Marcin Krysiński, Przemysław Miller, Anna Pamuła

Uniwersytet Łódzki

Wydział Zarządzania

Katedra Informatyki

e-mail: marcin.krysiniski@gmail.com, przemekm1@op.pl, apamula@wzmail.uni.lodz.pl

Bezpieczeństwo danych osobowych a ryzyko korzystania z publicznej chmury obliczeniowej na przykładzie Microsoft Office 365

Kody JEL: A12, L86, O30, 039

Słowa kluczowe: chmura obliczeniowa, infrastruktura IT, ryzyko

Streszczenie. W artykule podjęto tematykę określenia wpływu usług publicznej chmury obliczeniowej na działalność przedsiębiorstw. Przedstawiono zagadnienia ryzyka, dotyczące zwłaszcza utraty danych, która może mieć dla firmy negatywne skutki ekonomiczne. Analiza ryzyka wynikającego ze stosowania chmury obliczeniowej została zaprezentowana na przykładzie usługi Microsoft Office 365.

Wprowadzenie

Przetwarzanie, dostęp do danych oraz ich szybki i bezpieczny transfer należą do podstawowych potrzeb współczesnych organizacji, w tym także organizacji gospodarczych. Naprzeciw tym potrzebom wychodzą technologie oferowane przez branżę IT, wśród których coraz większe odgrywają usługi chmury obliczeniowej (Krysiński, Miller, 2016).

Chmura obliczeniowa (*cloud computing*) to technologia zapewniająca użytkownikom końcowym natychmiastowy dostęp do zasobów z dowolnego miejsca na świecie, pozwalająca na wykorzystanie zasobów rozproszonych w przestrzeni internetowej w celu wykonania obliczeń bez potrzeby instalowania oprogramowania na swoich komputerach. Obowiązek spełnienia wszystkich wymagań niezbędnych do wykonania usługi leży po stronie dostawców, a co za tym idzie cała złożoność procesu jest przed użytkownikiem ukryta.

Zainteresowanie usługami w chmurze rośnie, ponieważ firmy szukają sposobów na obniżenie kosztów i przeniesienie swoich usług do internetu. Analitycy Gartner Group wskazują, że wydatki na usługi w chmurze publicznej wzrosną o 16% w 2016 roku, osiągając wartość 204 mld USD (Gartner, 2016).

Korzystanie z chmury obliczeniowej nie jest wolne od ryzyka, związanego z naruszeniem danych osobowych, praw autorskich, nieuprawnionym transferem danych, praw cywilnych tak dostawców, jak i odbiorców usługi. Z uwagi na zasięg chmury obliczeniowej ryzyko związane z jej użytkowaniem ma charakter globalny. Dane osobowe podlegają zatem nie tylko ochronie prawa krajowego, europejskiego, ale także prawa międzynarodowego. Powstaje w związku z tym pytanie, na ile korzyści płynące z użytkowania chmury obliczeniowej równoważą ryzyka i straty z nich wynikające (Krysiński, Miller, 2016).

1. Cloud computing – definicje i charakterystyka

Nazwa *cloud computing* jest pewną metaforą. Definicja chmury obliczeniowej wymaga objaśnienia tego, co się za nią kryje. „Chmura” w tym kontekście to zwrot określający internet, a jej kształt wykorzystuje się często w celu przedstawienia internetu na diagramie sieci, ilustrując jej infrastrukturę, sprzęt i oprogramowanie. Barry Sosinski napisał bardzo ogólnie, że chmura obliczeniowa dotyczy aplikacji i usług działających w sieci rozproszonej za pomocą zwirtualizowanych zasobów obliczeniowych oraz na podstawie połączonych zasobów fizycznych, podzielonych według potrzeb oraz udostępnionych przez wykorzystanie protokołów internetowych i standardów sieciowych (Sosinski, 2011). Pierwszą definicję opracował Ian Foster, twierdząc, że chmura obliczeniowa to „napędzany efektem skali model obliczeniowy dystrybuowany na wielką skalę, w którym połączone abstrakcyjne, zwirtualizowane, dynamicznie zmienne i administrowanie platformy, usługi, moc obliczeniowa i zdolność przechowywania dostarczane są na żądanie klientów przez Internet” (Foster, Zhao, Raicu, Lu, 2008). Według definicji opracowanej przez Jeffa Kaplana chmura obliczeniowa to „obszerna matryca usług sieciowych, których celem jest umożliwienie użytkownikom pozyskania szerokiej gamy możliwości funkcjonalnych na zasadzie «płać za to, z czego korzystasz»”. Kolejną, obszerniejszą definicję stworzył Mohan. Według niego chmura obliczeniowa to „przełomowy model technologiczno-biznesowy polegający na wykorzystaniu rozproszonych dużych prywatnych, publicznych lub hybrydowych centrów danych, które oferują klientom skalowalną, zwirtualizowaną infrastrukturę lub zestaw abstrakcyjnych usług, bazujący na umowie o gwarantowanym poziomie usług (SLA), w którym płaci się tylko za wykorzystane zasoby informatyczne” (Buyya, Broberg, Goscinski, 2010).

Pałka zdefiniował chmurę obliczeniową „jako wszelakiego rodzaju usługi dostępne z poziomu rozległej sieci internetowej” (Pałka, Zaskórski, Zaskórski, 2013), bądź też jako „styl obliczeń, w którym dynamicznie skalowane zasoby informatyczne (zwykle zwirtu-

alizowane) są dostarczane zewnętrznym użytkownikom w postaci usług sieciowych na żądanie. Użytkownik nie musi ani wiedzieć, w jaki sposób ta usługa jest realizowana, ani też nie musi zajmować się aspektami technicznymi niezbędnymi do działania” (Pałka Zaskórski, Zaskórski, 2013). Co więcej, ze swoim urządzeniem, korzystającym z chmury obliczeniowej nie musi być wcale blisko. Wystarczy, gdy będzie z nią (chmurą obliczeniową) skomunikowany. Na tę okoliczność zwraca się uwagę w najczęściej przywoływanej w literaturze definicji chmury obliczeniowej, autorstwa Narodowego Instytutu Norm i Technologii Stanów Zjednoczonych (National Institute of Standards and Technology – NIST). Chmurą obliczeniową w świetle tej definicji jest „sposób dostępu poprzez sieć komputerową do współdzielonych i łatwo konfigurowalnych zasobów obliczeniowych (sieci, serwerów, magazynów danych, aplikacji i usług), które na żądanie, dynamicznie, mogą być przydzielane i zwalniane, przy równoczesnym minimalnym zaangażowaniu serwisów technicznych” (Czerwonka, Lech, Podgórski, 2011; Pazowski, 2014).

Według amerykańskiego NIST można wyróżnić, pięć zasadniczych cech chmury:

- samoobsługowe usługi na żądanie (*on-demand self-service*),
- szeroki dostęp do sieci,
- współdzielenie zasobów,
- szybka elastyczna rozbudowa,
- pomiar wykorzystania usług.

Oraz cztery modele świadczonych usług:

- IaaS – infrastruktura jako usługa (*infrastructure as a service*),
- PaaS – platforma jako usługa (*platform as a service*),
- SaaS – oprogramowanie jako usługa (*software as service*).

NIST w swoim dokumencie zdefiniował również cztery następujące modele chmury:

- chmura prywatna (*Private cloud*),
- chmura współdzielona (*Community cloud*),
- chmura publiczna (*Public cloud*),
- chmura hybrydowa (*Hybrid cloud*) (Mell, Grance, 2010).

Zadaniem IaaS jest dostarczanie wirtualnych maszyn, wirtualnej przestrzeni, wirtualnej infrastruktury oraz innych zwirtualizowanych zasobów obliczeniowych. Dostawca usług IaaS zarządza całą infrastrukturą, a klient odpowiada za wszelkie pozostałe aspekty rozwiązania, w tym systemy operacyjne i aplikacje. Przykładami dostawców usług IaaS są Amazon Elastic Compute Cloud (EC2), czy GoGrid.

Zadaniem PaaS jest dostarczanie wirtualnych maszyn, systemów operacyjnych, aplikacji, usług, schematów rozwoju, struktur transakcji i kontroli. Klient może dokonać rozmieszczenia aplikacji w infrastrukturze chmury lub skorzystać z aplikacji opracowanych za pomocą języków programowania i narzędzi wspieranych przez dostawcę PaaS. Dostawca zarządza infrastrukturą chmury, systemami operacyjnymi i oprogramowaniem, klient natomiast odpowiada za instalację i obsługę rozmieszczonych aplikacji

(Sosinski, 2011). Przykłady dostawców usług PaaS to Google AppEngine czy Zoho Creator.

SaaS to pełne środowisko operacyjne wraz z aplikacjami, zarządzaniem i interfejsem użytkownika. W modelu SaaS dostawca odpowiada za wszystko od aplikacji do infrastruktury, klient jedynie korzysta z aplikacji, otrzymuje dostęp do danych, może nimi zarządzać (Sosinski, 2011). SaaS jest modelem dystrybucji, który dostarcza przez internet aplikacje często nazywane usługami internetowymi. Microsoft Office 365 jest rodzajem SaaS oferującym pakiety biurowe i usługi e-mail. Użytkownicy mają dostęp do aplikacji i usług SaaS z dowolnej lokalizacji.

2. Cloud computing – korzyści, wyzwania, ryzyko

Najważniejsze korzyści płynące z wykorzystania chmury obliczeniowej związane są z jej głównymi cechami (abstrakcja, virtualizacja, skalowalność, użyteczność). Barrie Sosinski (2011) określił jej pięć głównych zalet:

- usługi na żądanie – klient ma dostęp do usług bez potrzeby kontaktowania się z personelem dostawcy,
- szeroki dostęp do sieci – dostęp do zasobów odbywa się przez sieć, za pomocą standardowych metod i w sposób, który pozwala na korzystanie z nich wszystkim użytkownikom, niezależnie od platformy,
- łączenie zasobów – zasoby zebrane są w systemie, który może być wykorzystywany przez wielu użytkowników,
- natychmiastowość i elastyczność – z zasobów można korzystać w sposób elastyczny dostępny natychmiast po uruchomieniu/zakupie usługi,
- pomiar usług – klienci rozliczają się na podstawie mierzalnych danych, takich jak przestrzeń, liczba transakcji, szerokość pasma.

Inne korzyści związane z usługami w chmurze to m.in. szeroki wachlarz aplikacji, których zastosowanie nie wymaga pobierania ani instalacji, niższe koszty, łatwość w obsłudze, jakość usług określonych w umowie, zarządzanie zasobami informatycznymi zlecone na zewnątrz, uproszczona konserwacja i ulepszanie, dostęp do aplikacji z dowolnego komputera za pomocą internetu, skalowalność (poprzez zasoby dostępne na żądanie), model płatności za bieżące wykorzystanie.

Na gruncie zarządzania ryzykiem definiuje się jako „skumulowany efekt prawdopodobieństwa niepewnych zdarzeń, które mogą korzystnie lub niekorzystnie wpłynąć na realizację projektu”. Generalnie więc ryzyko może być funkcją zdarzeń losowych, ludzkich błędów, albo też na poziomie najbardziej ogólnym, funkcją zmieniającej się nieuchronnie rzeczywistości, na których przebieg działające podmioty nie mają żadnego wpływu.

Przy każdej zmianie wprowadzonej w środowisku IT, warto wykorzystać idee zarządzania ryzykiem, definiowanym jako funkcja prawdopodobieństwa (tj. szansa, że jakiś niepożądany efekt pojawi się dla danej liczby zdarzeń lub zasobów) oraz wielkości

(tj. konsekwencjami związanymi z tym efektem). W zarządzaniu ryzykiem infrastruktury IT, prawdopodobieństwo niepożądanego efektu przekłada się na prawdopodobieństwo włamania. Jeśli nie ma żadnych zmian w sposobie używania systemów, zagrożenie wzrasta proporcjonalnie wraz ze wzrostem źródeł aktywności (np. połączeń) i tak samo zagrożenie maleje wraz z odpowiadającym mu spadkiem połączeń. W odniesieniu do lokalizacji lub systemu docelowego, podatność wzrasta proporcjonalnie wraz z liczbą rozmieszczanych zasobów (np. serwerów, aplikacji). Poprzez obserwację zarówno zagrożeń, jak i podatności oraz stosowanie odpowiednich środków technicznych, zarządzający ryzykiem może usunąć lub zminimalizować zagrożenia i ocenić zmianę w kwestii zagrożeń i podatności, niezależnie od tego, czy środowisko istnieje wewnątrz organizacji czy w chmurze.

Warto zauważyć, że każda firma, która rozbudowuje swoje zasoby informatyczne, zwiększa możliwość wystąpienia ryzyka. Taka jest natura ryzyka – im większa ilość zasobów i większe użycie, tym więcej firma może stracić. Tak więc najprężniejsze, nastawione na rozwój firmy to te, w których ryzyko wzrasta najszybciej. Jednym z bardziej wymagających aspektów oceny tego rodzaju ryzyka jest porównanie środków bezpieczeństwa obecnie używanych w organizacji ze środkami oferowanymi dla usług oferowanych „w chmurze”.

Architektura chmury sprawia, że firmom łatwiej tworzyć modele bezpieczeństwa które wykorzystują następujące możliwości:

1. Silniejsza separacja – więcej współdzielonych zasobów oznacza większą potrzebę silniejszej segmentacji. W konwencjonalnym centrum danych taka separacja może wymagać dużej ilości zasobów a wiele firm wierzy, że ryzyko jest ograniczone. Architektura chmury wymusza separację poszczególnych aplikacji.
2. Wprowadzenie szyfrowania – ze względu na skomplikowanie istniejących wewnątrz organizacji środowisk wiele firm świadomie rezygnuje z szyfrowania. Przejście do chmury w naturalny sposób wymusza włączenie szyfrowania, co w znaczący sposób podnosi bezpieczeństwo.
3. Silniejsze uwierzytelnianie – przedsiębiorstwa nadal często silnie ograniczają swoje możliwości wielopoziomowego uwierzytelniania. Przejście do chmury wymusza stworzenie mechanizmów ograniczenia swobodnego dostępu do danych i przyznawania określonych uprawnień tylko określonym użytkownikom.
4. Silniejsze logowanie zdarzeń i monitoring – w wielu firmach, ze względu na brak zasobów nie monitoruje się na bieżąco działania systemów. Jedną z cech chmury jest dostęp do szczegółowego monitorowania systemów.

3. Prywatność i bezpieczeństwo danych

Analitycy zajmujący się zagadnieniami związanymi z chmurą obliczeniową często podkreślali, że największe zagrożenie z nią związane dotyczy zapewnienia poufności i bezpieczeństwa danych. Technologia chmury wykorzystuje bardzo wiele infrastruktur i usług świadczonych przez osoby trzecie. Nie da się zatem uniknąć problemu bezpieczeństwa i prywatności danych wrażliwych przesyłanych za pomocą aplikacji w chmurze – środowisko chmury nie jest tak bezpieczne jak wewnętrzne systemy informatyczne. Ważne jest zaufanie wobec dostawców usług w chmurze. Ponadto procedury bezpieczeństwa, takie jak szyfrowanie danych, protokoły dostępu, metody agregacji danych oraz metody kasowania informacji po zakończeniu świadczenia usług to kluczowe techniki mające na celu zapewnienie bezpieczeństwa danych (Buyya, Broberg, Goscinski, 2011).

Według sondażu przeprowadzonego przez IDC, obawy dotyczące bezpieczeństwa są najważniejszym czynnikiem hamujący przejście technologii oraz usług do chmury (50% respondentów), na drugim miejscu znalazła się niezawodność (33%), a na trzecim – zgodność z przepisami prawa (30%) (Lindstrom, 2014).

Zasadą jest, że konsumenci korzystający z usług w chmurze nie mogą całkowicie polegać na dostawcach w kwestii ochrony danych prywatnych. Bezpieczeństwo danych i komunikacji to nie tylko problem technologiczny, ale również polityczny. Przykładem może być sytuacja z 2010 roku, gdy firma Google uznała, że chińscy dysydenci znaleźli się w niebezpieczeństwie po tym, jak chiński rząd wykorzystał technologię firmy w celu nadzoru politycznego. Firma Google zdecydowała, że wycofa swoje serwery z Hongkongu (Sosinski, 2011). Innym przykładem jest amerykańska organizacja wywiadowcza – Narodowa Agencja Bezpieczeństwa (NSA). Podejrzewa się, że agencja zapłaciła „setki milionów dolarów amerykańskim firmom za utajniony dostęp do ich sieci komunikacyjnych, co pozwoliło na filtrowanie ogromnych strumieni ruchu dla kierunków zagranicznych w procesie, który objął wiele połączeń telefonicznych, e-maili i wiadomości Amerykanów” (Timberg, Gellman, 2013). Dokumenty NSA, które wyciekły dzięki Edwardowi Snowdenowi (byłemu pracownikowi NSA) świadczą o tym, że dobrowolna współpraca pomiędzy NSA i dostawcami usług komunikacyjnych na świecie rozpoczęła się już w latach 70. XX wieku (Timberg, Gellman, 2013). Gdyby informacje o tym działaniu ujawniono, podobne umowy pomiędzy agencjami wywiadowczymi i dostawcami usług komunikacyjnych na świecie mogłyby gigantów przemysłu technologicznego i firmy świadczące usługi w chmurze (np. Google, Microsoft, IBM, Yahoo, Twitter, Facebook) kosztować miliardy dolarów. Fakt ten może ograniczać zamiary dostawców usług komunikacyjnych na świecie do naruszania prywatności danych. Fundacja ITIF (Information Technology & Innovation Foundation) oraz zespół ekspertów z siedzibą w Waszyngtonie opublikowali raport, w którym podano, że w związku z przeciekami ujawniającymi współpracę z agencjami wywiadowczymi, dostawcy usług w chmurze mogą do 2016 roku stracić nawet 35 mld USD (Gustin, 2014; Landau, 2014).

4. Ochrona danych osobowych w chmurze

Zobowiązania klientów i dostawców usług typu *cloud computing* do ochrony danych w dużym stopniu zależą od ról przydzielonych im w danym stosunku prawnym na mocy DPD (*Data Protection Directive* – Dyrektywa o ochronie danych). Jeżeli dane bądź ich fragment można uznać za dane osobowe w rozumieniu DPD i są one przetwarzane w chmurze, wówczas przynajmniej jedna z tych osób musi być administratorem danych. W rozumieniu DPD administratorem danych jest osoba, która „określa cele i sposoby przetwarzania” (Dyrektywa 95/46/WE Art.2 par. d).

W przypadku usług Google Apps for Work, Microsoft Office 365 i podobnych im rozwiązań SaaS, sytuacja jest odmienna. To oczywiste, że dane przetwarzane za pomocą tych usług wystarczą do zidentyfikowania poszczególnych użytkowników, przez co trzeba je uznać za dane osobowe w rozumieniu DPD. Można więc przyjąć, że korzystanie z tych usług stanowi przetwarzanie danych w rozumieniu DPD, przy czym klient usługi w chmurze jest administratorem danych, zaś dostawca tejże usługi – przetwórcą danych (Baltatescu, 2014).

Taki przydział ról stawia wiele wymogów odnośnie do stosunku prawnego pomiędzy dostawcą usługi a jej klientem. Pierwszym i najistotniejszym z nich jest istnienie aktu prawnego regulującego stosunki pomiędzy klientem usługi w chmurze, jako administratorem danych, a dostawcą tejże usługi jako przetwórcą danych (Dyrektywa 95/46/WE Art.7 par. 3). Choć DPD nie określa rodzaju takiego aktu, w ustawodawstwie wielu krajów wymaga się, by przyjmował on postać umowy (Data Protection Act 1998 Schedule 1, part II, par. 12). Umowa ta (zazwyczaj nazywana umową o przetwarzanie danych albo umową o powierzenie przetwarzania danych) powinna mieć formę pisemną bądź inną równoważną formę (Dyrektywa 95/46/WE Art. 17 par. 4).

Drugim kluczowym obowiązkiem dostawcy usług w chmurze, który musi zostać zawarty w umowie, jest obowiązek przestrzegania uzgodnionych środków technicznych i organizacyjnych wprowadzonych w celu ochrony danych osobowych (Dyrektywa 95/46/WE Art.6 par. 1 i 3). DPD nie określa konkretnych środków, jakie trzeba wprowadzić w życie celem ochrony danych osobowych. Istnieje jednak kilka krajowych wdrożeń, które wymieniają określone wymogi albo środki przeznaczone dla różnych profili ryzyka, np. w Hiszpanii i w Polsce (Rozporządzenie..., 2004, art. 6, par. 2; Spanish Data Protection Act, art. 80). Umowa o przetwarzanie danych powinna też dostarczyć klientowi narzędzia umożliwiające nadzór nad przestrzeganiem przez dostawcę powyższych środków. Powinna także dostarczyć środki zaradcze na wypadek sytuacji, w której obowiązek przestrzegania zostałby złamany (WP196, supra note 6).

Dostawca usług w chmurze powinien być zobowiązany do dostarczenia klientowi tych usług wystarczających dowodów przestrzegania wspomnianych środków, w postaci np. świadectwa bezpieczeństwa albo raportu z audytu, np. ISO 27001 albo nowej normy dotyczącej przetwarzania informacji identyfikujących osobowo w chmurze – ISO 27018.

Ostatni kluczowy element wymagany w umowie o przetwarzanie danych jest związany z miejscem przechowywania przetwarzanych danych. Bez informacji o miejscu przechowywania danych, klient usługi w chmurze nie może być pewien czy spełniony jest wymóg dotyczący transgranicznego przepływu danych osobowych. Dane osobowe można przysyłać poza granice UE jedynie do krajów zapewniających odpowiedni poziom ochrony ustalony decyzjami Komisji Europejskiej (Dyrektywa 95/46/WE Art. 25).

5. Microsoft Office 365

Podstawowe przepisy regulujące stosunek prawny są zawarte w umowie subskrypcyjnej usługi Microsoft Online – *Microsoft Online Subscription Agreement*, tzw. umowa MOS (Microsoft, 2014) i w informacji o polityce prywatności (Microsoft, 2015), na które klient przystaje, gdy wykupuje płatną wersję usługi. Najważniejszym dokumentem, na który powołuje się umowa MOS są postanowienia dotyczące Usług Online – *Online Services Terms* – tzw. postanowienia OS (Microsoft, 2016), w których szczegółowo opisano warunki świadczenia usług online, w tym usługi Office 365.

Umowa MOS jest zawierana z Microsoft Ireland Operations Limited (firmą Microsoft). Podstawy umowy o przetwarzaniu danych regulowane są przez podsekcję „Dodatkowe postanowienia europejskie” postanowień OS, w której stwierdzono, że firma Microsoft jest przetwórcą danych działającym w imieniu klienta i że będzie działać jedynie na polecenie klienta. W kwestii celu przetwarzania danych, w postanowieniach OS podano, że „Dane Klienta będą używane wyłącznie w celu świadczenia Klientowi Usług Online, w tym w celach powiązanych ze świadczeniem tych usług” (Microsoft, 2016). Kategorie przetwarzanych danych określa się jako „adresy e-mail, dokumenty i inne dane w formie elektronicznej w kontekście Usług Online” (Microsoft, 2016). Zakres poleceń klienta podany jest jedynie w umowie MOS oraz w postanowieniach OS (Microsoft, 2016).

Postanowienia OS opisują środki bezpieczeństwa wdrożone przez firmę Microsoft. Opis ten jest ogólny, ale obejmuje wiele obszarów (Microsoft, 2016). Rozważając argumenty na rzecz wdrożenia wspomnianych środków, należy zauważyć, że firma Microsoft udostępni klientowi swoją politykę bezpieczeństwa spełniającą normy ISO 27001 oraz 27002 i podda owe zabezpieczenia audytowi przeprowadzonemu przez niezależny podmiot posiadający odpowiednie kwalifikacje. Na życzenie klienta firma udostępni mu podsumowanie sprawozdania z audytu (Microsoft, 2016).

Umowa MOS nie upoważnia klienta do rozwiązania umowy za samo tylko naruszenie zobowiązań przez firmę Microsoft. Jednak nawet klient, który wykupił subskrypcję długoterminową, może zrezygnować z usługi z uzasadnionej przyczyny z zachowaniem miesięcznego okresu wypowiedzenia. Przysługuje mu wówczas prawo do zwrotu pieniędzy za pozostały okres subskrypcji (Microsoft, 2014). Ponadto, na mocy klauzuli 5, lit. b) Załącznika 3 do postanowień OS, klient ma prawo do rozwiązania umowy z powodu nieprzestrzegania przez firmę poleceń klienta albo standardowych

klauzul umownych wydanych przez Komisję Europejską. Odpowiedzialność firmy Microsoft za szkody spowodowane naruszeniem przez nią zobowiązań wynikających z umowy MOS jest ściśle ograniczona (Microsoft, 2014). Firma jest też zwolniona od odpowiedzialności za pewne rodzaje szkód (Microsoft, 2014). Ograniczenia te sprawiają, że istotna część ciężaru odpowiedzialności za osobę, której dane dotyczą, spoczywa na kliencie.

Umowa MOS ani postanowienia OS nie zezwalają na dokonywanie zmian bez zgody drugiej strony. Zmiany w umowie można wprowadzić jedynie po jej wygaśnięciu – za pośrednictwem odpowiedniej procedury jej przedłużenia (Microsoft, 2014).

Akceptując postanowienia umowy MOS, klient zgadza się także na korzystanie przez firmę Microsoft z usług podwykonawców. Każda umowa podwykonawcza będzie zawierać postanowienia zabezpieczające co najmniej w takim stopniu, jak sekcja „Ponstanowienia dotyczące przetwarzania danych” postanowień OS, zaś firma Microsoft będzie informować klienta o każdym nowym podwykonawcy uczestniczącym w procesie świadczenia usług z co najmniej czternastodniowym wyprzedzeniem. Klienci mogą zrezygnować z usługi podczas tego okresu, jeżeli nie aprobują nowego podwykonawcy (Microsoft, 2016).

Firma Microsoft zobowiązuje się usunąć dane klienta w ciągu 90 dni od rozwiązania umowy o świadczenie usługi (Microsoft, 2016). Jest też zobowiązana do zapewnienia klientowi możliwości korekty, usuwania lub blokowania przetwarzanych danych lub do przeprowadzania takich korekt, usunięć czy blokad w jego imieniu (Microsoft, 2016).

Firma Microsoft gwarantuje, że będzie przechowywać najbardziej poufne fragmenty danych klientów z UE w obrębie tego regionu (Microsoft, 2016). Jeśli natomiast chodzi o pozostałe dane, ma i pozostanie w posiadaniu certyfikatu programu „bezpiecznych przystani”, a w Załączniku 3 do postanowień OS znajdują się standardowe klauzule umowne wydane przez Komisję Europejską. Klauzule nie są w żaden sposób zmodyfikowane. Jeśli zaś chodzi o możliwe sprzeczności z klauzulami umowy MOS lub postanowień OS, problematyczną kwestią może być audyt usług. W postanowieniach OS podano, że klient wyraża zgodę na skorzystanie ze swojego prawa do audytu wynikającego ze standardowych klauzul umownych w taki sposób, że zleca firmie Microsoft przeprowadzenie audytu za pośrednictwem niezależnego podmiotu z odpowiednimi kwalifikacjami w dziedzinie bezpieczeństwa, jak wyjaśniono wcześniej. Klient ma jednak prawo do zmiany tego polecenia (Microsoft, 2016).

Umowa użytkowania usługi Microsoft Office 365 nie jest też wolna od pewnych uchybień, a konkretniej od ścisłego ograniczenia odpowiedzialności, które dotyczy nawet szkód spowodowanych naruszeniem prawa o ochronie danych. Okres wyprzedzenia, w którym firma Microsoft musi powiadomić o nowym podwykonawcy jest dość krótki. Ponadto, reguły dotyczące praw do audytu znajdujące się w postanowieniach OS mogą stać w sprzeczności ze standardowymi klauzulami umownymi.

Podsumowanie

Usługi chmury odgrywają coraz ważniejszą rolę w sektorze oprogramowania i na rynku usług. Z powodu ich niepodważalnych zalet – dostępności cenowej, łatwego dostępu do informacji, zlecenia zarządzania systemami informatycznymi na zewnątrz, obniżenia kosztów – wiele firm z prawie wszystkich branży zdecydowało się na korzystanie z publicznej chmury obliczeniowej.

Pomimo wielu zalet chmura publiczna ma również pewne wady, np. ryzyko związane z zapewnieniem poufności i bezpieczeństwem danych w chmurze i brak interoperacyjności pomiędzy platformami chmury (Krysiński, Miller, 2016A). W przypadkach, w których dostawca usług w chmurze przetwarza dane, np. w przypadku rozwiązań typu SaaS, stosunek prawny pomiędzy dostawcą a klientem usługi w chmurze musi być uregulowany umową. W umowie takiej muszą znaleźć się takie elementy, jak: zapis mówiący, że dostawca jest związany poleceniami klienta; zakres poleceń klienta; cel przetwarzania i rodzaje przetwarzanych danych. Ponadto umowa musi zawierać opis środków bezpieczeństwa, metody kontroli przestrzegania przez dostawcę tych środków oraz środki zaradcze na wypadek ich nieprzestrzegania. Umowa nie może zezwalać na jednostronne dokonywanie zmian w jej zasadniczych postanowieniach i musi regulować korzystanie z usług podwykonawców przez dostawcę.

Bibliografia

- Article 29 Data Protection Working Party (2012). Opinion 05/2012 on Cloud Computing (WP196). Pobrano z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf (14.05.2016).
- Baltatescu, I. (2014). Cloud Computing Services: Benefits, Risks and Intellectual Property Issues. *Global Economic Observer*, 230.
- Buyya, R., Broberg, J., Goscinski, A.M. (red.) (2010). *Cloud computing: principles and paradigms* (vol. 87). USA: John Wiley & Sons.
- Czerwona, P., Lech, T., Podgórski, G. (2011). Chmura obliczeniowa. *Acta Universitatis Lodzensis, Folia Oeconomica*, 261.
- Data Protection Act 1998 (UK Data Protection Act).
- Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.
- Gustin, S. (2014). *NSA Spying Scandal Could Cost U.S. Tech Giants Billions*. TIME.com. Pobrano z: business.time.com/2013/12/10/nsa-spying-scandal-could-cost-u-s-tech-giants-billions/ (14.05.2016).
- Jonson, B. (2008). Cloud computing is a trap, warns GNU founder Richard Stallman. *The Guardian*. Pobrano z: <https://www.theguardian.com/technology/2008/sep/29/cloud.computing.richard.stallman> (14.05.2016).

- Foster, I., Zhao, Y., Raicu, I., Lu, S.Y. (2008). Cloud computing and grid computing 360-degree compared. W: *Proceedings of the Grid Computing Environments Workshop (GCE'08)*. Austin, TX.
- Gartner (2013). *Forecast: Public Cloud Services, Worldwide, 2014–2020, 1Q16 Update*. Gartner. Pobrano z: <https://www.gartner.com/doc/2642020/forecast-public-cloud-services-worldwide> (14.05.2016).
- Krysiński, M., Miller, P. (2016). Cloud Computing – szansa i ryzyko dla firmy. *Ekonomiczne Problemy Usług*, w druku.
- Krysiński, M., Miller, P. (2016A). Cloud computing – a risk or an opportunity for business. *World Scientific News*, 48.
- Landau, S. (2014). Highlights from making sense of Snowden, part II: What's significant in the NSA revelations. *Security & Privacy, IEEE*, 12 (1).
- Lindstrom (2014). *Assessing the Risk: Yes, the Cloud Can Be More Secure Than Your On-Premises Environment*. IDC White Paper, IDC, Framingham.
- Mell, P., Grance, T. (2011). *The NIST definition of cloud computing*. NIST Special Publication, Gaithersburg.
- Microsoft (2014). *Microsoft Online Subscription Agreement*. Pobrano z: [https://www.microsoft.com/online/mosa/MOSA2014Agr\(NA\)\(ENG\)\(Nov2014\)\(HTML\).htm](https://www.microsoft.com/online/mosa/MOSA2014Agr(NA)(ENG)(Nov2014)(HTML).htm) (14.05.2016).
- Microsoft (2015). *Privacy Notice*. Pobrano z: <https://www.microsoft.com/online/legal/v2/?docid=18&langid=en-UK> (14.05.2016).
- Microsoft (2016). *Online Services Terms*. Pobrano z: <http://www.microsoft.com/volumelicensing.com/Downloader.aspx?DocumentId=10408> (14.05.2016).
- Pałka, D., Zaskórski, W., Zaskórski, P. (2013). Cloud computing jako środowisko integracji usług informatycznych. *Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki*, 9.
- Pazowski, P. (2014). Ekonomiczne aspekty wdrożenia modelu cloud computing. *Modern Management Review*, XIX (April–June).
- Rozporządzenie Ministra spraw wewnętrznych i administracji Dz. U. z 2004 r., nr 100, poz. 1024, w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
- Sosinski, B. (2011). *Cloud Computing Bible*. Indianapolis: Wiley Publishing, Inc.
- Spanish Data Protection Act sets security measures for low, medium and high level of protection, Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Timberg, C., Gellman, B. (2013). NSA paying U.S. companies for access to communications networks. *The Washington Post*, 29.08.2013. Pobrane z: www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html (14.05.2016).

RISKS ASSOCIATED WITH THE USE OF PUBLIC CLOUD BASED ON THE MICROSOFT OFFICE 365 EXAMPLE

Keywords: computing, SaaS, PaaS, IaaS, IT infrastructure, risk

Summary. This paper presents an impact of public cloud computing services on business. The article points out the risks associated with the use of the public cloud computing. The major concerns is a loss of data, which may bring the adverse economic consequences for the enterprises. The analysis of risk is conducted on the basis of Microsoft Office 365. It is estimated that the benefits from the use of services provided by cloud computing overcome the risks.

Translated by Marcin Krysiński

Cytowanie

Krysiński, M., Miller, P., Pamuła, A. (2017). Bezpieczeństwo danych osobowych a ryzyko korzystania z publicznej chmury obliczeniowej na przykładzie Microsoft Office 365. *Ekonomiczne Problemy Usług, 1* (126/2), 93–104. DOI: 10.18276/epu.2017.126/2-10.