ziennik bezpieczeniowy

Nr (6263)
2025-06-27

Spojrzenie na rynek

Data publikacji: 2025-06-27
Dz.U. nr: 6263

Podnoszenie świadomości największym wyzwaniem cyber

Szkolenia dla pracowników, zabezpieczenia sprzętowe i software'owe, firewalle, antywirusy - o to i wiele innych muszą zadbać przedsiębiorcy, którzy chcą się ubezpieczyć od ryzyk cyber. Ubezpieczyciele mają bowiem wiele wymagań i nie biorą pod swoje skrzydła kogoś, kto sam nie zadba wcześniej o swoją firmę. A na cyberincydenty narażony jest każdy, kto posiada dostęp do internetu... Jednak w tym zakresie potrzebna jest jeszcze edukacja.
- Martyna Skalska

W poprzednim ***Spojrzeniu na rynek*** na ubezpieczenia cybernetyczne światło rzucili brokerzy. Mówili o rosnącej z roku na rok liczbie cyberataków w Polsce, nieubezpieczonym lub niedoubezpieczonym sektorze MŚP oraz o wymaganiach ubezpieczycieli, które firmy muszą spełnić, aby zawarcie umowy ubezpieczenia w ogóle było możliwe. A jak do klientów podchodzą ubezpieczyciele?

Różni ubezpieczyciele, w teorii różne wymogi

Juliusz Małyszko, cyber practice leader w **Colonnade**, tłumaczy:

> *"Underwriting cyber bada podejście i gotowość klienta na zagrożenia związane z przetwarzaniem danych, z działalnością w sieci, z atakami hakerskimi - sprawdzane są wdrożone procesy i systemy. Każdy ubezpieczyciel ma szereg swoich wymogów, ale najbardziej powszechne są regularnie wykonywane i testowane kopie zapasowe, szkolenia pracownicze, wielostopniowa autoryzacja przy połączeniach zdalnych i zgodność ze wszystkimi obowiązującymi regulacjami".*

Maciej Kleina, starszy underwriter w Biurze Ubezpieczeń Korporacyjnych, wyjaśnia, jak do tematu cyber podchodzi **Ergo Hestia**:

> *"Badamy 2 aspekty:*
> *1. Skalę działalności klienta w kontekście ryzyk cyber, rozumianych jako ilość danych elektronicznych, rekordów danych osobowych, obrót, liczba komputerów/serwerów.*
> *2. Ocenę infrastruktury teleinformatycznej, czyli systemy, ludzi (szkolenia) oraz zabezpieczenia sprzętowe i software'owe."*

Paulina Borowiec, koordynator ds. underwritingu z Biura Analiz i Oceny Ryzyka Ubezpieczeń Korporacyjnych w **PZU**, zapewnia:

> *"Każdy klient jest oceniany indywidualnie - z uwzględnieniem wielkości firmy, profilu działalności oraz oczekiwanego zakresu ochrony. Istnieją jednak podstawowe wymogi, które muszą zostać spełnione, aby możliwe było objęcie ochroną".*

Wśród wymagań wymienia m.in.: firewalla i aktualne oprogramowanie antywirusowe, regularne tworzenie i testowanie kopii zapasowych, zabezpieczenie zdalnego dostępu

za pomocą uwierzytelnienia wieloskładnikowego (MFA) i bieżącą instalację krytycznych aktualizacji oprogramowania.

Z kolei **Michał Balwiński**, senior underwriter, cyber practice leader w **Generali**, mówi:

> *"Proces oceny ryzyka w Generali można określić jako dwuetapowy. W pierwszej części dokonujemy wstępnego scoringu higieny cybernetycznej klienta na podstawie publicznie dostępnych danych jego domen internetowych przy wykorzystaniu własnych narzędzi zasilanych również poprzez zewnętrzne silniki OSINT-u sieciowego w celu uzyskania możliwie pełnego obrazu przy braku jakiejkolwiek ingerencji w wewnętrzne sieci i systemy klienta".*

I dodaje:

> *"Pozytywne przejście scoringu przenosi nas bezpośrednio do drugiego etapu oceny ryzyka - badania zarządzania nim wewnątrz organizacji w aspektach technicznych, proceduralnych i organizacyjnych - co do zasady na bazie kwestionariusza zawierającego konkretne pytania dotyczące kluczowych elementów cyberzarządzania. Jeżeli ryzyko jest bardziej złożone, prowadzimy bezpośrednie rozmowy z klientem - zazwyczaj online, w czasie rzeczywistym".*

Podkreśla również, że ubezpieczenie ryzyk cybernetycznych nigdy nie zastąpi zarządzania ryzykiem w organizacji, a klient który nie zaopiekował się swoim ryzykiem cyber - nie otrzyma oferty ubezpieczenia.

Trzeba zadbać o edukację

Dla wielu przedsiębiorstw, szczególnie tych z sektora MŚP, wymagania ubezpieczycieli w zakresie cyberbezpieczeństwa stanowią wyzwanie. Jednak od wyzwań nie są również wolni ubezpieczyciele. **Maciej Kleina**, Ergo Hestia, wskazuje:

> *"Rynek się ustabilizował, jeśli chodzi o zakres ubezpieczenia oraz wycenę, choć zdarzają się zwroty w podejściu do ubezpieczenia, jak np. całkowite wycofanie się z oferowania cyber. Wyzwaniem w dalszym ciągu pozostaje poprawa aktualnie niskiej świadomości konieczności ubezpieczania się, co przekłada się na wyniki sprzedażowe".*

I precyzuje:

> *"Firmy z sektora MŚP są wyraźnie niedoubezpieczone w zakresie cyber, a wynika to od lat z tych samych powodów: po pierwsze brak świadomości ryzyka, po drugie niechęć do poświęcania budżetu na ubezpieczenia z tego zakresu. Najpierw trzeba zbudować świadomość ryzyka, która pobudzi potrzebę i zrozumienie ubezpieczenia. Sami próbujemy to robić organizując spotkania dla pośredników poświęcone ryzykom cyber. Obecnie duży nacisk kładziemy na autentyczne szkody, które sami mieliśmy okazję likwidować".*

Tak samo uważa **Juliusz Małyszko**, Colonnade:

> *Największym wyzwaniem obecnie i w przyszłości jest edukacja rynku. Sam produkt jest dojrzały, a pojemność dostępna, jedynie świadomość klientów i zrozumienie produktu wymaga jeszcze pracy".*

Natomiast **Paulina Borowiec**, PZU, do tej listy dodaje również rosnącą złożoność zagrożeń i konieczność dostosowania ofert do zmieniających się regulacji (np. w zakresie odporności cyfrowej).

Cyber - trzeba zadbać nie tylko o ubezpieczenie

I choć ubezpieczenie pomoże po cyberincydencie, firmy muszą zadbać o cyberbezpieczeństwo, aby zminimalizować ryzyko ataków. **Michał Balwiński**, Generali, zaznacza:

> *"W świecie, w którym pytanie nie brzmi "czy", ale "kiedy" organizacja stanie się celem ataku, dobrze skonstruowana polisa cyber może być ostatnią linią obrony - i pierwszym krokiem do szybkiego powrotu do normalności".*

Zwraca jednak uwagę:

> *"Cyberubezpieczenie nie jest produktem masowym - to narzędzie dla świadomych organizacji, które traktują bezpieczeństwo cyfrowe jako integralną część swojej strategii zarządzania ryzykiem. Proces underwritingowy nie powinien być postrzegany jako bariera, lecz jako okazja do weryfikacji i wzmocnienia własnych mechanizmów ochrony".*

Jak podsumowuje **Paulina Borowiec**, PZU:

> *"Pozytywnym sygnałem jest rosnąca świadomość zagrożeń oraz rozwój nowoczesnych narzędzi ochronnych - takich jak sztuczna inteligencja, która umożliwia automatyczne wykrywanie i reagowanie na incydenty.*
>
> *Niemniej jednak, fundamentem skutecznej ochrony pozostaje edukacja i świadomość użytkowników - to oni stanowią pierwszą linię obrony przed cyberatakami".*