026 r.

Czego przedsiębiorcy mogą nauczyć się z incydentów MyDr i Fakturownia?

Ostatnie miesiące przyniosły dwa głośne incydenty bezpieczeństwa. Nawet jeśli skrót „UODO” brzmi dla Ciebie tajemniczo, a temat ochrony danych osobowych zwykle omijasz szerokim łukiem, prawdopodobnie słyszałeś już o co najmniej jednym z nich.

Pierwszy dotyczył systemu medycznego MyDr, wykorzystywanego przez placówki medyczne, gdzie według publicznie dostępnych informacji nieuprawniony dostęp objął dane milionów pacjentów oraz tysiące centrum i przychodni medycznych.

Drugi dotyczył platformy Fakturownia, która poinformowała o uzyskaniu przez osobę nieuprawnioną dostępu do systemów i skopiowaniu znacznej części bazy danych. Spółka wskazała, że incydent dotyczy wszystkich kont, choć zakres danych różni się w zależności od użytkownika.

Choć okoliczności obu zdarzeń są różne, płyną z nich podobne wnioski dla właścicieli firm i osób odpowiedzialnych za ochronę danych.

Jak się okazało, to bezpieczeństwo danych to nie tylko problem dużych korporacji

Wielu przedsiębiorców zakłada, że cyberprzestępcy interesują się wyłącznie dużymi korporacjami lub instytucjami publicznymi. W praktyce każdy podmiot przetwarzający dane osobowe może stać się pośrednią ofiarą incydentu występującego u swojego dostawcy usług. Niewielki gabinet lekarski, jednoosobowa działalność gospodarcza czy lokalna firma usługowa mogą zostać dotknięte skutkami naruszenia w takim samym stopniu jak duża organizacja.

Korzystanie z zewnętrznych systemów nie zwalnia z odpowiedzialności

Jedną z najczęstszych reakcji przedsiębiorców po informacji o incydencie jest stwierdzenie: „Przecież dane były w systemie dostawcy. To on odpowiada za bezpieczeństwo”. Z perspektywy RODO nie zawsze jest to prawda. Jeżeli przedsiębiorca pozostaje administratorem danych swoich klientów lub pacjentów, musi samodzielnie ocenić skutki naruszenia, udokumentować zdarzenie oraz ustalić, czy zachodzi obowiązek zgłoszenia naruszenia do Prezesa UODO lub poinformowania osób, których dane dotyczą.

Choć wielu przedsiębiorców chciałoby w takiej sytuacji uznać problem za wyłącznie problem dostawcy, rzeczywistość jest bardziej złożona. Warto jednak docenić, że w obu przypadkach dostawcy relatywnie informowali o zdarzeniach i zapewniali swoim klientom istotne wsparcie w zakresie dalszych działań oraz oceny obowiązków wynikających z przepisów o ochronie danych.

W wielu organizacjach proces wyboru dostawcy do dziś uwzględnia tylko korzyść cenową, ale ostatnie incydenty pokazały, że jednak należy poświęcić trochę czasu przed i w trakcie dostarczania usług na:

- zawarcie umowy powierzenia lub zweryfikowanie czy taka była wśród zaakceptowanych regulaminów;
- jak wygląda proces zgłaszania incydentów i wsparcie ze strony dostawcy w takim przypadku;
- jakie środki bezpieczeństwa zapewnia dostawca a jakie musi przedsiębiorca jako użytkownik systemu;
- najlepiej sporządzenie procedury, ale co najmniej instrukcji działań w sytuacji awaryjnej przy otrzymaniu informacji o incydencie, mogącym być naruszeniem ochrony danych;
- przeszkolenie pracowników z zakresu podstawowego cyberbezpieczeństwa i ochrony danych osobowych w pracy z danymi.

Dzięki temu uda się uniknąć chaosu i zareagować ze wszystkimi obowiązkami na czas!

Największym zagrożeniem nie zawsze jest sam wyciek

Krzykliwe tytuły w mediach społecznościowych i prasie koncentrują się zwykle na liczbie rekordów objętych naruszeniem czy skali zdarzenia. Tymczasem dla przedsiębiorcy większym problemem mogą okazać się późniejsze działania atakujących:

- phishing,
- podszywanie się pod kontrahentów,
- próby zmiany numerów rachunków bankowych,
- fałszywe faktury,
- wyłudzenia danych uwierzytelniających,
- oszustwa wykorzystujące wiedzę o relacjach biznesowych.

W przypadku danych finansowych lub medycznych ryzyko może utrzymywać się przez długi czas po wykryciu samego incydentu. Cyberbezpieczeństwo stało się elementem zarządzania ryzykiem biznesowym. Incydenty takie jak MyDr czy Fakturownia pokazują, że ten temat przestał być wyłącznie zagadnieniem technicznym. Dziś wpływa ono na reputację przedsiębiorstwa, relacje z klientami, ciągłość działania i ryzyko finansowe. **Postaw na spokojny sen i odpowiedzialne prowadzenie biznesu zgodnego z RODO.**

Kateryna Stryhina – specjalistka ds. ochrony danych osobowych w iSecure Sp. z o.o.