CHMURA CHMURZE NIERÓWNA, CZYLI CYBERBEZPIECZEŃSTWO NA NAJWYŻSZYM POZIOMIE

Jeszcze nigdy się nie zdarzyło, by podczas dyskusji o chmurze publicznej nie mówić o cyberbezpieczeństwie. Kilka lat temu wszelkie spory były przez potencjalnych odbiorców ucinane autorytatywnym stwierdzeniem, że chmura jest niebezpieczna, nasze służby bezpieczeństwa są na najwyższym poziomie, korzystamy z najnowszych narzędzi, a kierownictwo nadało sprawie wysoki priorytet.

Od tego czasu zmieniło się wszystko – zagrożenia stały się prawdziwie globalne, wektory ataku coraz bardziej zróżnicowane, użytkownicy mobilni, a dostawcy chmury przenieśli usługi na zupełnie inny poziom bezpieczeństwa. Co więcej, świadomość rozwiązań chmurowych wśród odbiorców także stała się inna. Pojawiło się także kilka regulacji, które wymagają by zarządzanie bezpieczeństwem stało się rozliczalne nie tylko dla własnego kierownictwa, ale także dla zewnętrznego regulatora i audytorów.

Dzisiaj „*cloud*" odmieniany jest przez wszystkie przypadki. Jednak chmura i chmura to nie to samo. Należy od początku odrzucać propozycje skierowane do konsumentów, zwłaszcza kiedy darmowa usługa korzysta z danych użytkownika dla celów reklamowych. W przypadku analizy ofert profesjonalnych rozważania należy zacząć od tego jaka jest szansa odejścia w niebyt dostawcy. Największe światowe firmy często są określane jako „*hyperscalers*", ponieważ utrzymują po kilkaset centrów danych połączonych własnymi podmorskimi kablami, a ich inwestycje w chmurę liczone są w grubych miliardach. Poziom utrzymywanego przez takich dostawców bezpieczeństwa jest porównywalny z najbardziej zaawansowanymi państwami i rządami, a nawet jest zdecydowanie wyższy niż dla dużych organizacji czy mniejszych państw. Wykorzystanie ich usług ma absolutny sens tam, gdzie mówimy o standardowych usługach, typowych procesach informatycznych i standardowych warunkach. Tacy usługodawcy zapewniają wówczas optymalne warunki bezpieczeństwa, liczne narzędzia kontroli i raportowania, a ich klienci mogą mieć pewność, że ich dostawcy będą intensywnie inwestowali w obszar cybersec. Oferują też dodatkowe usługi cyberbezpieczeństwa i supportu. A także przystosowują swoją ofertę do zmieniających się wymagań prawnych i organizacyjnych. To ostatnie jest naprawdę istotne, gdyż obszar IT stał się obiektem licznych regulacji. Jeśli wielki dostawca chmurowy wypełnia kryteria dla Dostawcy Usług Cyfrowych zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa i rozporządzeniem UE 2018/151 – to będzie je dalej spełniał, kiedy te kryteria się zmienią. Czy będą to normy określające bezpieczeństwo fizyczne, zasady przetwarzania, zasady rozliczalności, częstości i profesjonalności audytów czy reguły raportowania incydentów to *hyperscaler* będzie się dostosowywał. Korzystając z jego usług dostajemy „w pakiecie" pewność zgodności i to nie tylko na dzisiaj, ale także na cały czas korzystania z usługi. Nie mamy przy tym wątpliwości, że ustawodawcy będą mocno pracowali nad nowymi regulacjami! Nawet jednak przy korzystaniu z oferty wielkich graczy trzeba sprawdzić i odpowiednio udokumentować, że to na czym nam zależy od strony bezpieczeństwa faktycznie jest nam dane.

Czy to oznacza, że inni gracze chmurowi nie mają racji bytu? Oczywiście nie! Wielcy dostawcy chmurowi mogą obsłużyć wszystkie typowe scenariusze, ale nie są zbyt elastyczni. Podobieństwo do oprogramowania z półki jest uderzające – odnosimy korzyść z tego, że używają go miliony osób na świecie, ale gdyby chcieć specjalnej wersji tylko dla nas to nie mamy szans powodzenia w negocjacjach. Wartość lokalnego dostawcy chmury przejawia się w jego elastyczności, możliwościach dopasowania części technicznej, jak i organizacyjnej oferty do wymagań nawet pojedynczego klienta. Niemniej to właśnie przy takim scenariuszu warto dokonać precyzyjnej analizy potencjalnej upadłości dostawcy, warunków exit planu, a wreszcie – co może zaskakiwać – zabezpieczenia przed vendor lock. O ile bowiem wielcy są nieustannie w świetle reflektorów i jakiekolwiek podejrzenie o siłowe utrzymywanie klientów jest dla nich niszczące, to w przypadku mniejszych i lokalnych dostawców podobna refleksja może nie mieć miejsca. Również kwestie zgodności z wymaganiami formalnymi muszą być weryfikowane znacznie dokładniej niż dla *hyperscalers*, gdyż mniejszym po prostu jest trudniej nadążać i proporcjonalnie kosztuje to ich więcej.

Jeśli zatem zamierzamy wykorzystać chmurę publiczną to na początek należy odrzucić konsumenckie rozwiązania. Następnie warto określić do czego chcemy chmurę stosować i jeśli jest to typowy projekt to rozpocząć analizę rynku od propozycji największych dostawców. Czym jest typowy scenariusz może podpowiedzieć Uchwała Rady Ministrów „Wspólna Infrastruktura Informacyjna Państwa” z 24.09.2019, gdzie w załączniku nr 2 zostały one wymienione. Jeśli wymagania, w tym cybersec, są wyjątkowe to wtedy warto przeanalizować oferty innych dostawców lub zdecydować się na chmurę hybrydową.

Michał Jaworski, Dyrektor Strategii Technologicznej, Microsoft Sp. z o.o.

Materiał powstał we współpracy z Microsoft Sp. z o.o.