aut. Andrzej Kozłowski 07.06.2018

NAJWIĘKSZE RYZYKO TO PRZERWA W DZIAŁALNOŚCI FIRMY [WYWIAD]

O polskim rynku ubezpieczeń od ryzyka cybernetycznego oraz wpływie RODO na jego przyszłość mówi dla CyberDefence24.pl Małgorzata Splett z Marsh.

Dr Andrzej Kozłowski: Jak RODO może wpłynąć na ubezpieczenia od ryzyka cybernetycznego?

Małgorzata Splett: W kontekście RODO wszyscy mówią o karach, które miałyby wynosić do 20 milionów euro lub 4 % dochodu. To są ogromne kary. Ostatnio coraz więcej klientów pyta czy istnieją ubezpieczenia pod RODO. Ubezpieczenie od ryzyka cybernetycznego jedynie w pewnym zakresie odpowiada na potrzeby RODO. Nie ma jednak dedykowanych stricte pod RODO produktów ubezpieczeniowych.

Ubezpieczenia od ryzyka cybernetycznego pokryją tylko pewne obszary związane z RODO. Częściowo, ale nie w całości pokryją np. kary. Ponadto zapewnią firmie doradcę ds. sytuacji kryzysowych, który zajmie się przedsiębiorstwem w momencie ataku, wymuszenia czy wycieku danych wrażliwych. Poza tym, odpowie ono w zakresie pokrycia kosztów związanych z obowiązkiem notyfikacyjnym, czyli mówiąc krótko w ciągu 72 godzin należy poinformować o wycieku danych wszystkich, których dane osobowe zostały naruszone. Ponadto, firma być może będzie musiała odpowiedzieć finansowo na roszczenia klientów, w przypadku gdy ich dane zostaną naruszone.

Wszyscy mówią o karach, jednak dla wielu klientów największym ryzykiem związanym z cyberatakiem jest przerwa w działalności i to, że firma przestaje funkcjonować. Warto tu wrócić do ataku NotPetya z poprzedniego roku. Systemy jednego z naszych klientów zostały całkowicie zablokowane. Hakerzy zwrócili się o okup w bitcoinach. Firma posiadała polisę, dzięki której przedsiębiorstwo otrzymało wsparcie doradcy do spraw kryzysowych, który natychmiast włączył się w temat i pomógł zarządzać kryzysem. Udało się też uniknąć zapłaty za okup a system został odblokowany. W tym przypadku pojawiły się również roszczenia ze strony kilku kontrahentów. Koszty potencjalnych odszkodowań dla kontrahentów mogą wynieść nawet kilkaset tysięcy złotych.

Co jednak się dzieje jak mamy do czynienia z elektrownią czy firmą świadczącą usług telekomunikacyjne?

Wystarczy sobie wyobrazić, że firma zostaje wyłączona na 24 godziny - roszczenia z tego tytułu mogą poważnie wpłynąć na jej sytuacją finansową i dalsze funkcjonowanie.

Jak wygląda na tle Europy, polski rynek ubezpieczeń od ryzyka cybernetycznego ?

Polski rynek jest w fazie ciągłego rozwoju. Zupełnie inaczej sytuacja wygląda np. w Wielkiej Brytanii, Niemczech, czy Francji, gdzie ubezpieczenia cyber są już znacznie bardziej popularne i stosowane.

Według Raportu „Global Risks Report 2018" cyberataki były wskazywane jako jedne z wielu niebezpieczeństw i na mapie Europy pokazano, dla których krajów stanowią największe zagrożenie. Największe potencjalne straty odnotowano w Niemczech i krajach Beneluksu, w których doszło do największej liczby ataków w roku 2017.

Firmy będą też zainteresowane ryzykami powiązanymi z cybernetycznym wynikającym z delikatnie innej odpowiedzialności. Przykładowo - będzie zainteresowana odpowiedzialnością zarządu w zakresie wycieku danych. W polisie D&O odpowiedzialność zarządcza i nadzorcza w tym zakresie powinna uruchomić polisę D&O np. w przypadku roszczeń spółki do menedżerów z tego tytułu.

Czy w takim razie ubezpieczenie od ryzyka cybernetycznego pokrywa wszystkie koszty?

„Zwykła" polisa cyber raczej nie pokryje np. takiego przypadku - atak hakerski na bank i wyciek pieniędzy z kont klientów. Klient przychodzi do banku z roszczeniem i mówi, że z jego konta zniknęło 500 tys. złotych. Polisa od ubezpieczenia od ryzyka cybernetycznego nie jest raczej w stanie pokryć tej utraty środków, natomiast pokryje inne związane z atakiem. Dla takich celów dedykowana jest jeszcze polisa chroniąca przed sprzeniewierzeniem czyli tzw. crime. Banki i inne instytucje finansowe często korzystają z takiego rozwiązania.

Czyli tak naprawdę, żeby odzyskać utracone środki to polisa cyber nie wystarczy?

Trzeba pomyśleć o klauzuli sprzeniewierzenia, albo o osobnej polisie od ryzyka sprzeniewierzeń. Polis crime na polskim rynku jest bardzo niewiele. Posiadają je głównie banki i firmy spożywcze, które obawiają się sprzeniewierzeń pracowniczych. Z kolei za granicą tego rodzaju polisy są dużo bardziej popularne. Rozmawiając z klientami staramy się rozmawiać z klientami om ryzyku cyber szeroko. Rozpoznając ryzyko cyber powiązane z OC zawodową, OC zarządu, ze sprzeniewierzeniem. Polscy klienci są coraz bardziej świadomi tego ryzyka i rzeczywiście przestali patrzeć na ten problem wycinkowo.

Kto jest głównym klientem? Banki?

Nie ma reguły. Można powiedzieć, że banki są bardzo świadome jeżeli chodzi o ryzyla cybernetyczne, ze względu na fakt, iż podlegają mocniej odpowiednim regulacjom i są instytucjami zaufania publicznego. Bardzo duże zainteresowanie obserwujemy również w takich branżach, jak telekomunikacja, IT, sklepy internetowe, czy sektor zdrowia - ogólnie wszystkie przedsiębiorstwa, które posiadają dane klientów lub dla których przerwa w działalności jest dużym problemem.

Jakie jest zainteresowanie sektora publicznego takimi usługami?

Obserwujemy pewne zainteresowanie wśród jednostek sektora publicznego. Jednak w tym przypadku temat jest dość złożony. Ryzyko cybernetyczne trzeba tu bardzo dobrze skwantyfikować, ocenić zanim zaprojektuje się odpowiedni zakres ubezpieczenia i dostosuje go do potrzeb tak złożonych organizacji.

A sektor medyczny?

To jest bardzo duże ryzyko. Przykładowo, wyciek danych z kart medycznych pacjentów, gdzie jest zapisana cała historia choroby. Takie wycieki występowały już zagranicą. Firmy medyczne mocno interesują się rozwiązaniami w zakresie cyber ryzyka. RODO z pewnością dodatkowo napędziło tę sytuację.

Największym problemem RODO nie będą gigantyczne kary administracyjne, ale pozwy cywilnoprawne, w szczególności biorąc pod uwagę skromne zasoby UODO. Czy się Pani

zgodzi z tym twierdzeniem?

Wysokość kar przeraża, ale czy one faktycznie będą nakładane, pokaże przyszłość. Firmy powinny szerzej patrzeć na to ryzyko, także w kontekście roszczeń ich klientów, co może się zdarzyć w przypadku przerwy/zatrzymania działalności. Jest to szczególnie istotne w newralgicznych sektorach, jak sektor logistyczny, energetyczny czy telekomunikacyjny. Nie można powiedzieć, że kar nie będzie, ale na pewno będą one działały jako dodatkowy „straszak" i będą nakładane na nie jedynie największe podmioty działające w danej branży.