ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 798 STUDIA INFORMATICA NR 34 2014

Piotr Fulmański
Sebastian Wojczyk
Uniwersytet Łódzki

CHMURA DZISIAJ – DOBRE MIEJSCE DLA BIZNESU?

Streszczenie

W medialnym szumie, jaki powstał wokół technologii chmury, i wobec marketingowej konieczności oferowania usług opartych na tej technologii, mało osób zadaje sobie pytanie o to, czy warto i czy jesteśmy na to gotowi. Czy istnieją odpowiednie podstawy prawne i standardy techniczne zapewniające jakość działania i świadczenia usług w chmurze? Jak w rzeczywistości ma się świat reklam usługodawców technologii chmury i firm ją wykorzystujących do tego, co faktycznie mogą w tej chwili zaoferować? Czy aby nie jest to bańka mydlana – z pozoru piękna, bo kolorowa, ale tak delikatna, że może prysnąć w każdej chwili, a w raz z nią dane naszej firmy i klientów. W artykule poszukujemy odpowiedzi na pytanie, czy chmura jest dziś odpowiednim miejscem dla biznesu.

Słowa kluczowe: chmura, prywatność danych, bezpieczeństwo danych

Wprowadzenie: chmura

Różnorodny pod względem technologicznym, koncepcyjnym i aplikacyjnym świat komputerowy przypomina trochę zestaw naczyń (tajemniczo) połączonych. Zmiany czy rozwój jednej z gałęzi wywiera wpływ na pozostałe, choć zwykle trudno ocenić, które, w jaki sposób i kiedy. Dynamiczny rozwój gier komputerowych pociągnął za sobą niesłychanie szybki rozwój urządzeń przyspieszających tworzenie grafiki, co w efekcie przekształciło się w zupełnie nowy sposób przeprowadzania obliczeń typu HPC (ang. *High-performance Computing*) z wykorzystaniem właśnie kart graficznych [na przykład architektura CUDA (ang. *Compute Unified Device Architecture*) (www2) czy framework OpenCL]. Podobnie rozwój sieci komputerowych przyczynił się do powstania internetu – dzięki niemu zmianie uległ sposób prowadzenia biznesu, a w chwili obecnej także i postrzegania paradygmatów związanych z modelem przetwarzania danych, dostępem do aplikacji

i jej zasobów. Modelem tym jest chmura (ang. *cloud computing*). Model chmury historycznie wiąże się z przetwarzaniem w sieci (tzw. grid). Celem technologii gridowej było stworzenie z bardzo dużej liczby połączonych, niejednorodnych systemów współdzielących różnego rodzaju zasoby prostego w użytkowaniu, ale potężnego, biorąc pod uwagę zasoby, jednego wirtualnego komputera. Tak więc grid stanowił rozwinięcie idei klastra poza tradycyjne granice domeny. Sama nazwa – chmura obliczeniowa – w języku polskim wydaje się kiepską kalką językową – nie chodzi tutaj bowiem tylko o obliczenia, ale raczej całe spektrum związane z ogólnie rozumianym przetwarzaniem danych. W modelu tym zakłada się użytkowanie usług (na przykład aplikacji, danych) z dowolnego miejsca i całej gamy urządzeń (telefon, tablet, cienki klient, komputer typu desktop itd.), przy czym usługi zlokalizowane są „gdzieś" w internecie. Stąd też nazwa modelu, która wzięła się ze sposobu przedstawiania internetu na diagramach sieci komputerowych właśnie pod postacią chmury.

Co ciekawe, usługi działające w podobnej technologii, a więc oparte na globalnej technologii gwarantującej dostęp z dowolnego miejsca na świecie, funkcjonują już od dawna. Wystarczy choćby wymienić usługę poczty elektronicznej, komunikatory czy repozytoria. Tak więc z punktu widzenia odbiorcy końcowego – użytkownika pracującego przy użyciu danej usługi – chmura nie różni się od tego, z czym działał do tej pory. Można by powiedzieć, że jest to chwyt marketingowy i z pewnością w wielu przypadkach tak jest. Z technicznego punktu widzenia chmura oparta jest na zupełnie innych założeniach, które nie koniecznie przekładają się na sposób jej postrzegania przez użytkowników, ale istotnie wpływają na sposób zarządzania usługami w niej działającymi. To z kolei rodzi obszerną klasę zagadnień, które są całkowicie nowe i wymagają opracowania odpowiednich procedur i ram prawnych.

1. Przeznaczenie chmury

W zależności od potrzeb i posiadanej już infrastruktury oraz wielkości firmy usługa *cloud computing* może być świadczona w trzech odmianach (Serafinowicz 2011; www1): jako chmura prywatna (ang. *private cloud*), publiczna (ang. *public cloud*) lub łączona (ang. *hybrid cloud*).

Chmura prywatna określa firmową (prywatną) strukturę informatyczną, która dostarcza usługi IT dla określonej liczby użytkowników chronionych wspólnym systemem zabezpieczeń, i zarządzana jest przez przedsiębiorstwo, w którym funkcjonu-

je. Mówiąc inaczej, chmury prywatne to takie, w których odbiorcą usług jest jedna firma. Biorąc pod uwagę jedynie niezbędną infrastrukturę chmura taka niczym się nie różni od własnej serwerowni. Postęp w wirtualizacji i rozpraszaniu zasobów sprawia, że administratorzy systemów IT w największych korporacjach mogą w efektywny sposób stać się dostawcami usług spełniających oczekiwania użytkowników IT wewnątrz danej korporacji. Posiadanie własnej chmury wiąże się z inwestycją w:

a) sprzęt i infrastrukturę – w przypadku istniejących firm sprzęt zwykle już jest, więc co najwyżej wymaga odświeżenia lub zaadaptowania do nowej specyfiki wykorzystania;
b) specjalne oprogramowanie: systemowe (na przykład do zarządzania zasobami i maszynami wirtualnymi) oraz aplikacyjne.

Ponieważ chmura prywatna już na starcie jej tworzenia wymaga inwestycji kapitału (sprzęt, oprogramowanie, koszty zarządzania), dlatego w organizacjach, w których początkowe znaczące nakłady na IT nie są pożądane, nie wydaje się ona dobrym rozwiązaniem. Alternatywą może okazać się chmura publiczna.

Chmura publiczna (czasem nazywana też chmurą zewnętrzną dla odróżnienia od chmury prywatnej działającej wewnątrz jednej organizacji) to model przetwarzania danych oparty na przekazywaniu realizacji usług zewnętrznemu dostawcy, przy równoczesnym dzieleniu zasobów z innymi użytkownikami. Podstawowe korzyści korzystania z chmury zewnętrznej to:

a) minimalne nakłady związane z uruchomieniem – koszty maszyn, aplikacji i działania są pokrywane przez dostawcę usługi;
b) skalowalność według potrzeb, a więc nie ma przypadków niedoinwestowania lub przeinwestowania w infrastrukturę; o ile niedoinwestowanie nie jest problemem, gdyż braki można zawsze uzupełnić, to przeinwestowanie zwykle wiąże się z konkretnymi stratami finansowymi;
c) ponieważ użytkownik płaci tylko za to, czego używa, to stosunek poniesionych nakładów do wykorzystania sprzętu jest niezwykle korzystny. W tym przypadku można powiedzieć, iż zasoby użytkowane są w 100%, co rzadko się zdarza, gdy korzystamy z własnego zaplecza IT.

Istnieją sytuacje, gdy technologia chmury publicznej może sprawdzić się doskonale:

a) okresowość zapotrzebowania na wydajność dostępnego środowiska IT lub względnie mała częstotliwość jego występowania;
b) niewystarczające możliwości przetwarzania danych przez istniejącą w organizacji infrastrukturę IT przy jednoczesnym braku możliwości jej rozbudowy czy to ze względów finansowych, czy czasowych;

c) czasowe korzystanie z oprogramowania bez konieczności zakupu drogich bezterminowych licencji; w chwili obecnej taką usługę oferuje na przykład Adobe w oparciu o Adobe Creative Cloud, gdzie dostęp do najnowszych aplikacji rozliczany jest w okresach miesięcznych i nie jest wymagana ciągłość zobowiązania.

W dalszej części artykułu, pisząc o chmurze, zwykle będziemy mieli na myśli właśnie chmurę publiczną jako tę, która najbliższa jest ogólnej idei chmury, czyli nieokreślonego miejsca, gdzie przetwarzane są dane.

Trzeci model, chmura hybrydowa, stanowi połączenie dwóch poprzednich modeli: wydajnej, sprawnie działającej chmury publicznej i zapewniającej wymagany poziom bezpieczeństwa i prywatności chmury prywatnej. Oznacza to środowisko chmury, w którym firma dostarcza zasoby wewnątrz organizacji i zarządza nimi, a inne usługi są jej udostępniane przez zewnętrznego dostawcę. W praktyce takie połączenie polega zwykle na korzystaniu z chmury publicznej na poziomie aplikacji, ale trzymaniu danych (na przykład danych klientów) we własnej bazie.

Z punktu widzenia potencjalnego odbiorcy usług najważniejszym jest, aby:

a) właściwie zrozumiał udostępniane funkcjonalności chmury, zdawał sobie sprawę z możliwych do zrealizowania aplikacji i ograniczeń;
b) dokonał właściwego i obiektywnego porównania z realnymi potrzebami i posiadanymi już tradycyjnymi rozwiązaniami IT.

To, co jest dobre dla jednej firmy, niekoniecznie musi takie być dla innej. Chmura publiczna może być dobrym rozwiązaniem dla małych firm, które nie chcą ponosić kosztów związanych z utrzymaniem działów IT. W chwili obecnej większe organizacje nie są zainteresowane przenoszeniem swoich rozwiązań do chmury publicznej (Suchta, 2011). Z chmur prywatnych mogą korzystać (i korzystają) duże firmy, które z pewnych względów (bezpieczeństwa, prawnych itp.) nie mogą przetwarzać danych poza własną siedzibą. Wydaje się, że najpopularniejszy w najbliższym czasie będzie model hybrydowy, który daje największą elastyczność, a jednocześnie pozwala pozbyć się znacznej liczby problemów, z którymi wykorzystanie chmury się wiąże (zostaną one opisane w dalszej części).

2. Charakterystyka chmury obliczeniowej

Usługi oparte na chmurze, choć działające za pomocą sieci, w istotny sposób różnią się od tradycyjnego modelu usług sieciowych (Raport, 2012a; Raport, 2012b).

a) sprzęt zapewniający działanie usługi jest własnością dostawcy usług w chmurze, a nie użytkownika, który uzyskuje dostęp do chmury za pośrednictwem internetu;

b) dostawcy usług w modelu chmury często przenoszą dane i aplikacje użytkowników (na przykład między różnymi komputerami lub między różnymi centrami przetwarzania danych) w celu optymalnego wykorzystania dostępnego sprzętu;
c) wykorzystanie sprzętu jest dynamicznie zoptymalizowane za pomocą sieci współdziałających komputerów, tak że użytkownik w zasadzie nie musi znać dokładnej lokalizacji danych lub procesów ani wiedzieć, który sprzęt w danym momencie faktycznie obsługuje tego użytkownika – **może to jednak mieć istotne znaczenie dla mających zastosowanie ram prawnych**;
d) urządzenia, na których działa chmura, **pozostają poza fizyczną kontrolą użytkowników**, a ich rozmieszczenie przestrzenne (lokalizacja) może być różnorodne i geograficznie rozproszone;
e) użytkownicy zwykle płacą za to, z czego korzystają, unikając dużych stałych kosztów początkowych, związanych z samodzielną konfiguracją i eksploatacją zaawansowanego sprzętu komputerowego;
f) jednocześnie użytkownicy mogą bardzo łatwo zmienić zasoby, z których korzystają (na przykład liczbę procesorów czy dostępną pamięć).

Niestety, zalety chmury podawane są równie często jako jej wady. Z powyższej charakterystyki widać, że stosowanie chmury rodzi ważne pytania odnośnie do zasad związanych z tym, jak ludzie, organizacje czy nawet instytucje rządowe przetwarzają dane, a dokładniej, co się z nimi w chmurze dzieje, jaką mamy nad tym kontrolę i czy rzeczywiście kontrolę mamy.

3. Wątpliwości związane z prowadzeniem działalności biznesowej w chmurze

Z punktu widzenia możliwości prowadzenia działalności biznesowej najważniejsze kwestie związane z ewentualną decyzją o wykorzystaniu chmury wiążą się z ochroną prywatności i bezpieczeństwem. Prywatność (poufność) w nierozerwalny sposób powiązana jest z zagadnieniami bezpieczeństwa. Bezpieczeństwo stanowi fundament działania wszelkiego rodzaju usług, ale to właśnie zasady prywatności decydują o tym, czy danym rozwiązaniom zaufają klienci detaliczni, duży biznes w postaci korporacji lub instytucje państwowe. Wszystkie rodzące się w tym zakresie wątpliwości sprowadzić można do dwóch aspektów (Brodkin; Hölbl, 2011; Raport, 2009):

– obawy utraty kontroli nad danymi,
– praktycznie całkowitej zależności od dostawcy chmury.

W ramach dwóch powyżej wymienionych grup najczęściej dyskutowane są następujące zagadnienia:

1. Dane przechowywane w chmurze zagrożone są ujawnieniem zarówno przez niepożądane działania dostawcy chmury, jak i innych użytkowników. Nie ma jasności co do tego, jak, kiedy, dlaczego i gdzie dane są przetwarzane i składowane. Sama deklaracja usługodawcy związana na przykład z szyfrowaniem naszych danych nie wystarcza. Użytkownik musi mieć pewność, że taka operacja istotnie została wykonana. Sposobem na to są certyfikacje i audyty, choć nawet wtedy całkowitej pewności mieć nie można.
2. Jak wiadomo, najsłabszym ogniwem we wszelkiego rodzaju zabezpieczeniach zwykle jest człowiek. Przez swoje umyślne lub nie działanie potrafi bardzo szybko uczynić bezużytecznym lub obejść najwymyślniejsze systemy zabezpieczeń. Naturalne jest więc pytanie o dobór kadry obsługującej infrastrukturę IT chmury, procedury sprawowania nad nią kontroli, zakres jej uprawnień i odpowiedzialności.
3. Kiedyś zwykło się mówić, iż światem rządzi pieniądz. Dziś światem rządzi informacja. Dostęp do odpowiednich danych w odpowiednim czasie pociągać za sobą może konkretne skutki finansowe, biznesowe, polityczne itd. Dostawca chmury ma potencjalne możliwości wykorzystania technik eksploracji danych na powierzonych mu danych. Działanie to, samo w sobie, nie niesie dla nikogo bezpośredniego zagrożenia, ale może zagwarantować przewagę informacyjną dostawcy nad konkurencją, a to już może przekładać się na konkretne straty/zyski. Może także stać się silną kartą przetargową (na przykład nieujawnianie odkrytych danych w zamian za konkretne korzyści). Ujawniony przez Edwarda Snowdena program PRISM polegający na monitorowaniu na szeroką skalę kont pocztowych, połączeń VoIP i danych z serwisów społecznościowych jest potwierdzeniem realności tego zagrożenia. Zagrożenia tym bardziej prawdopodobnego, że użytkownicy, wierząc w reklamę i siłę marketingową chmury, mogą bez zastanowienia powierzać jej, całkowicie dobrowolnie, najprzeróżniejsze dane.
4. Chmura, przez swoją wszechobecność, daje złudzenie lokalności działań. Wymieniając na przykład kontakty pomiędzy dwoma telefonami znajdującymi się obok siebie, dane fizycznie transmitowane są przez chmurę, a więc narażone są na opisane wcześniej zagrożenia. Jeśli nawet je pominiemy, to zawsze mamy do czynienia z uzależnieniem funkcjonowania pewnej usługi od dostępu do chmury. Nietrudno wyobrazić sobie aplikację działającą na telefonie,

a służącą na przykład do obróbki zdjęć czy filmów. Zadania te ze względu na znaczne zapotrzebowanie na moc obliczeniową fizycznie realizowane mogą być „gdzieś w chmurze", a użytkownik obserwuje jedynie efekt końcowy. Problemem jest to, że korzystając z takiej aplikacji, można nie mieć świadomości tego procesu. Co więcej, wraz z tym, jak urządzenia i oprogramowanie stają się coraz bardziej przyjazne, świadomość tego, co i gdzie się dzieje z danymi, będzie się zmniejszała.

5. Chmura z założenia jest usługą zdalną. Tak więc oprócz użytkownika i dostawcy w procesie transmisji danych bierze udział także trzecia strona – dostawca usług sieciowych (internetowych). Jest to kolejny element niepewności dotyczący bezpieczeństwa i jakości usług.
6. Często podaje się, iż bazowanie na zdalnych usługach jest wygodne choćby dlatego, że ciężar posiadania odpowiedniej mocy obliczeniowej przeniesiony jest na usługodawcę. Użytkownikowi wystarczy tylko tak zwany cienki klient czy wręcz telefon. Rzadko zaś wspomina się o kluczowym wymaganiu, jakim jest odpowiednia przepustowość łączy czy wręcz dostępność do jakiegokolwiek łącza. Najlepiej widać to na przykładzie sieci telefonii komórkowej, w przypadku której pomimo zapewnień operatorów bez problemu można znaleźć miejsca, w których internet nie będzie dostępny.
7. Tradycyjnie pojmowane zarządzanie ryzykiem w przypadku chmury jest znacząco utrudnione lub wręcz niemożliwe.
8. Ponieważ sprawowanie technicznej kontroli nad danymi leży po stronie dostawcy, dlatego niezmiernie ważne jest wiarygodne rejestrowanie jego działań i weryfikacja ich przez niezależne audyty. Do informacji w ten sposób otrzymanych musi mieć dostęp użytkownik.
9. Wbrew pozorom także usuwanie danych z chmury jest tak samo trudnym zadaniem (w zakresie kontrolowalności tego procesu i jego wykonalności), jak zapewnienie ich istnienia. Kopie mogą być pofragmentowane i rozproszone geograficznie, a całkowite usunięcie danych (aby zabezpieczyć je przed jakąkolwiek możliwością odczytu) trudne do zweryfikowania.
10. Z usuwaniem danych wiąże się także jeszcze jeden problem. Otóż urządzenia masowe wykorzystywane w chmurze, jak wszystkie urządzenia, z pewnością będą podlegały awariom. Zastąpienie egzemplarza uszkodzonego nowym nie stanowi obecnie problemu (działanie dysków w macierzach, wymiana w locie itp.). Kłopotem może być zapewnienie (a raczej dopilnowanie usługodawcy), aby uszkodzony element został bezpowrotnie zniszczony. Na przykład dysk,

który nie działa z powodu awarii kontrolera, nadal ma zapisane na talerzach dane. Istnieje potencjalne niebezpieczeństwo odczytu takich danych. Teoretycznie trudno sobie wyobrazić, aby ktoś przeszukiwał złomowiska w poszukiwaniu dysków, a następnie próbował odczytać zawarte na nich informacje – zadanie to jest jeszcze trudniejsze niż znalezienie igły w stogu siana, ale zgodnie z prawami Murphy'ego sytuacja taka będzie miała miejsce w praktyce szybciej, niż ktokolwiek się tego spodziewa, a jej skutki będą poważniejsze, niż nam się wydaje.

11. Ustawodawstwo dotyczące prywatności i ochrony danych cechuje się dużym zróżnicowaniem w różnych krajach. Niezwykle istotne jest więc, w jaki sposób rozumieć bezpieczeństwo i prywatność w globalnej usłudze. Jakie regulacje będą miały zastosowanie, gdy użytkownik znajduje się w innym kraju niż składowane są jego dane, a do tego sam usługodawca nie pochodzi z żadnego z nich? Co w przypadku, gdy dane użytkownika składowane będą w dwóch różnych krajach? **Na te pytania chwilowo nie ma odpowiedzi**.
12. Użytkownik prowadzący swoją działalność (biznesową) w chmurze może stanąć przed nie lada problemem w przypadku zawieszenia działalności przez usługodawcę. Może się wówczas zdarzyć, że z dnia na dzień **zostanie pozbawiony wszystkich swoich danych wraz z możliwością prowadzenia jakiejkolwiek działalności**.
13. Istnieje bardzo duże ryzyko uzależnienia klienta od wykorzystywania chmury oferowanej przez pewnego usługodawcę. Przenosząc działalność do chmury, mamy (a raczej dopiero będziemy mieć w przyszłości ze względu na obecny brak stosownych rozwiązań, o czym dalej) możliwość wyboru konkretnej oferty. Istnieje jednak obawa, że po jej zaakceptowaniu i wywiązaniu się z wszelkich postanowień umowy (na przykład czas obowiązywania umowy) możemy mieć znaczne trudności na przykład z rezygnacji z takiej usługi lub zmiany usługodawcy. I niekoniecznie musi to wynikać z jego złej woli, co ze znacznych trudności technologicznych z tym związanych. Potencjalna różnorodność stosowanych rozwiązań jest ogromna, co może wiązać się z koniecznością konwersji danych, zmiany platformy aplikacyjnej itp. i narazić użytkownika na koszty, stratę czasu, a w najgorszym razie na bezpowrotną utratę pewnych zasobów. W takiej sytuacji należy się spodziewać, iż użytkownicy niechętnie rozważać będą zmianę usługodawcy, pozostając w całkowitej zależności od niego.

W (Raport, 2009) przedstawiono pogląd na kwestę bezpieczeństwa, według którego to usługobiorca chmury, a nie dostawca odpowiedzialny jest za wła-

ściwe zabezpieczenie swoich dokumentów. Według tego stanowiska, chmura to bardzo duża przestrzeń magazynowa, w której sami musimy zatroszczyć się o nasze dane. Porównana została do sytuacji, w której firma wynajmuje powierzchnię magazynową. Mimo że ktoś inny może być właścicielem budynku, dostęp do umieszczonych w nim dokumentów i korzystanie ze znajdujących się w nich informacji nadal regulowane są przez politykę firmy, która wynajmuje przestrzeń. Te same zasady powinny mieć zastosowanie w chmurze. Pytanie, czy nakład pracy i kosztów, jaki będzie z tym związany – a zapewne nie będzie mniejszy niż przy tradycyjnych, przetestowanych i co najważniejsze, działających poprawnie rozwiązaniach wdrożonych już w istniejącej firmie – zostanie zrównoważony przez zalety chmury, jak na przykład jej skalowalność. Rodzi się więc pytanie o opłacalność tej operacji.

Opisane wątpliwości i obawy rodzą się w sposób naturalny u potencjalnych użytkowników i nie pozostają niezauważone (Raport, 2012b): „Celem kilku spośród zaplanowanych działań jest rozwianie wątpliwości wielu potencjalnych użytkowników chmury obliczeniowej związanych z postrzeganiem przez nich tej technologii jako niosącej dodatkowe ryzyko. Działania te ukierunkowane są na zwiększenie przejrzystości i pogłębienie wiedzy na temat obowiązujących ram prawnych, ułatwiając powoływanie się na zgodność z ramami prawnymi i weryfikację tej zgodności (np. poprzez normy i certyfikację), oraz obejmują dalsze rozwijanie ram prawnych (np. poprzez planowane inicjatywy ustawodawcze w odniesieniu do bezpieczeństwa cybernetycznego). (…) Aby zbudować zaufanie do rozwiązań w modelu chmury obliczeniowej, konieczne jest wykonanie całego szeregu ukierunkowanych na to działań. Po pierwsze, należy ustalić odpowiednie normy, których spełnienie może być potwierdzone certyfikatem, tak aby publiczni i prywatni nabywcy mieli pewność, że wprowadzając usługi w modelu chmury obliczeniowej, wywiązali się ze swoich obowiązków związanych z przestrzeganiem przepisów oraz że otrzymują odpowiednie rozwiązanie spełniające ich potrzeby. Wspomniane normy i certyfikaty z kolei mogą zostać uwzględnione w warunkach umownych, tak aby dostawcy i użytkownicy mieli pewność, że umowy są uczciwe. (…) wskazano na potrzebę stworzenia szczególnych ram dla chmur obliczeniowych zarówno w odniesieniu do norm i certyfikacji, jak i warunków umownych".

W chwili obecnej chmura jest zbyt młodą koncepcją, aby można sobie było pozwolić na prowadzenie (częściowo lub w całości) działalności biznesowej. Odpowiednie regulacje w tym zakresie dopiero powstają. W 2012 roku nakreślono pierwszy zarys strategii związanej z wykorzystaniem potencjału chmury obliczeniowej w Europie (Raport, 2012b). Do końca 2013 roku Komisja Europej-

ska zobowiązała się przedłożyć sprawozdanie na temat poczynionych postępów w odniesieniu do wszystkich podjętych już działań i przedstawić dalsze inicjatywy dotyczące wniosków politycznych i ustawodawczych. W ciągu kolejnych dwóch lat mają zostać stworzone podstawy do tego, by Europa stała się światową siłą napędową w dziedzinie chmur obliczeniowych. Poczynienie właściwych postępów zapewnić ma stabilną podstawę dla szybkiego upowszechnienia w Europie technologii chmur obliczeniowych w latach 2014–2020.

Z biznesowego punktu widzenia istotne jest to, że „pomimo rosnących obaw dotyczących prywatności w chmurze, **wciąż brak jest odpowiednich standardów**. W celu wsparcia zastosowań opartych o chmurę standardy określać będą wymagania dotyczące oceny i wyboru rozwiązań spełniających oczekiwany poziom bezpieczeństwa i prywatności. Prace nad standardami są obecnie w toku" (Raport, 2012a).

Tak więc realne wykorzystanie chmury w biznesie dzisiaj jest raczej wątpliwe i ryzykowne. Korzystanie z jej usług traktowane jako wyznacznik nowoczesności, ma bardziej wydźwięk marketingowy niż praktyczny. Z pewnością warto prowadzić prace przygotowawcze pozwalające firmie na skorzystanie z chmury, gdy ta osiągnie odpowiedni stopień dojrzałości. Dokumenty takie jak (Hölbl, 2011) czy (Jansen, Grance, 2011) wyraźnie formułują i akcentują niebezpieczeństwa związane z chmurą. Zawierają także zestaw „dobrych praktyk", których należy przestrzegać przy dokonywaniu wyboru usługodawcy. Jak czytamy w podsumowaniu (Jansen, Grance, 2011): „Przejście do outsourcingu, środowiska chmury jest w wielu aspektach ćwiczeniem w zakresie zarządzania ryzykiem. Zarządzanie ryzykiem wiąże identyfikację i ocenę ryzyka oraz podejmowanie kroków w celu zmniejszenia go do akceptowalnego poziomu. **Ocena i zarządzanie ryzykiem w chmurze może być wyzwaniem**".

Podsumowanie

Chmura nie jest rewolucją w operowaniu informacją, ale raczej efektem ewolucji. Zwykli użytkownicy w wielu przypadkach nie zauważą jej wprowadzenia w firmie. Wykorzystanie technologii chmury może przynieść pewne korzyści ekonomiczne, a z czasem, gdy zostaną wypracowane odpowiednie normy (techniczne, prawne) i zasady ich certyfikacji, będzie ich zapewne więcej i staną się łatwiej dostrzegalne. Jednakże w obecnej sytuacji, biorąc pod uwagę liczne wątpliwości w zakresie prywatności, a także bezpieczeństwa czy natury prawnej, należy uczciwie powiedzieć, iż dojrzałość biznesowa tej koncepcji nie jest

wystarczająca, aby zrównoważyć ryzyko związane z oparciem działalności organizacji czy firmy tylko na niej. W chwili obecnej trudno wyobrazić sobie duże przedsiębiorstwo zlecające obsługę IT zewnętrznym kontrahentom i opierające się wyłącznie na *cloud computingu*.

Bibliografia

Brodkin J., Gartner, *Seven Cloud-computing Security Risks*, www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853 (2.03.2014).

Hölbl M. (2011), *Cloud Computing Security and Privacy Issues*, CEPIS LSI SIN (10)02, Version V17/15.03.2011.

Jansen W., Grance, T. (2011), *Guidelines on Security and Privacy in Public Cloud Computing*, Draft NIST (National Institute of Standards and Technology, U.S. Department of Commerce) Special Publication, Draft Special Publication 800-144, January 2011.

Raport (2009), *Privacy in the Cloud Computing Era. A Microsoft Perspective*, Microsoft Whitepaper, November 2009.

Raport (2012a), *Privacy in Cloud Computing*, ITU-T Technology Watch Report, March 2012.

Raport (2012b), *Wykorzystanie potencjału chmury obliczeniowej w Europie*, Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Bruksela, 27.09.2012, COM(2012) 529 final.

Serafinowicz A. (2011), *Cloud computing, czyli chmury obliczeniowe. Nie błądzić w chmurach*, http://pclab.pl/art44389.html (2.03.2014).

Suchta A. (2011), *Chmura musi mieć fundament*, http://www.crn.pl/artykuly/wywiady/chmura-musi-miec-fundament?searchterm=chmura%20 musi%20mie%C4%87%20 fundament (7.03.2014).

www1: *Chmura prywatna, publiczna a może hybrydowa?*, http://computingcloud.pl/pl/cloud-przewodnik/219-chmura-prywatna-publiczna-a-moze-hybrydowa (2.03.2014).

www2: http://www.nvidia.pl/object/cuda-parallel-computing-pl.html (2.03.2014).

IS THE CLOUD COMPUTING A RIGHT PLACE FOR BUSINESS?

Summary

In the medial turmoil around the cloud computing, or even more: the marketing necessity to offer cloud-based services, only a few people are asking if it is worth and whether we are ready for it. Are there adequate legal basis and technical standards to en-

sure quality of service and the provision of services in the cloud? How the world of cloud technologies providers and companies that use it could be compared to what they really can offer at the moment? Isn't it a one more soap bubble – colorful, but so delicate that it can be broken at any time and with it data of our company and customers. In the article we seek for the answer to the question whether the cloud is today a good place for business.

Translated by Piotr Fulmański

Keywords: cloud computing, data privacy, data security

Informacja o autorach:

Piotr Fulmański, dr, Uniwersytet Łódzki, Wydział Matematyki i Informatyki, Katedra Analizy Matematycznej i Teorii Sterowania, fulmanp@math.uni.lodz.pl.

Sebastian Wojczyk, dr, Uniwersytet Łódzki, Wydział Matematyki i Informatyki, Katedra Analizy Matematycznej i Teorii Sterowania, wojczyk@math.uni.lodz.pl.