ziennik bezpieczeniowy

Nr (6203)
2025-03-28



Spojrzenie na rynek

Data publikacji: 2025-03-28
Dz.U. nr: 6203

# Fałszywy wyciek danych a ubezpieczenie cyber

**Informacje o głośnym, lecz fałszywym wycieku danych klientów Empiku, w weekend obiegły media. Sytuacja sprowokowała ważne pytanie: czy jeśli do szkody w rzeczywistości nie doszło, to ubezpieczenie cyber i tak zadziała? Zapytani o to brokerzy i ubezpieczyciele odpowiadają zgodnie: zadziała, ale na różnych warunkach.**
**- Martyna Skalska**

W sobotę 22 marca na jednym z forów hakerskich pojawiły się informacje o możliwości zakupu bazy danych użytkowników serwisu ***Empik.com***, zawierającej ok. 25 mln rekordów. Po tym, jak **Empik** zweryfikował podejrzenia wystąpienia cyberincydentu, okazało się, że do żadnego wycieku danych wcale nie doszło. Rzekoma oferta była po prostu wabikiem w celu wyłudzenia pieniędzy od osób chętnych na transakcję (zobacz: Fałszywy wyciek danych z Empiku).

## Rynkowe praktyki w cyber

**Piotr Rudzki**, cyber practice leader w **Aonie**, tłumaczy, jak należy się zachować już w przypadku podejrzenia cyberincydentu:

> *"Odpowiednia i szybka reakcja na zdarzenie jest kluczowa w zarządzaniu zdarzeniem cybernetycznym. Z jednej strony wynika to wprost z przepisów prawa, w przypadku naruszenia danych osobowych mamy przecież obowiązek notyfikacji regulatora i osób, których dane dotyczą. Z drugiej strony każda stracona godzina może się przełożyć na zwiększenie się wymiaru szkody - w przypadku naruszenia systemu infekcja będzie się szybko rozprzestrzeniać, a to będzie zwiększać koszty odtworzenia danych, utracone zyski, ale także prowadzić do szkody wizerunkowej".*

Jednak w przypadku Empiku do żadnej szkody właściwie nie doszło, bo wyciek danych okazał się fałszywy. Natomiast ustalenie tego faktu wymagało dużego nakładu pracy i pieniędzy. Sytuacja jest jedną z tych bardziej skomplikowanych z punktu widzenia ubezpieczeń, bo jak w takim przypadku zadziała ubezpieczenie cyber?

**Piotr Rudzki** mówi:

> *"Warunki praktycznie wszystkich liczących się ubezpieczycieli przewidują, że koszty reakcji na zdarzenie uruchamiają się już w przypadku uzasadnionego podejrzenia wystąpienia zdarzenia. Wydaje się, że upublicznioną informację o wycieku należy w tych kategoriach traktować. Różnić się za to może zakres kosztów, jakie ubezpieczyciel zapłaci w przypadku rzekomego zdarzenia".*

Podkreśla, że o ile wszyscy ubezpieczyciele powinni zapłacić koszty zaangażowania incydent menedżera i informatyków śledczych, to nie zawsze pokryją koszty kancelarii prawnej czy firmy PR-owej. Wymienia też, że w przypadku rzekomych zdarzeń, ubezpieczyciele stosują podlimit dla kosztów, jakie ubezpieczony może ponieść oraz znoszą udział własny kosztów reakcji na zdarzenie.

Jak wyjaśnia **Szymon Bąk**, broker, specjalista ds. ubezpieczeń ryzyk cybernetycznych w **EIB**:

> *"W zasadzie mówimy tutaj o stracie klienta w postaci poniesionych nakładów finansowych, celem bezpośredniej reakcji na potencjalny incydent i minimalizacji ewentualnej szkody - do której w praktyce najprawdopodobniej nie dojdzie. Ubezpieczyciele rynku cyber nie zignorowali takich sytuacji i dali im odzwierciedlenie w warunkach ubezpieczenia, wytyczając swoje granice w kontekście potencjalnej odpowiedzialności".*

**I** dodaje:

> *"W obszarze kosztów reakcji na incydent, które dotyczą m.in. kosztów PR, zaangażowania specjalistów w zakresie informatyki śledczej czy szeroko rozumianego cyberbezpieczeństwa, co do zasady mamy pokrycie w polisach ubezpieczenia, jeżeli istnieją uzasadnione podstawy, aby sądzić, że doszło do naruszenia danych. Empik w oparciu o takie przeświadczenie podjął konkretne*

*działania i poniósł koszty, aby ustalić czy faktycznie miało miejsce naruszenie danych i ograniczyć ewentualne skutki. Rozwińmy ten case nieco dalej, w kierunku potencjalnych roszczeń klientów. W obszarze pokrycia dla odpowiedzialności prawnej polisy cyber także wskazują, że koszty obrony ewentualnych postępowań cywilnych są pokrywane w sytuacji, gdy ubezpieczony naruszenia faktycznie dokonał lub gdy mu się to tylko zarzuca, co mogłoby mieć miejsce w przypadku Empiku".*

**Mateusz Manuszak**, broker ubezpieczeniowy, **Attis**, zwraca uwagę, że jeśli w omawianym przypadku ubezpieczony zdecydowałby się skorzystać z polisy cyber, modelowo powinien zgłosić incydent do partnera ubezpieczyciela. Wtedy eksperci mogą pomóc poprzez:

*"1. Weryfikację, co się w ogóle wydarzyło i czy oferowana baza jest prawdziwa (tak jak mieliśmy w tym przypadku), a więc usługi informatyków śledczych. Mogą się pojawić koszty związane z dochodzeniem i weryfikacją, czy podejrzenie wycieku danych jest zasadne.*

*2. Przygotowanie komunikacji z rynkiem i odpowiedniej odpowiedzi na artykuły pojawiające się w mediach, więc koszty działań informacyjnych i PR. Zarządzanie reputacją oraz komunikacja kryzysowa to często niedoceniany punkt ochrony w polisie cyber. To aspekt szczególnie istotny np. dla podmiotów notowanych na giełdzie, gdzie informacja o incydencie może mieć wpływ na negatywną odpowiedź inwestorów lub gdy trzeba odbudować zaufanie klientów i uspokoić ich o bezpieczeństwie danych".*

Wskazuje, że w powyższych przypadkach poniesione zostaną koszty w postaci honorariów dla ekspertów, które w obliczu incydentu i uzasadnionego podejrzenia wycieku, powinny być pokryte przez ubezpieczenie cyber.

## Fałszywy incydent okiem ubezpieczycieli

**Michał Balwiński**, senior underwriter, cyber practice leader, przedstawia przypadek fałszywego incydentu z punktu widzenia **Generali**:

*"Warunki ubezpieczenia Generali CyberRED wskazują, że ubezpieczony powinien raportować do zespołu reagowania na incydent (czyli w tym wypadku naszego partnera świadczącego incident response) wszelkie incydenty - faktyczne jak i domniemane".*

Ocenia, że w przypadku Empiku:

*"Zasadne jest skorzystanie z ubezpieczenia cyber w ramach zakresu dotyczącego reakcji na zdarzenie w celu weryfikacji, czy do faktycznego naruszenia doszło i skorzystania ze wsparcia analityków bezpieczeństwa, którzy mogą stanowić wsparcie w poszukiwaniu odpowiedzi na zadane pytanie. W omawianym kontekście można by też rozważać uruchomienie kosztów ochrony reputacji, w sytuacji, gdyby niezbędne było przygotowanie komunikacji kryzysowej w związku z medialnością zdarzenia".*

**Monika Ściuba**, koordynator ds. Underwritingu w **PZU**, podkreśla, że zakres ubezpieczenia cyber w PZU jest szeroki i zapewnia:

*"W PZU pokrywamy koszty zaistniałego naruszenia danych, naruszenia bezpieczeństwa sieci, a także tzw. koszty naprawienia, czyli takie, które poniósł ubezpieczony w wyniku zagrożenia naruszenia danych (tak jak w przypadku fałszywego wycieku w Empiku). Koszty naprawienia to m. in. koszty informatyków*

*śledczych, specjalistów IT, koszty obsługi prawnej czy public relations".*

Z kolei w **Ergo Hestii**, jak opisuje **Tomasz Dolata**, starszy underwriter zajmujący się ubezpieczeniami mienia, technicznymi oraz cyber:

> *"W ubezpieczeniach cyber - jak w każdym innym - wypłatę odszkodowania determinuje zaistnienie rzeczywistej szkody. Co jednak istotne, w ramach procesu likwidacyjnego, to my pokrywamy koszty całej informatyki śledczej, która pozwala znaleźć źródło problemu i stwierdzić, czy szkoda rzeczywiście zaistniała. Klient otrzymuje w tym wypadku szybkie i bezpośrednie wsparcie, które może ograniczyć negatywne skutki takiej sytuacji".*

**Juliusz Małyszko**, lider praktyki cyber w **Colonnade**, podsumowuje:

> *"Jeżeli zachodziłoby uzasadnione podejrzenie wycieku danych (a przypadku historii Empiku można tak podejrzewać) w ramach ubezpieczenia ryzyka cybernetycznego można skorzystać z zakresu usług śledczych, celem ustalenia, czy taki wyciek faktycznie miał miejsce, jakie były jego przyczyny oraz celem pozyskania rekomendacji w zakresie zapobiegania tego rodzaju naruszeniom lub ograniczania ich skutków. Dodatkowo, w ramach tego samego zakresu istnieje możliwość wdrożenia powyższych rekomendacji, a także zatrudnienia specjalistów z zakresu zarządzania reakcją na incydent".*

Nieważne, czy cyberincydent rzeczywiście miał miejsce, czy firma tylko podejrzewa, że do niego doszło. Branża jest zgodna - żeby zminimalizować potencjalne szkody, trzeba reagować od razu. I mimo że w zależności od ubezpieczyciela warunki ochrony cyber są różne, to pokryją chociaż część kosztów tej reakcji.

**Martyna Skalska**

---