Firmy powoli przekonują się do cyberubezpieczeń

FINANSE | Po niedawnych atakach hakerów przedsiębiorcy zaczęli pytać brokerów o polisy od tych zagrożeń, ale wzrostu sprzedaży jeszcze nie widać.

REGINA SKIBIŃSKA

Ostatni atak typu ransomware (szyfrujący dane, żądając okupu pieniężnego) dotknął wiele polskich firm, doprowadzając w kilku przypadkach do paraliżu ich działalności.

– 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 również aktywności związane z wykryciem i usunięciem zagrożenia – tłumaczy Łukasz Zoń, prezes Stowarzyszenia Polskich Brokerów Ubezpieczeniowych i Reasekuracyjnych.

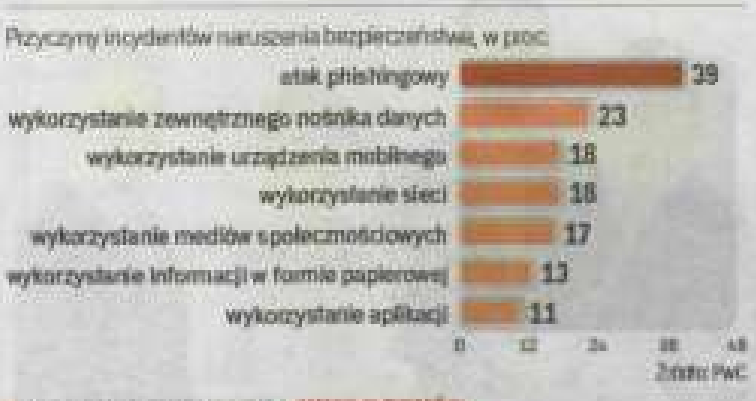
Rośnie ryzyko

Do niedawna polscy przedsiębiorcy nie byli zainteresowani ochroną przed cyberatakami. Zagrożenia wydawały się mało realne, a konsekwencje odległe.

– Zarówno towarzystwa ubezpieczeniowe, jak i właściciele firm bagatelizowali problem, o czym świadczy uboga oferta produktów mających na celu zabezpieczenie przed tego typu zagrożeniami oraz niski popyt na takie usługi – mówi Michał Kwasek z ANG Spółdzielni.

@ masz pytanie, wyślij e-mail do autorki

r.skibinska@rp.pl



PHISHING WYRZĄDZA WIELE SZKÓD

Zaczyna się to zmieniać, ale przełamywanie niechęci do drogich polis (ceny wahają się od kilkuset złotych dla małych kancelarii do kilku milionów złotych dla dużych instytucji) przychodzi z trudem. Jeszcze nie widać wzrostu sprzedaży, ale przedsiębiorcy coraz częściej pytają brokerów o taką ochronę ubezpieczeniową.

RZECZPOSPOLITA
PISALIŚMY O TYM:
Na rynku jest coraz więcej polis zdrowotnych dla przedsiębiorców
„Ubezpieczeniowa wojna o małe firmy"
30 czerwca 2017 r.
archiwum.rp.pl

– Zainteresowanie ubezpieczeniem od konsekwencji incydentów cybernetycznych zdecydowanie wzrosło w ostatnim kwartale. Spodziewamy się, że druga połowa roku 2017 będzie jeszcze bardziej zdominowana pytaniami o dostępność rozwiązań w tym zakresie – mówi Anna Pluta, lider Praktyki Ryzyka Cybernetyczne z firmy brokerskiej Marsh.

Potrzeba czasu

Wśród przedsiębiorców często pokutuje opinia, że najlepszym zabezpieczeniem są „fizyczne" rozwiązania w postaci nowoczesnego hardware i software, jednak co jakiś czas pojawiają się nowe groźby, wobec których najlepszy nawet sprzęt i oprogramowanie ochronne okazują się bezradne.

– Firmy powoli decydują się na zawieranie umów ubezpieczeń od ryzyk cybernetycznych. Działy IT, które dotychczas często wstrzymywały zawieranie takich ubezpieczeń, aktualnie zmieniają optykę, uświadamiając sobie, że nawet najlepsze zabezpieczenia mogą okazać się niewystarczające, i nie chcą brać odpowiedzialności za ogromne straty, które firma może ponieść wskutek ataku hakerskiego – podaje Jakub Płócienniczak, broker ubezpieczeniowy z Willis Towers Watson Polska.

Pytania o polisy dopiero będą skutkowały umowami.

– Proces zawierania umów ubezpieczeniowych dla dużych organizacji często trwa ok. trzech miesięcy od momentu pierwszego zainteresowania transferem ryzyka na ubezpieczyciela – wyjaśnia Anna Pluta.

Wrażliwe dane

Nie tylko ostatnie ataki hakerów wpłynęły na ożywienie dyskusji na temat konieczności ochrony danych osobowych. W maju 2018 roku wchodzi w życie RODO, czyli nowe unijne rozporządzenie dotyczące ochrony tych danych. 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 rozporządzenie 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. Dyrektywa RODO powinna zmienić podejście do polis cyber.

– Tempo tych zmian zależeć będzie również od faktycznego podejścia organów nadzorczych do możliwości nakładania kar i ich wysokości. Zgodnie z nowym prawem może to być nawet do 4 proc. obrotów lub 4 mln euro – tłumaczy Płócienniczak. ee