

**Ubezpieczenia** > Po atakach hakerów.

# Słaba sprzedaż polis od cyberzagrożeń

Po ostatnim ataku ransomware, który dotknął wiele polskich firm, doprowadzając w kilku przypadkach do całkowitego paraliżu działalności, przedsiębiorcy zaczęli interesować się polisami cyber.

- Likwidacja skutków ataku wiąże się nie tylko z koniecznością wypłaty odszkodowań oraz przeprowadzenia akcji informacyjnej skierowanej do osób, których dane firma przetwarza. Wysokich nakładów finansowych wymagają też aktywności związane z wykryciem i usunięciem zagrożenia - tłumaczy Łukasz Zon, prezes Stowarzyszenia Polskich Brokerów Ubezpieczeniowych i Reasekuracyjnych.

Do niedawna przedsiębiorcy nie byli zainteresowani tymi polisami. Zaczyna się to zmieniać, ale przelamywanie niechęci do drogiego polisa przychodzi z trudem. Jeszcze nie widać wzrostu sprzedaży, ale przedsiębiorcy pytają brokerów o taką ochronę.

- Firmy na naszym rynku powoli decydują się na zawieranie umów ubezpieczeń od ryzyk cybernetycznych. Działy IT, które dotychczas

często wstrzymywały zawieranie takich ubezpieczeń, aktualnie zmieniają swoją optykę, uświadamiając sobie, że nawet najlepsze zabezpieczenia mogą okazać się niewystarczające, i nie chcą brać odpowiedzialności za potencjalne straty, które firma może ponieść wskutek ataku hakerskiego - mówi Jakub Płocienniczak, broker ubezpieczeniowy z Willis Towers Watson Polska.

Nie tylko ostatnie ataki hakerów wpłynęły na ożywienie dyskusji na temat konieczności ochrony danych osobowych. W maju 2018 roku wchodzi w życie RODO - unijne rozporządzenie dotyczące ochrony danych osobowych. Przedsiębiorstwa będą musiały przeanalizować, jak wysokie ryzyko wiąże się z utraceniem gromadzonych przez nie informacji, i stworzyć skuteczny system ochrony.

- Proces może być o tyle skomplikowany, że RODO nie podpowiada, co konkretnie przedsiębiorca ma zrobić, aby uniknąć kary, sam będzie musiał poczynić kroki, które w najlepszy sposób ochronią jego firmę - tłumaczy Michał Kwasek z ANG Spółdzielni. © 110