Ekonomiczne Problemy Usług nr 1/2017 (126), t. 2

ISSN: 1896-382X | www.wnus.edu.pl/epu
DOI: 10.18276/epu.2017.126/2-13 | strony: 125–134

Artur Rot
Uniwersytet Ekonomiczny we Wrocławiu
Wydział Zarządzania, Informatyki i Finansów
Katedra Systemów Informacyjnych
e-mail: artur.rot@ue.wroc.pl

Wyzwania bezpieczeństwa danych i usług w modelu *cloud computing*

Kody JEL: M15, O33
Słowa kluczowe: *cloud computing*, bezpieczeństwo, prywatność, uwierzytelnienie
Streszczenie. Cloud computing (CC), jak większość nowoczesnych rozwiązań w obszarze IT, może dostarczyć organizacjom wiele korzyści, jednak usługi w chmurze nie są całkowicie pozbawione wad i niosą ze sobą pewne ryzyka. Główne zagrożenia i podatność są związane z obszarami uwierzytelniania, bezpieczeństwa i prywatności danych oraz dostępności i ciągłości działania systemu. Wśród tych czynników ryzyka, bezpieczeństwo i prywatność stanowią najistotniejszy obszar. Celem artykułu jest zaprezentowanie CC z perspektywy bezpieczeństwa danych i usług, a w szczególności wskazanie najistotniejszych wyzwań stojących przed stosowaniem tego modelu.

Wprowadzenie

W ostatnich latach biznes, a w szczególności stosowane w nim technologie informacyjne uległy radykalnej zmianie i trzy nowe aspekty ich rozwoju zupełnie zmieniają tradycyjne podejście do zarządzania. Te trzy nowe zjawiska to: przetwarzanie w chmurze, rozwiązania mobilne i media społecznościowe. Cloud computing należy obecnie do najszybciej rozwijających się usług informatycznych, bazuje, korzysta lub rozwija takie rozwiązania jak: wirtualizacja (*Virtualisation*), przetwarzanie sieciowe (*Grid Computing*), przetwarzanie autonomiczne (*Autonomic Computing*) i architektura zorientowana na usługi (*Service-Oriented Architecture*). Głównym argumentem za wdrażaniem CC w firmach są względy ekonomiczne. Rozwiązanie to może sprzyjać obniżeniu kosztów działalności gospodarczej, zapewnić dostęp do większych mocy obliczeniowych oraz

niesie inne korzyści, co sprzyja wzrostowi popularności tego modelu zarządzania zasobami IT. CC ma wiele zalet, ale stoi przed nim wiele wyzwań, gdyż jego stosowanie nie jest wolne od zagrożeń. Najczęściej przywołuje się w tym miejscu kwestę prywatności i bezpieczeństwa danych oraz dostępności oraz ciągłości działania usług.

Niniejszy artykuł ma na celu zaprezentowanie cloud computingu jako modelu wykorzystującego najnowsze technologie IT oraz wskazanie najważniejszych wyzwań dotyczących bezpieczeństwa danych i usług związanych z implementacją takiego modelu dostarczania usług IT w dobie wirtualizacji organizacji.

1. Koncepcja modelu *cloud computing*

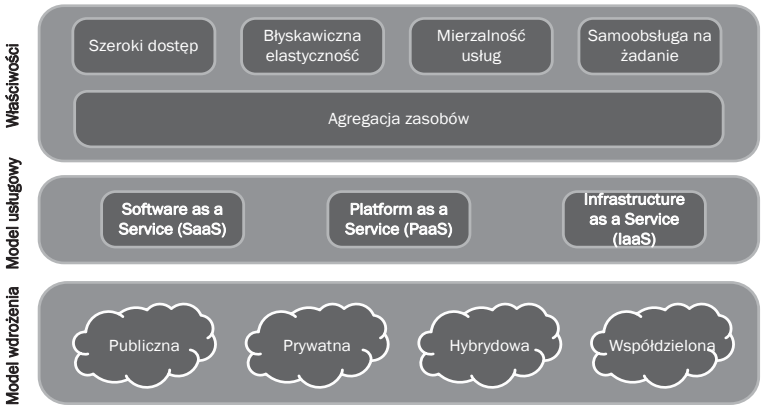
Termin „cloud computing" jest pojęciem dość nowym, bywa definiowany w różny sposób, dlatego nie istnieje jego jedna, ogólnie przyjęta definicja. Na przykład Vaquero (2008) przedstawia aż 22 współcześnie obowiązujące definicje chmury. Chmura obliczeniowa jest pojęciem, które zostało użyte po raz pierwszy w 1996 roku przez Gillet i Kapora (1996). Chellapa (1997) już w 1997 roku przyjął, że CC to paradygmat przetwarzania, mówiący o tym, że granice zarządzania informacjami wynikają z uzasadnienia ekonomicznego, a nie z ograniczeń technicznych.

Jedna z najbardziej dokładnych i kompletnych definicji *cloud computingu* została zaproponowana przez amerykański National Institute of Standards and Technology (NIST). Zgodnie z nią (Badger, Grance, Patt-Corner, Voas, 2011): „cloud computing to model umożliwiający powszechny i wygodny dostęp na żądanie za pomocą sieci do współdzielonej puli konfigurowalnych zasobów teleinformatycznych (np. serwerów, pamięci masowych, aplikacji, platform, sieci) oraz ich szybkie pozyskanie i wydanie przy minimalnym wysiłku i interakcji z dostawcą modelu".

W niniejszym artykule zdefiniowano przetwarzanie w chmurze przez określenie pięciu istotnych jej cech, trzech modeli usług oraz czterech modeli rozmieszczenia usług (zob. rys. 1). Jako cechy chmury wymieniono następujące właściwości (Fronczak, 2013):

1. Szeroki dostęp (*Broad Network Access*) – zasoby IT są dostępne przez istniejące mechanizmy, smartfony, laptopy, komputery oraz aplikacje.
2. Błyskawiczna elastyczność (*Rapid Elasticity*) – zasoby w chmurze powinny być możliwe do wykorzystania w dowolnej ilości i w dowolnym czasie (możliwość skalowania infrastruktury w dowolnym czasie).
3. Mierzalność usług (*Measured Service*) – zasoby mogą być monitorowane, kontrolowane i raportowane, dostarczając przejrzystości zarówno dla dostawcy, jak i odbiorcy usługi. Kryteria mierzalności zasobów to np.: moc obliczeniowa, pamięć, przepustowość, ilość przestrzeni dyskowej.
4. Samoobsługa na żądanie (*On-Demand Self-Service*) – klient może jednostronnie skorzystać z oferowanych zasobów zgodnie ze swoimi potrzebami, w sposób zautomatyzowany, bez interakcji z dostawcą.

5. Agregacja zasobów (*Resource Pooling*) – usługi w modelu chmury osiągają efekt dźwigni i skali poprzez agregację zasobów w obrębie wspólnej infrastruktury, koncepcja ta znana pod nazwą współdzielenia (*multi-tenancy*) rozdziela zasoby pośród wielu różnych klientów, stosując separację i mechanizmy kontrolne w celu zapobiegania mieszania się danych.



Rysunek 1. Model chmury według National Institute of Standards and Technology (NIST)
Źródło: opracowanie własne na podst. Mell i Grance (2011).

W powyższym modelu uwzględniono omówione wcześniej właściwości chmury, oraz modele wdrożenia i modele usług, o których będzie mowa w dalszej części.

2. Typologia modeli usług przetwarzania w chmurze

W modelu *cloud computing* możemy wyróżnić trzy typy usług określanych jako stos SPI (*Software, Platform, Infrastructure as a Service*):

- oprogramowanie jako usługa (*Software as a Service* – SaaS) – udostępnienie konkretnych funkcjonalności i oprogramowania, klient płaci za ich użycie, a dostęp do nich uzyskuje na żądanie (Rot, 2008),
- platforma jako usługa (*Platform as a Service* – PaaS), polegająca na sprzedaży gotowego (często dostosowanego do potrzeb użytkownika) kompletu aplikacji, ujednoliconego środowiska pracy,
- infrastruktura jako usługa (*Infrastructure as a Service* – IaaS), polegająca na dostarczaniu infrastruktury IT (sprzęt, oprogramowanie i serwis).

Nierzadko do powyższych rodzajów modeli dostarczania usług dodaje się jeszcze następujące (Kuc i Niemczyk, 2013): *Network as a Service* (NaaS) – zarządzanie siecią jako usługa, *Storage as a Service* (STaaS) – udostępnienie miejsca na serwerach usługodawcy np. w celu zarządzania archiwami i kopiami zapasowymi, *Database as a Se-*

rvice (DBaaS) – środowisko bazodanowe jako usługa oraz *Communications as a Service* (CaaS) – platforma do komunikacji pomiędzy użytkownikami. Z punktu widzenia tematyki niniejszego artykułu warto wspomnieć o kolejnym modelu dostarczania usług w chmurze, a mianowicie *Security as a Service* (SECaaS) – bezpieczeństwo jako usługa, obejmującego np.: testy penetracyjne, ocenę potencjalnych zagrożeń, testy odtworzeniowe kopii zapasowej, analizę konfiguracji urządzeń, określenie środków i przedsięwzięć z zakresu bezpieczeństwa, wskazanie kierunków polityki bezpieczeństwa i strategii jej realizacji czy analizę dokumentacji w zakresie bezpieczeństwa IT.

Z perspektywy bezpieczeństwa ważne jest, aby przy wyborze modelu chmury dokonać dokładnej analizy po czyjej stronie (odbiorcy czy dostawcy usługi) spoczywa odpowiedzialność za zarządzanie ryzykiem i implementację odpowiednich zabezpieczeń na każdej z warstw stosu SPI. Eksperci Garner Group zaznaczają, że poziom ryzyka jest różny dla różnych modeli usług *cloud computing*. Co prawda wymagania odnośnie do bezpieczeństwa są jednakowe, to jednak poziom kontroli użytkownika nad zabezpieczeniami zmienia się w zależności od modelu usług.

3. Typologia modeli dostępu do usług przetwarzania w chmurze

W zależności od umiejscowienia serwerów i sposobu przetwarzania danych istnieje kilka typów modeli wdrożenia chmury (IBM, 2014):

1. Chmura prywatna (*Private Cloud*) – rozwiązanie korzystające z infrastruktury i zasobów IT klienta, co pozwala na wprowadzenie wewnętrznego procesu rozliczania z wykorzystania zasobów, przy zapewnieniu elastyczności i efektywności. Wszelkie dane oraz usługi są oferowane w ramach jednego przedsiębiorstwa (choć serwery nie muszą się znajdować fizycznie w pobliżu korporacji, ze względów bezpieczeństwa mogą być rozlokowane w kilku miejscach).
2. Chmura publiczna (*Public Cloud*) – usługa dostarczana jest w formie ustalonej i zwymiarowanej w aspekcie funkcjonalności i uwarunkowań związanych ze świadczeniem samej usługi. Specyfikacja zasobów i konfiguracja infrastruktury IT jest niewidoczna dla klienta końcowego (często nie jest znana lokalizacja usługi), jest to jednak bez znaczenia, bowiem o jakości decyduje funkcjonalność i dostępność usługi. Jest to najpopularniejsza forma występowania centrów obliczeniowych.
3. Chmura hybrydowa (*Hybrid Cloud*) – połączenie chmur prywatnych oraz publicznych. W praktyce część serwerów danej firmy może się znajdować wewnątrz korporacji, natomiast same usługi są zwykle ładowane ze zdalnych urządzeń należących do większych koncernów informatycznych.
4. Chmura współdzielona/społecznościowa (*Community Cloud*) – dzielenie pewnych usług chmury między kilka organizacji, które łączy wspólny cel. Fizycznie całość może być zarządzana wewnętrznie i zewnętrznie (np. przez wspomnianych wcześniej producentów rozwiązań IT).

4. Podstawowe zagrożenia i podatności w modelu *cloud computing*

Cloud computing może dostarczyć wielu korzyści, m.in.: brak wydatków kapitałowych na infrastrukturę, elastyczność, nieograniczoną skalowalność, optymalne wykorzystanie zasobów oraz płatność za ich faktyczne wykorzystanie. Usługi w chmurze nie są jednak całkowicie pozbawione wad i niosą ze sobą pewne zagrożenia (Rot, Sobińska, 2013). Do najczęściej wymienianych form ryzyka można wymienić następujące zagrożenia (Fulmański, Wojczyk, 2014):

1. Niedostępność usług – awaria chmury obsługującej organizacje może mieć bezpośredni wpływ na jej działalność. Wykorzystując chmurę, firmy oczekują ciągłej gotowości, która staje się podstawowym wymogiem obecnych czasów. Potencjalne przyczyny niedostępności usług w chmurze to np.: przerwa w zasilaniu energią elektryczną, awaria sprzętu, sytuacje losowe, celowe działanie osób trzecich.
2. Ryzyko utraty integralności danych – dane w chmurze powinny być przez cały czas kompletne oraz zabezpieczone przed nieuprawnioną zmianą, uszkodzeniem czy zniszczeniem. Usługodawca zarządzający chmurą musi odpowiednio dobierać mechanizmy zapewniające gwarancję integralności danych, co również jemu pozwoli ograniczyć koszty i oszczędzić czas potrzebny na odzyskiwanie danych w przypadku awarii.
3. Uzależnienie od dostawcy chmury – dostawcy chmur oferują różne możliwości jej zastosowania, co wynika często z braku wspólnych standardów, co znacząco utrudnia możliwość migracji z jednej chmury do drugiej z zachowaniem pełnej aktualnej funkcjonalności.
4. Niepowołany dostęp i poufność danych – dane powinny być dostępne tylko dla uprawnionych użytkowników, chmura powinna być wyposażona w bezpieczne mechanizmy ich identyfikacji, uwierzytelniania i autoryzacji.
5. Niewystarczające uregulowania prawne – fizyczne dyski z danymi w chmurze są często współdzielone przez wielu klientów, w przypadku podejrzenia popełnienia przestępstwa może dojść do sytuacji, gdy wspólny sprzęt zostanie zajęty w celu ujawnienia danych (dane należące do klientów chmury mogą zostać ujawnione, nie ma tu precyzyjnych norm prawnych). Istotne są kwestie związane z ochroną danych osobowych, których utrata może podlegać nawet sankcjom karnym. Nieuregulowane prawnie są także kwestie licencjonowania oprogramowania.

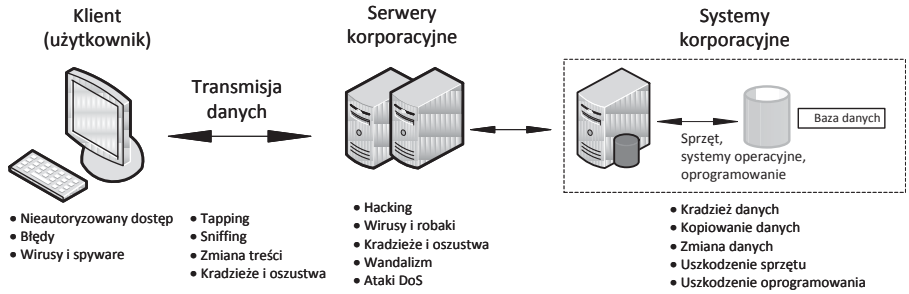
Mówiąc o wyzwaniach związanych z bezpieczeństwem danych i usług w CC, warto przywołać raport Gartner Research – *Assessing the Security Risks of Cloud Computing* (Heiser, Nicolett, 2008), w którym zwrócono uwagę na siedem kluczowych zagrożeń i podatności oraz możliwych sposobów ich eliminacji:

1. Uprzywilejowany dostęp użytkownika – w celu minimalizacji tego ryzyka analitycy Gartnera radzą, aby zażądać od dostawcy szczegółowych danych na te-

mat wynajmu oraz nadzoru nad uprzywilejowanymi administratorami, a także sposobów kontroli dostępu do przetwarzanych informacji.

2. Zgodność z przepisami – ostatecznie to klienci zamawiający usługę są odpowiedzialni za bezpieczeństwo i integralność ich własnych danych, nawet jeśli ich przetwarzanie odbywa się u usługodawcy.
3. Lokalizacja danych – w modelu *cloud* praktycznie bardzo rzadko precyzyjnie wiadomo, gdzie znajdują się składowane i przetwarzane dane. Należy zatem żądać od dostawców usługi, zobowiązania do przetwarzania i przechowywania danych w wyspecyfikowanych jurysdykcjach i potwierdzenia o zobowiązaniu się do zachowania prywatności danych zgodnie z obowiązującymi lokalnymi przepisami i normami.
4. Rozdział danych – ze względu na przechowywanie danych różnych klientów we wspólnym środowisku, należy zażądać od dostawcy, aby systemy szyfrowania zostały zaprojektowane przez specjalistów.
5. Odzyskiwanie danych – obowiązkiem usługodawcy jest poinformowanie, co się dzieje z danymi po awarii i jak długo trwa ich odzyskiwanie.
6. Wsparcie śledcze – raport Gartnera przestrzega przed niemożnością lub utrudnieniami w wykryciu piractwa i innych nielegalnych działań w wypadku używania *cloud computingu*.
7. Długoterminowe działanie usługi – należy mieć pewność, że dane i usługi będą dostępne w dłuższej perspektywie, a także w takich przypadkach jak np. bankructwo dostawcy chmury lub przejęcie go przez inny podmiot.

Każde z opisanych w raporcie Gartnera zagrożeń jest niezwykle istotne w odniesieniu do bezpiecznego zastosowania i implementacji CC. Poza wymienionymi zagrożeniami i podstawową kwestią czynnika ludzkiego, należy pamiętać o pozostałych podatnościach. Potencjalne włamanie do systemu informatycznego, nieautoryzowany dostęp czy w końcu zniszczenie, bądź kradzież danych może wystąpić w każdym miejscu dostępu do danych. Na rysunku 2 przedstawiono właśnie takie miejsca występowania oraz rodzaje zagrożeń i podatności.



Rysunek 2. Wyzwania i podatności z perspektywy cyberbezpieczeństwa

Źródło: opracowanie własne na podst. Laudon (2010).

Jak już podkreślano, dokonując wyboru zewnętrznego dostawcy usług, brane powinny być pod uwagę takie parametry, jak m.in.: bezpieczeństwo i prywatność danych oraz prawa własności. Przy wdrażaniu modelu CC wyzwaniem staje się całościowe zabezpieczenie usług na wielu poziomach, w tym (Dybka i in., 2013):

a) warstwy fizycznej w centrach danych: fizyczne środki kontroli dostępu, nadzór kamer, kontrola zapewniająca dostęp fizyczny wyłącznie dla osób upoważnionych, gwarantowanie rezerwowego źródła zasilania, kontrola warunków klimatycznych w celu zapewnienia optymalnej temperatury i wilgotności powietrza dla funkcjonowania sprzętu, kontrola skutków klęsk żywiołowych, systemy przeciwpożarowe i gaśnicze, monitoring fizyczny;
b) warstwy logicznej: izolacja danych, bezpieczeństwo obsługiwanych aplikacji, usługi infrastrukturalne, poziom sieci, zarządzanie tożsamością i dostępem. Bezpieczeństwo logiczne usług jest zapewnione dzięki:
   a) rozdzieleniu danych;
   b) bezpieczeństwu aplikacji zdalnych, które zapewniane jest dzięki funkcjom takim jak: obsługa komunikacji uwierzytelnionej i zaszyfrowanej; ochrona przed oprogramowaniem złośliwym; zabezpieczenie infrastruktury usług w chmurze; zabezpieczenia na poziomie sieci; zarządzanie tożsamością i dostępem; ograniczenie funkcjonalności serwerów przez wyłączenie usług nieistotnych; logowanie i nadzór; ograniczony dostęp do usług; nadzorowanie treści; lepsza ochrona sesji dzięki protokołom SSL/TLS, itp.

5. Narzędzia i mechanizmy bezpieczeństwa w chmurze

W chmurze obliczeniowej istnieje wiele narzędzi i mechanizmów, które zastosowane w odpowiedni sposób wręcz gwarantują ochronę danych firmy, o wiele pewniejszą niż rozwiązania bazujące na wewnętrznych centrach danych. Dostawcy usług stosują zazwyczaj najbardziej sprawdzone i niezawodne metody zabezpieczania danych, wykorzystują dobrze rozpoznane technologie, takie jak (Pałka, Zaskórski, Zaskórski, 2013):

- szyfrowanie danych (wdrażanie protokołów szyfrowania SSL wymiany danych, które zapewniają poufność i integralność transmisji danych, a także uwierzytelnienie serwera, a niekiedy również klienta, oparte są na szyfrowaniu asymetrycznym oraz certyfikatach X.509, zapewniają także wierzytelność i niezaprzeczalność transmitowanych danych),
- tworzenie wirtualnych sieci lokalnych VPN – tuneli, przez które płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi za pośrednictwem publicznej sieci w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów (można opcjonalnie szyfrować przesyłane dane w celu większego bezpieczeństwa),

- wdrażanie sprawdzonych, bezpiecznych i wydajnych urządzeń i systemów sieciowych (firewall, filtry pakietów danych, systemy autentykacji itp.),
- mechanizmy bezpieczeństwa fizycznego, które odnoszą się do kompleksowego zabezpieczenia budynków, w których zlokalizowany jest cały sprzęt udostępniający usługi CC (dostawcy usług powinni dysponować światowymi certyfikatami bezpieczeństwa, np. SAS 70).

Bezpieczeństwo danych w chmurze obliczeniowej to nie tylko procedury bezpieczeństwa wdrażane przez dostawcę usług, lecz również konieczność zastosowania odpowiednich procedur bezpieczeństwa przez jej użytkowników końcowych. Wśród najważniejszych elementów tej ochrony należy wymienić następujące mechanizmy (Pałka, Zaskórski, Zaskórski, 2013):

- konieczność organizowania i prowadzenia ciągłych szkoleń,
- wdrożenie wewnętrznej polityki bezpieczeństwa pracy z danymi w chmurze,
- przyznawanie użytkownikom certyfikatów bezpieczeństwa,
- stosowanie właściwych metod dostępu użytkowników do danych z zastosowaniem uwierzytelnienia i mechanizmów poświadczania,
- stosowanie mechanizmów logowania do systemu z użyciem specjalnych kluczy dostępowych, uwierzytelniających użytkownika,
- stosowanie właściwych certyfikatów kryptografii dla zachowania bezpieczeństwa danych udostępnianych i przetwarzanych w chmurze.

W celu minimalizacji ryzyka przetwarzania danych w chmurze, firmy powinny decydować się na korzystanie ze sprawdzonych rozwiązań i powinny zrozumieć, że pod względem bezpieczeństwa systemów informatycznych coraz bardziej uzależnione są od stron trzecich. Jeżeli w organizacji obowiązują wysokie standardy dotyczące bezpieczeństwa danych, należy wymagać podobnych zabezpieczeń od podmiotów zewnętrznych i dostawców *cloud computingu*.

Podsumowanie

Konkludując można stwierdzić, że *cloud computing*, jak każde rozwiązanie IT, ma wiele zalet, ale stoi przed nią jednocześnie wiele wyzwań, gdyż jej stosowanie nie jest wolne od zagrożeń. Najczęściej przywołuje się w tym miejscu kwestę bezpieczeństwa danych i usług. Środowisko chmury nie będzie jednak zagrożeniem dla bezpieczeństwa firmy, jeżeli właściwe będzie przygotowana infrastruktura systemu oraz zostaną odpowiednio wdrożone, wskazane w artykule, procedury i mechanizmy w zakresie ochrony danych i usług. Dodatkowym źródłem wątpliwości jest brak jasnych uregulowań prawnych oraz jednolitych standardów. Istotnym elementem całego procesu implementacji chmury obliczeniowej jest dlatego wybór sprawdzonego i zaufanego dostawcy tych usług oraz dokładna analiza zapisów umowy SLA (*Service Level Agreement*), za pomocą której można zniwelować zagrożenia związane z użytkowaniem zasobów IT w chmurze.

Bibliografia

Badger, L., Grance, T., Patt-Corner, R., Voas, J. (2011). *Cloud Computing Synopsis and Recommendations. NIST Special Publication 800-146, US Department of Commerce*. Pobrano z: http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf (11.05.2016).

Chellapa, K. (1997). *Intermediaries in Cloud Computing: A New Computing Paradigm*. Dallas, TX: INFORMS Annual Meeting.

Dybka, E., Falkowski, D., Gajda, R. i in. (2013). *Cloud Computing w sektorze finansowym*. Kraków: Wydawnictwo edu-Libri. Pobrane z: zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/technologie_bankowe/publikacje/Raport_Cloud_computing_w_sektorze_finansowym_2013-_z_recenzjami.pdf (9.12.2016).

Fronczak, M. (2013). *Zarządzanie ryzykiem w modelu cloud computing – wprowadzenie*. Pobrane z: https://www.governica.com/wiadomosc/Zarzadzanie_ryzykiem_w_modelu_cloud_computing_-_wprowadzenie (24.11.2016).

Fulmański, P., Wojczyk, S. (2014). Potencjalne korzyści i zagrożenia związane z chmurą obliczeniową. *Zeszyty Naukowe Uniwersytetu Szczecińskiego. Studia Informatica*, *34*.

Gillett, S.E., Kapor, M. (1996). *The Self-governing Internet: Coordination by Design, Coordination and Administration of the Internet*. Workshop at Kennedy School of Government, Harvard University.

Heiser, J., Nicolett, M. (2008). *Gartner Research, Assessing the Security Risks of Cloud Computing*. Pobrano z: http://s3.amazonaws.com/academia.edu.documents /33355553/Gartner_Security_Risks_of_Cloud.pdf (22.08.2016).

IBM SmartCloud (2014). Pobrano z: www-05.ibm.com/pl/cloud/ (30.09.2015).

Kuc, M.E., Niemczyk, W. (2013). Rynek usług cloud computing – współczesne wyzwania, zagrożenia, trendy, perspektywy. *Zarządzanie i Finanse, 1/1*, 391–410.

Laudon, K.C., Laudon, J.P. (2010). *Management Information Systems*. Managing the Digital Firm, 11th ed., Pearson.

Mell, P., Grance, T. (2011). *The NIST Definition of Cloud Computing, NIST Special Publication 800-145, U.S. Dept. of Commerce*. Pobrano z: nvlpubs.nist.gov /nistpubs/Legacy /SP/nistspecialpublication800-145.pdf (12.06.2016).

Pałka, D., Zaskórski, W., Zaskórski, P. (2013). Cloud computing jako środowisko integracji usług informatycznych. *Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki*, *9* (7).

Rot, A. (2008). Oprogramowanie dostarczane jako usługa – model SaaS. Stan obecny, perspektywy rozwoju oraz przykłady rozwiązań. *Informatyka Ekonomiczna*, *12*.

Rot, A., Sobińska, M. (2013). IT security threats in cloud computing sourcing model. W: M. Ganzha, L. Maciaszek, M. Paprzycki (red.), *Proceedings of the 2013 Federated Conference on Computer Science and Information*. Kraków: PTI. Pobrano z: https://fedcsis.org/proceedings/2013/pliks/fedcsis.pdf (28.10.2016).

Vaquero, L.M., Rodero-Merino, L., Caceres, J., Lindner, M. (2008). A break in the clouds: towards a cloud definition. *ACM SIGCOMM Computer Communication Review*, *39* (1), 50–55.

THE CHALLENGES OF DATA AND SERVICES SECURITY IN THE CLOUD COMPUTING MODEL

Keywords: cloud computing, security, privacy, authentication

Summary. Cloud computing, like most modern IT solutions, can provide many benefits for organizations, but cloud services are not completely free of risks and carry certain threats. Main threats and vulnerabilities of cloud services are related to the areas of authentication, data security and privacy, system availability and business continuity. The security and privacy are the most important area among these risk factors. The purpose of this article is to present cloud computing from the perspective of data and services security, and in particular to indicate the biggest challenges facing the application of this model.

Translated by Artur Rot

Cytowanie

Rot, A. (2017). Wyzwania bezpieczeństwa danych i usług w modelu cloud computing. *Ekonomiczne Problemy Usług, 1* (126/2), 125–134. DOI: 10.18276/epu.2017.126/2-13.