ziennik bezpieczeniowy

Nr (6604)
2026-11-06

Ten egzemplarz został wysłany na adres: ukubicka@pzu.pl.

Spojrzenie na rynek

Data publikacji: 2026-11-06
Dz.U. nr: 6604

Ubezpieczyciele o cyber: rozwój, konkurencja, szkody

Rynek cyberubezpieczeń w Polsce na razie nie jest duży, ale dynamicznie się rozwija - uważają zgodnie ubezpieczyciele. Bodźcami wzrostu są m.in. rosnąca liczba cyberataków, cyfryzacja przedsiębiorstw i nowe regulacje. Między ubezpieczycielami rośnie konkurencja, jednak nie dotyczy ona wyłącznie cen i zakresu oferowanych rozwiązań. Dla klientów ważne bowiem są również procesy związane z ochroną.
- Martyna Skalska

W poprzednich ***Spojrzeniach na rynek*** o rynku cyberubzpieczeń mówili brokerzy ubezpieczeniowi. Opisywali oni szanse i zagrożenia dla cyberubezpieczeń, a także przedstawili swoje perspektywy o przyszłości rynku cyberubezpieczeń.
Dziś oddajemy głos ubezpieczycielom.

Dynamiczny rozwój i konkurencja

Ubezpieczyciele przyznają, że choć w Polsce rynek ubezpieczeń cybernetycznych nie jest jeszcze duży i na pewno jest mniej rozwinięty od rynków zachodnich, to cechuje go dynamiczny rozwój. **Paulina Borowiec**, koordynator ds. underwritingu, Biuro Pozakomunikacyjnych Ubezpieczeń Korporacyjnych w **PZU**, mówi:

> *"Rynek cyberubezpieczeń w Polsce dopiero dojrzewa. Coraz więcej firm dostrzega, że cyberatak może przełożyć się na realne straty finansowe i operacyjne, co z kolei przekłada się na rosnące zainteresowanie ochroną ubezpieczeniową".*

Jednocześnie podkreśla, że rośnie konkurencja między ubezpieczycielami.
W tej kwestii **Michał Balwiński**, cyber insurance product manager, w **Generali**, zwraca uwagę, że konkurencja nie sprowadza się jednak wyłącznie do ceny i zakresu polisy:

> *"Coraz większe znaczenie ma cały proces związany z ubezpieczeniem: sposób oceny ryzyka, działania prewencyjne i przede wszystkim jakość wsparcia, kiedy rzeczywiście dochodzi do incydentu. To właśnie wtedy klient najlepiej widzi praktyczną wartość cyberubezpieczenia".*

O obecnej sytuacji na rynku mówi również **Monika Rychlik**, PI/cyber product development leader w **Colonnade**. Ocenia, że rynek cyberubezpieczeń pozostaje miękki. Dostępna pojemność i obecność nowych ubezpieczycieli sprzyjają konkurencji cenowej oraz negocjowaniu szerszego zakresu ochrony:

> *"Klienci mogą uzyskać ochronę bez podlimitów dla istotnych elementów zakresu, co jeszcze kilka lat temu było znacznie trudniejsze. Zdarzają się jednak oferty, których cenę trudno uzasadnić oceną ryzyka. W części przypadków tę konkurencję oceniamy już jako dumping cenowy".*

Z perspektywy Colonnade opisuje, że dla ubezpieczyciela priorytetem pozostaje jakość przyjmowanego ryzyka:

> *"Nie chcemy budować portfela za cenę rezygnacji z rzetelnej oceny zabezpieczeń i potencjalnej skali szkody. Niska składka nie zmniejsza przecież kosztu przywrócenia działalności po incydencie".*

Jednocześnie **Juliusz Małyszko**, lider praktyki cyber w Colonnade, przyznaje, że sam proces oceny ryzyka stał się bardziej przyjazny dla klienta:

> *"Akceptujemy formularze brokerów lub innych ubezpieczycieli, jeżeli zawierają informacje potrzebne do przygotowania oferty. Nie ma powodu, aby klient kilkakrotnie odpowiadał na te same pytania tylko dlatego, że poszczególne towarzystwa posługują się innymi wzorami dokumentów. Uproszczenie formalności nie oznacza przy tym obniżenia wymagań dotyczących bezpieczeństwa".*

W kwestii rozwoju **Tomasz Dolata**, kierownik ds. ubezpieczeń mienia i utraty zysku w **Ergo Hestii**, ocenia z kolei, że głównymi bodźcami do wzrostu rynku są rosnąca liczba cyberataków, cyfryzacja przedsiębiorstw oraz nowe regulacje, takie jak NIS2 i DORA. Zauważa on jednak, że:

> *"Cyberubezpieczenia posiada przede wszystkim część dużych przedsiębiorstw oraz firm z sektorów regulowanych (finanse, energetyka). W segmencie MŚP poziom polis cyber pozostaje relatywnie niski, mimo że firmy te są częstym celem ataków".*

Częste i kosztowne szkody

Rosnąca liczba cyberataków w tym momencie jest dostrzegana już nawet przez osoby, które ze światem cyberincydentów nie mają do czynienia na porządku dziennym. Każdy większy przypadek jest nagłaśniany przez media. Aż strach pomyśleć, ile mniejszych przechodzi bez większego echa. Nawet tylko z ostatniego

tygodnia mieliśmy na łamach Dziennika Ubezpieczeniowego (nie licząc mniejszych przypadków w Szkodach w skrócie):

- Anatomia incydentu w Binance: analiza wektora ataku na kwotę 6,4 mld USD i implikacje dla korporacyjnego IT
- Cyberatak na systemy chłodnicze europejskich supermarketów
- Niemieccy politycy ostrzeżeni przed cyberatakami na iPhone'y
- Cyberatak na systemy chłodnicze w Polsce
- Francja: cyberatak na bank krwi; Auchan potwierdza atak w Polsce
- Cyberatak na bank Crédit Mutuel Arkéa

Cyberzagrożenia czają się na każdym kroku i dotyczą każdej branży. Świetnym przykładem są na to cyberataki na lodówki w supermarketach. Myślę, że jeszcze kilka miesięcy temu, nikomu nie przyszłoby do głowy, że dojdzie do takiego cyberincydentu i to w dodatku na taką skalę.

Właśnie w kontekście szkód zgłaszanych przez klientów ubezpieczyciele zgodnie przyznają, że do najczęstszych należą:

- zdarzenia związane z ransomware,
- wyłudzenia środków finansowych,
- naruszenie bezpieczeństwa i wyciekiem danych,
- incydenty prowadzące do czasowej niedostępności systemów informatycznych.

Również wśród najkosztowniejszych prym wiodą ataki ransomware, szczególnie te, które prowadzą do przerwy w działalności firmy. Jak zauważa **Michał Balwiński**, Generali:

> *"Przy poważnym ataku ransomware koszt nie kończy się przecież na ewentualnym okupie. Dochodzą koszty pracy ekspertów, odtworzenia systemów i danych oraz straty związane z przerwą w działalności. Dlatego z punktu widzenia przedsiębiorcy równie ważne jak pytanie "ile kosztował atak?" jest "jak długo firma nie mogła normalnie działać?".*

Również zdaniem **Pauliny Borowiec**, PZU, równie kosztowne są szkody związane z ransomware, w których dochodzi do podwójnego czynnika wymuszenia, tj. kradzieży danych oraz zaszyfrowania dysków:

> *"Prowadzi to do długotrwałego zakłócenia działalności firmy, a poza kosztami przywrócenia generuje dodatkowo straty związane z przestojem biznesowym".*

Jak w tej kwestii tłumaczy **Juliusz Małyszko**, Colonnade:

> *"Przy ustalaniu limitu patrzymy przede wszystkim na możliwy czas przestoju i jego skutki finansowe. Choć z naszego doświadczenia wynika, że przy dużych przedsiębiorstwach dużo szybciej zostanie skonsumowany limit, niż upłynie umówiony czas świadczenia BI".*

Tak więc nawet jeden, potencjalnie niegroźny cyberincydent, może przynieść firmie duże straty i spowodować przestój w jej działaności. A w kolejnym *Spojrzeniu na rynek* przyjrzymy się dostępnym na rynku rozwiązaniom cyber, dowiemy się, czy ubezpieczyciele planują wprowadzić coś nowego do oferty, a także przekonamy się, co może stać na przeszkodzie w dalszym dynamicznym rozwoju rynku cyberubezpieczeń.

Martyna Skalska







Strona przygotowana przez Ogma Sp. z o.o.