Bezpieczeństwo chmury: podziel na dwa

Korzystanie z chmury obliczeniowej nie zwalnia użytkownika usług chmurowych od odpowiedzialności za bezpieczeństwo przetwarzanych danych. Zapewnienie bezpieczeństwa środowiska chmurowego musi być współdzielone przez usługodawcę i usługobiorcę.

W powszechnej świadomości wciąż jeszcze często pokutuje przekonanie, że z chwilą przeniesienia firmowych zasobów do chmury cała odpowiedzialność za ich bezpieczeństwo przechodzi na dostawcę chmury. To jednak nieprawda. Część obowiązków pozostaje nadal po stronie użytkownika usług chmurowych.

Co ciekawe, do wykreowania tego fałszywego wyobrażenia o roli operatorów chmury sami się oni w dużej mierze przyczynili. W kampaniach marketingowych zachęcających do korzystania z usług chmurowych, szczególnie w początkowym okresie rozwoju tego segmentu rynku, mocno podkreślali znaczenie bezpieczeństwa jako jednej z najważniejszych zalet środowiska chmurowego. Dzisiaj coraz częściej zwracają

Andrzej Gontarz
ekspert ds. monitoringu rynku w zespole Sektorowej Rady ds. Kompetencji – Informatyka

uwagę na to, że usługodawca i usługobiorca muszą razem odpowiadać za całościowo rozumiane bezpieczeństwo chmury.

Przekonują się o tym w praktyce sami użytkownicy usług chmurowych.

> *Specjaliści od cyberbezpieczeństwa podkreślają, że chmura stanowi tylko kolejny element firmowego środowiska cyfrowego. Zmienia się lokalizacja serwerów przetwarzających dane, ale nie zmieniają się podstawowe zasady zapewnienia ochrony firmowym zasobom. Firma nie może być zwolniona z tego obowiązku bez względu na rodzaj wykorzystywanych technologii.*

Powszechną praktyką stało się obecnie udostępnianie przez dostawców chmury, takich jak Amazon, Google czy Microsoft, modeli współdzielonej odpowiedzialności (*Shared Responsibility Model*). Określają one zakresy zadań i obowiązków obu stron chmurowej aktywności. Wskazują obszary, za które odpowiada dostawca, i granice, za którymi odpowiedzialność musi już wziąć na siebie klient.

Modele dzielenia odpowiedzialności w chmurze:

Amazon
https://aws.amazon.com/compliance/shared-responsibility-model/

Google
https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate

Microsoft
https://learn.microsoft.com/pl-pl/azure/security/fundamentals/shared-responsibility

Ministerstwo Cyfryzacji
https://chmura.gov.pl/zuch/static/media/SCCO_v_1.00.pdf (str. 16)

National Cyber Security Centre
https://www.ncsc.gov.uk/collection/cloud/understanding-cloud-services/cloud-security-shared-responsibility-model

Zasada współdzielonej odpowiedzialności mówi o podziale obowiązków między usługodawcą a usługobiorcą. Referencyjne modele opracowywane są przez różnego rodzaju organizacje branżowe, jak na przykład Cloud Security Alliance. Stają się one również składnikiem niektórych dokumentów państwowych. Model dzielenia odpowiedzialności zawierają na przykład opublikowane w 2020 r. przez ówczesne Ministerstwo Cyfryzacji „Narodowe Standardy Cyberbezpieczeństwa. Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO)". Wchodzi on też w skład przygotowanego przez brytyjskie National Cyber Security Centre przewodnika „Cloud security guidance".

W zależności od modelu

Szczegółowy podział zakresu odpowiedzialności między operatora a użytkownika chmury publicznej zależy od modelu usługi chmurowej, a także od warunków świadczenia tejże usługi, określonych przez dostawcę w jego modelu współdzielenia odpowiedzialności. Generalnie najmniej obowiązków jest po stronie użytkownika w modelu SaaS (*Software as a Service*), a najwięcej w modelu IaaS (*Infrastructure as a Service*). W przypadku PaaS (*Platform as a Service*) odpowiedzialność rozkłada się w miarę równomiernie na obie strony kontraktu. Nie ma jednak takiej możliwości, żeby w jakiejkolwiek sytuacji użytkownik mógł się pozbyć w pełni odpowiedzialności za bezpieczeństwo wykorzystywanych rozwiązań chmurowych.

Dostawca odpowiada generalnie za zabezpieczenie wszystkiego, co znajduje się i działa w jego centrum danych, którego używa do świadczenia usług. Do jego obowiązków należy zapewnienie bezpieczeństwa wykorzystywanej przez niego infrastruktury chmurowej. Użytkownik odpowiada zaś za wszystko, co w związku z korzystaniem z rozwiązań chmurowych dzieje się w jego środowisku.

Po stronie klienta jest odpowiedzialność za ochronę danych i innych zasobów przechowywanych, przetwarzanych i wykorzystywanych w środowiskach chmurowych. Usługobiorca odpowiada generalnie za procesy korzystania z chmury, za wszystko co się dzieje w jego środowisku, w którym rozwiązania chmurowe są wykorzystywane i z którego dane trafiają do przetwarzania w chmurze.

Dostawcy oferują zazwyczaj wiele różnych możliwości konfiguracji chmury oraz narzędzi do zapewnienia bezpieczeństwa i ochrony środowiska chmurowego. O ich konkretnym wykorzystaniu i sposobie zastosowania decyduje już jednak sam odbiorca. Tylko on jest bowiem w stanie określić obowiązujące w organizacji reguły przetwarzania danych i przypisać zasady korzystania z konkretnych zasobów czy usług do konkretnych pracowników.

W konsekwencji w wielu przypadkach może nie mieć znaczenia, jak dobre zabezpieczenia zastosuje dostawca chmu-

ry, jeśli sam użytkownik nie będzie w stanie we właściwy sposób zabezpieczyć swojego środowiska. Dlatego też powinien dokładnie zapoznać się z usługą, z której korzysta, żeby wiedzieć, jaki jest faktycznie zakres jego odpowiedzialności. Każdy dostawca może bowiem oferować inne rozwiązania, nawet w odniesieniu do tych samych usług. Trzeba je dobrze poznać i zrozumieć, żeby we właściwy sposób przeprowadzić konfigurację środowiska chmurowego.

Użytkownicy odpowiadają za zabezpieczenie kanałów komunikacji i procesów uruchamianych w chmurze. Do ich zadań należy: ochrona danych będących w gestii firmy i aplikacji współpracujących z rozwiązaniami chmurowymi, ochrona stosowanych systemów operacyjnych i sieci, zarządzanie prawami dostępu do aplikacji i danych, zapewnienie integralności przetwarzanych danych czy na przykład szyfrowanie transmisji danych w ruchu sieciowym oraz odpowiedzialność za funkcjonowanie własnej sieci i punktów końcowych, w tym urządzeń mobilnych czy stosowanych w ramach telepracy stanowisk typu home office. Przede wszystkim jednak użytkownik odpowiada za właściwą konfigurację zakupionej usługi chmurowej. Chodzi o przystosowanie jej do wykorzystania, zoptymalizowanie pod kątem własnych warunków, potrzeb i możliwości z zachowaniem wszelkich wymogów i zasad określonych przez dostawcę. Jest to konieczne nawet w przypadku tak prostej, wydawałoby się, aplikacji jak poczta elektroniczna. Zła konfiguracja może narazić firmę i jej zasoby na liczne zagrożenia i niebezpieczeństwa.

Architektura spaja całość

Użytkownik odpowiada za zbudowanie architektury bezpieczeństwa swojego środowiska chmurowego. Powinna ona stanowić integralną część architektury bezpieczeństwa całego firmowego środowiska teleinformatycznego czy – szerzej – cyfrowego. Musi też jednak uwzględniać specyficzne wymagania ochrony zasobów i usług chmurowych.

Działania na rzecz zapewnienia bezpieczeństwa środowiska chmurowego w przedsiębiorstwie najlepiej zacząć jeszcze przed podpisaniem umowy z dostawcą usług chmurowych. Składa się bowiem na nie wiele różnych elementów, które przy tworzeniu architektury bezpieczeństwa należy wziąć pod uwagę – użytkownicy, sieć dostępowa, wykorzystywana infrastruktura, polityka bezpieczeństwa, zarządzanie tożsamością, wymagania prawne itp. Ważne jest dokładne przemyślenie, jak ma wyglądać firmowe środowisko chmurowe – jakie aplikacje czy usługi będzie obejmować, jakie będą zasady korzystania z nich, skąd będą pobierane dane do przetwarzania, z jakimi innymi systemami rozwiązania chmurowe będą się komunikować. Ustalenie priorytetów działania w tych obszarach pozwoli na jak najbardziej świadomy, a w konsekwencji także bezpieczny wybór odpowiednich rozwiązań chmurowych i ich dostawcy.

Zanim się wykupi usługę w chmurze, warto też wiedzieć, co się chce konkretnie przenieść do chmury i przewidzieć tego skutki dla funkcjonowania firmy i jej infrastruktury teleinformatycznej. Trzeba zrobić rozeznanie własnego środowiska, żeby wiedzieć chociażby to, z jakimi innymi systemami aplikacja w chmurze będzie się komunikować, z jakimi będzie wymieniać dane, do jakich może mieć dostęp.

> *Zalecane jest sprawdzenie wykorzystywanej infrastruktury i oprogramowania, aby wiedzieć, co naprawdę nadaje się do efektywnego i jednocześnie bezpiecznego funkcjonowania w chmurze.*

Potrzebna jest także identyfikacja zależności i relacji między różnymi usługami, zasobami i danymi w firmie, żeby w odpowiedni sposób uwzględnić je potem podczas migracji do chmury czy właściwie odwzorować w środowisku chmurowym. Nawet jeśli dotyczy to przeniesienia najprostszych aplikacji czy też o najmniejszym znaczeniu dla funkcjonowania przedsiębiorstwa, to należy w miarę precyzyjnie określić, w jaki sposób są one powiązane z innymi i jakie relacje między nimi należy wziąć pod uwagę przy wdrażaniu usług i rozwiązań chmurowych. Dzięki temu można będzie w jak największym stopniu zoptymalizować usługę i stworzyć odpowiednią architekturę środowiska chmurowego, co stworzy dobre podwaliny pod dalszy jego rozwój i optymalne wdrażanie kolejnych usług chmurowych.

Przy podejmowaniu decyzji o migracji do chmury trzeba też wziąć pod uwagę ryzyka związane z wyjściem z chmury lub przeniesieniem usługi do innego usługodawcy. Czasami jest to trudniejsze i kosztowniejsze niż samo wejście do chmury. Przed przeniesieniem danych do chmury należy więc rozważyć i przeanalizować związane z tymi sytuacjami zagrożenia i ryzyka. Dzisiaj mogą się bowiem wydawać tylko hipotetyczne, ale gdy w przyszłości się zmaterializują, mogą stać się źródłem poważnych problemów i dodatkowych wydatków.

Korzystanie pod kontrolą

W trakcie korzystania z chmury ważne jest natomiast monitorowanie działania wdrożonych usług chmurowych, w tym sposobów korzystania z nich przez pracowników przypisanych do określonych ról i uprawnień. Firma będąca

usługobiorcą powinna sprawdzać na bieżąco, czy wszystko rzeczywiście działa jak należy, zgodnie z założeniami i oczekiwaniami. Do tego może użyć własnych rozwiązań albo narzędzi udostępnianych przez dostawcę chmury lub pochodzących od firm trzecich.

Kiedy już chmura pojawi się w firmie, kluczowe staje się zarządzanie dostępem do usług chmurowych i monitorowanie korzystania z nich. W ustaleniu, kontroli i egzekwowaniu zasad dostępu nikt użytkownika chmury nie zastąpi i nie wyręczy. Do jego obowiązków należy stworzenie kont dostępowych dla pracowników, określenie ról użytkowników końcowych i związanych z tym poziomów uprawnień oraz kryteriów dostępu.

Rolą odbiorcy usług chmurowych jest jak najbardziej precyzyjne określenie: kto, kiedy, na jakich zasadach, w jakich sytuacjach, do jakich celów, z jakich zasobów i usług może korzystać, a następnie monitorowanie i egzekwowanie stosowania się do wprowadzonych zasad. Mimo że dostawcy oferują gotowe, standardowe role użytkowników i poziomy ich uprawnień, to eksperci zachęcają, żeby każda organizacja tworzyła je sama, mając na uwadze własne, specyficzne potrzeby i wymagania.

Trzeba w zasadzie stale sprawdzać, czy ustalone warunki korzystania przez pracowników z usługi chmurowej są respektowane i faktycznie przestrzegane. Do tego celu mogą służyć różne, też powszechnie dostępne systemy zarządzania dostępem, w tym zarządzania dostępem uprzywilejowanym (PAM – *Privileged Access Management*). Przydatne mogą być też systemy zarządzania hasłami czy systemy pojedynczego logowania do firmowych zasobów.

Należy monitorować funkcjonowanie usług sieciowych, żeby wiedzieć, czy wszyscy korzystają z nich prawidłowo, czy nie ma gdzieś zagrożeń i czy w razie potrzeby będzie można odpowiednio zareagować na incydent cyberbezpieczeństwa. Generalnie nie należy przydzielać nadmiernych uprawnień. Optymalny model ról, uprawnień i reguł dostępności powinien być dopasowany do podziału kompetencji w firmie, ale pozwalający też na łatwe i jednocześnie bezpieczne korzystanie z usługi chmurowej. To ułatwi również właściwą jej konfigurację.

Polityka i prawo

Co może pomóc firmie będącej użytkownikiem usług chmurowych w zapewnieniu bezpieczeństwa środowiska chmurowego? Przede wszystkim dobrze przygotowana i faktycznie stosowana w praktyce polityka bezpieczeństwa. Opisane w niej wytyczne i zasady pomogą przy wyborze dostawcy usług chmurowych, a potem ułatwią monitorowanie przebiegu procesu korzystania z chmury.

Polityka bezpieczeństwa ma kluczowe znaczenie dla sprawnego i bezpiecznego korzystania z chmury. Określa bowiem zasady postępowania z zasobami przedsiębiorstwa, w tym reguły posługiwania się systemami teleinformatycznymi służącymi do przetwarzania ważnych dla organizacji danych i informacji. Musi więc obejmować również i rozwiązania chmurowe.

W gruncie rzeczy ważna jest nie tyle sama polityka, co przestrzeganie jej reguł w praktyce i egzekwowanie określonych w niej zaleceń. Nawet najlepiej napisany dokument odstawiony potem na półkę nie spełni swojego zadania. Ważna jest też stała aktualizacja założeń polityki bezpieczeństwa i dostosowywanie wskazanych w niej zasad postępowania do aktualnych warunków, zarówno tych wewnątrz organizacji, jak i na zewnątrz, w całym otoczeniu biznesowym.

W dobrym skonfigurowaniu usług chmurowych mogą pomóc użytkownikowi również regulacje prawne, które w określonych przypadkach wskazują zasady i warunki korzystania przez firmę z chmury obliczeniowej. Z drugiej strony, przepisy i wynikające z nich wymagania mogą też stanowić utrudnienie dla odbiorcy usług chmurowych. Prawo nakłada bowiem w wielu sytuacjach określone obowiązki na użytkownika chmury.

> *Należy pamiętać, że spełnienie wymogów regulacyjnych jest jednym z kluczowych obszarów odpowiedzialności korzystającego z usług chmurowych. Wymagania wynikające z obowiązków prawnych powinny też zostać uwzględnione w projekcie architektury środowiska chmurowego i zapisach polityki bezpieczeństwa.*

W obowiązujących regulacjach prawnych również znajduje odzwierciedlenie omawiana zasada współdzielenia odpowiedzialności za bezpieczeństwo wykorzystywanego środowiska chmurowego. Problem w tym, że na gruncie polskim nie ma jednego uniwersalnego aktu prawnego, który by w sposób całościowy regulował zasady korzystania z chmury i związane z tym kwestie bezpieczeństwa. Poszczególne rozwiązania, przepisy i wymogi są porozrzucane po różnych aktach prawnych. Na dodatek, jedne odwołują się do chmury obliczeniowej wprost, inne – w sposób pośredni. Są wśród nich zarówno ustawy o charakterze ogólnym, jak też i regulacje branżowe.

Usługa cloud computing jest usługą cyfrową, należy więc przy korzystaniu z niej stosować się do regulacji wynikających z ustawy o świadczeniu usług drogą elektroniczną. Trzeba brać pod uwagę również ustawę o krajowym systemie cyberbezpieczeństwa. Obejmuje ona m.in. dostawców usług elektronicznych, do których zaliczeni zostali

także dostawcy usług w chmurze. Przy ochronie danych poufnych zastosowanie będą miały zapisy ustawy o zwalczaniu nieuczciwej konkurencji, która określa zasady ochrony tajemnicy przedsiębiorstwa oraz ustawy o ochronie informacji niejawnych.

Szczególnej ochronie podlegają dane osobowe. Wymagania pod jej adresem określa obowiązujące od 2018 r. unijne Rozporządzenie o ochronie danych osobowych (RODO). Wskazane w nim wymogi odnoszą się nie tylko do administratorów danych osobowych, lecz również do podmiotów, którym administratorzy powierzyli przetwarzania, tych danych, czyli także i do operatorów usług chmurowych.

Wśród regulacji branżowych warto zwrócić uwagę na przepisy dotyczące wykorzystania chmury obliczeniowej w bankach. Zawarte one zostały w ustawie Prawo bankowe. Dodatkowo niektóre aspekty zostały doprecyzowane w wydanej przez Komisję Nadzoru Finansowego Rekomendacji D, dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach.

Dostawcy i użytkownicy usług chmurowych powinni też w swojej działalności uwzględniać też regulacje o charakterze pozaprawnym. Należą do nich wszelkiego rodzaju standardy, normy (w tym normy ISO), rekomendacje oraz zbiory dobrych praktyk. Dookreślają one wskazane na poziomie ustawowym wymagania i zasady korzystania z rozwiązań chmurowych. Swoje standardy chmurowe ma na przykład środowisko radców prawnych i sektor publiczny.

Jak najdokładniejsze ustalenie granic odpowiedzialności przy korzystaniu z usługi chmurowej jest bardzo ważne, bo dostawcę i użytkownika wiąże umowa cywilnoprawna. Na jej podstawie można m.in. dochodzić ewentualnych roszczeń. Tutaj zastosowanie będzie miał kodeks cywilny, o którym również nie należy zapominać w kontekście otoczenia prawnego chmury obliczeniowej.

Potrzebni specjaliści

Na odbiorcy usług chmurowych ciąży więc całkiem sporo obowiązków. Zadaniem użytkownika rozwiązań typu cloud comuting jest dobór odpowiednich usług, ich właściwa konfiguracja oraz zapewnienie bezpieczeństwa i zgodności z regulacjami prawnymi. Do tego potrzebna jest odpowiednia wiedza, umiejętności i kompetencje.

Na polskim rynku obserwowany jest od lat niedobór specjalistów od wdrażania i zarządzania środowiskami chmurowymi. Ich brak jest uznawany za jedną z głównych przeszkód na drodze do szerszego wykorzystania chmury obliczeniowej przez polskie firmy. Zapełnienie tej luki jest tym bardziej trudne, że do korzystania z chmury potrzebne są, jak widać, nie tylko kwalifikacje techniczne, lecz także znajomość kontekstów stosowania technologii chmurowych.

Nowe kwalifikacje

Sektorowa Rada ds. Kompetencji – Informatyka przygotowała propozycje nowych kwalifikacji chmurowych:

- **Projektowanie usług chmurowych w organizacji**
- **Zarządzanie usługami chmurowymi**
- **Zapewnianie cyberbezpieczeństwa rozwiązań chmurowych**

Uwzględniają one w dużej mierze potrzeby kompetencyjne firm z sektora MŚP oraz jednostek samorządu terytorialnego. Złożone zostały wnioski o włączenie tych kwalifikacji do Zintegrowanego Systemu Kwalifikacji.

Osoby legitymujące się tymi kwalifikacjami będą przygotowane do:

- zaprojektowania i wyboru rozwiązania chmurowego adekwatnego do potrzeb organizacji, wdrożenia i monitorowania jego funkcjonowania zgodnie z projektem i wymogami organizacji oraz podejmowania działań dotyczących zabezpieczenia wdrożonych rozwiązań chmurowych.

- Kwalifikacja **Projektowanie usług chmurowych w organizacji** pozwoli m.in. na analizę i porównanie usług chmurowych pod kątem ich funkcjonalności i warunków wdrożenia oraz możliwości zastosowania w konkretnej firmie.

- Pracownik z kwalifikacją **Zarządzanie usługami chmurowymi w organizacji** będzie potrafił zamówić potrzebną usługę chmurową, wdrożyć ją w organizacji i odpowiednio skonfigurować. Będzie także monitorował poprawność jej działania i wykorzystania.

- Kwalifikacja **Zapewnianie cyberbezpieczeństwa rozwiązań chmurowych** będzie potwierdzała m.in. umiejętności identyfikacji wymagań związanych z koniecznością zapewnienia bezpieczeństwa stosowanych rozwiązań chmurowych, wykonania analizy ryzyka oraz wdrożenia odpowiednich narzędzi zabezpieczających.

Zgodnie z wymogami Zintegrowanego Systemu Kwalifikacji opisy zaproponowanych przez Sektorową Radę ds. Kompetencji – Informatyka kwalifikacji chmurowych zawierają zestawy efektów uczenia się oraz wskazania dotyczące warunków walidacji i certyfikacji (metody, zasoby kadrowe, wymagania organizacyjne).