Cyberdefence 24

aut. Andrzej Kozłowski 23.11.2018

CYBERPOLISY W ERZE RODO [ANALIZA]

Wejście w życie w RODO 25 maja 2018 roku było przedstawiane jako jedna z najbardziej rewolucyjnych zmian w przepisach polskiego prawodawstwa w obszarze ochrony danych. Wysokie kary, które grożą firmom za naruszenie danych spowodowały, że poszukują one sposobów na zabezpieczenie się przed cyberatakami oraz ich negatywnymi skutkami. Doprowadziło to do większego zainteresowania wśród przedsiębiorców ubezpieczeniami typu cyber. Pozwalają one m.in. na pokrycie kosztów kar administracyjnych nakładanych przez regulatora.

W Polsce rynek cyberpolis rozwijał się powoli, trend ten ma jednak szanse ulec zmianie. Jest to związane z wejściem w życie Rozporządzania o Ochronie Danych Osobowych (RODO). Nowe zasady wprowadzone przez te przepisy dotyczące ochrony danych osobowych wymogły od przedsiębiorców przetwarzających informacje przemodelowania sposobu działania w tym obszarze. Chodziło tu o kwestie fizycznych zabezpieczeń w postaci nowoczesnego hardware i software oraz modyfikacji wewnętrznych procedur i protokołów bezpieczeństwa.

Najbardziej na wyobraźnie wszystkich działają kary pieniężne, które ma wprowadzić RODO. W nowym prawie można wyróżnić dwa przedziały administracyjnych kar pieniężnych. Za nieprzestrzeganie podstawowych obowiązków grozi sankcja do 10 mln euro, a przedsiębiorcy alternatywnie mogą zapłacić 2 proc. całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Wybrana tu zostanie kara wyższa. Drugi przedział to kara, która może zostać nałożona np. za niewykonanie poleceń Urzędu Ochrony Danych Osobowych, za co grozi nawet 20 mln euro lub 4 proc. całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Kary te powodują, że praktycznie wszyscy zainteresowali się problematyką ochrony danych, a jednym z narzędzi, które może to ułatwić są właśnie ubezpieczenia Cyber.

Polisy te są najbardziej popularne w Stanach Zjednoczonych, gdzie zaczęły pojawiać się w latach 90. W Europie, najczęściej korzystają z nich Brytyjczycy, Niemcy i Francuzi. Nie tylko jednak RODO wpływa na zmiany na rynku cyber ubezpieczeń, ale też dynamiczny rozwój technologii. Zmusza to sektory MŚP do szukania rozwiązań minimalizowania skutków cyberataków. Bardzo rzadko małe i średnie firmy mają możliwość zatrudnienia odpowiednich osób i wdrożenia rozwiązań technologicznych, które są bardzo drogie. Dlatego jedynym rozwiązaniem mogą być tutaj cyber-ubezpieczenia. Na początku 2018 roku w Stanach Zjednoczonych polisę cyber posiadało już ponad 60 proc. przedsiębiorstw. W Polsce tylko 8 proc. firm posiadało taką polisę. Prognozuje się, że w przeciągu kilku lat sytuacja ta ulegnie zmianie i ponad połowa firm będzie miała taką polisę.

Należy jednak pamiętać, że cyber ubezpieczenia nie są tanie. Zależą w dużej mierze od maksymalnej wartości gwarantowanego odszkodowania oraz od stopnia narażenia na ryzyko, a to jest większe w przypadku sektora MŚP niż dużych przedsiębiorstw. Po drugie, wciąż niewielu ubezpieczycieli na polskim rynku je oferuje. Po trzecie wciąż dotyczą obszaru słabo zbadanego, gdzie przeprowadzenie analizy ryzyka jest bardzo trudne. Pomimo 20 lat obecności na rynku nie stworzono uniwersalnego modelu mierzenia unikalnego ryzyka związanego z ryzykiem cybernetycznym. W innych branżach

używa się doświadczeń i incydentów z przeszłości do szacowania przyszłości, ale w cyberprzestrzeni nie ma dwóch takich samych incydentów, dlatego ta metoda się nie sprawdza. Kilka lat temu głównym ryzykiem były przecieki danych, dzisiaj do tego dochodzi szyfrowanie danych podczas ataków ransomware. Wreszcie, liczba cyberataków stale rośnie, więc firmy oferujące polisy wiedzą doskonale, że znajdą klientów na swoje usługi.

Nie wszystkie firmy mogą być jednak objęte polisą. Niektórzy brokerzy ubezpieczeniowy wykluczają podmioty odpowiedzialne za kontrolowanie ruchu społeczeństwa, udostępniania mediów społecznościowych, treści pornograficznych czy windykację należności.

Stawka polisy zależy od wielu czynników. Istotna jest branża, w której funkcjonuje firma oraz ilość i jakoś danych, którymi obraca. Im informacje są bardziej wrażliwe tym większa będzie cena. Dlatego też polisy dla np. sektora medycznego będą droższe niż dla pozostałych branż. Istotne znaczenie mają również zabezpieczenia i procedury istniejące w firmach, co pozwala ocenić stan zabezpieczeń w przedsiębiorstwie. Jeżeli jest ono wyposażone w odpowiednie narzędzia ochrony sieci i systemów oraz jeśli wprowadzone są odpowiednie procedury, to automatycznie spada ryzyko udanego ataku. Sama polisa w takim przypadku kosztuje mniej. Analiza tych wszystkich czynników pozwala wycenić polisę. Przedział cenowy jest tu bardzo zróżnicowany od kilku tysięcy złotych dla małych firm do kilkuset tysięcy dla dużych przedsiębiorstw, w niektórych skrajnych przypadkach można mówić o milionach złotych.

Zadaniem ubezpieczenia cyber jest przede wszystkim zapewnienie ochrony w przypadku wycieku danych. Podstawowym zakresem jest tutaj kwestia odpowiedzialności cywilnej z tytułu naruszenia dóbr osobistych w związku z utratą czy ujawnieniem danych osobowych przechowywanych bądź przetwarzanych przez ubezpieczonego Ubezpieczenie cyber może również pokryć szkody następcze w wyniku danych osób trzecich. Polisy obejmują również koszty prowadzenia sporów sądowych z poszkodowanym oraz postępowania regulacyjnego czy też działań związanych z powiadomieniem regulatora i osób, których dane zostały naruszone. Niektóre z ofert na rynku obejmują również nakłady potrzebne na znalezienie przyczyny naruszenia bezpieczeństwa danych, likwidacje zagrożenia oraz środki mające na celu zapobieżenie atakom w przyszłości. Niektórzy oferują również pomoc w odtworzeniu informacji.

Z punktu widzenia RODO bardzo ważną kwestią jest możliwość pokrycia kosztów obsługi prawnej prowadzonej kontroli administracyjnej oraz refundacji samej kary administracyjnej. W przypadku wszczęcia postępowania administracyjnego przez inspektorów Urzędu Ochrony Danych Osobowych ubezpieczenie pokryje koszty prowadzonej obrony prawnej, konsultacji, ewentualnego sporu. Ponadto, jeżeli wystąpi wyciek danych, ubezpieczyciel zapłaci również koszty powiadomienia osób, których informacje zostały ujawnione. Co więcej, jeżeli osoby te zdecydują się złożyć pozew o odszkodowanie, to z polisy będą wypłacone koszty obrony, zasądzone odszkodowania lub zawartej ugody. Jeżeli wizerunek ubezpieczonego uległ nadszarpnięciu to również ubezpieczyciel pokrywa koszty PR. Jeżeli chodzi o koszy polisy to wysokość składki waha się od 0,5 % do 1 % sumy gwarancyjnej w zależności od tego co obejmuje ubezpieczenie oraz od stosowanych systemów ochrony.

Cyberpolisy dopiero podbijają polski rynek. Przedsiębiorstwa powinny jednak rozważyć ich zakup. Pozwoli to uniknąć wielu problemów po wystąpieniu cyberataku. W końcu zarząd powinien pamiętać, że firmy dzielą się na dwie grupy: te które padły ofiarą cyberprzestępców i te które jeszcze o tym nie wiedzą. W dobie RODO i ogromnych kar administracji oraz możliwych pozwów cywilnoprawnych ubezpieczenie cyber jest interesującym narzędziem, którym warto się zainteresować.