Małgorzata Ziemecka

Rozwiązania "cloud computing" w administracji publicznej

Ekonomiczne Problemy Usług nr 88, 454-462

2012

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 703 EKONOMICZNE PROBLEMY USŁUG NR 88 2012

MAŁGORZATA ZIEMECKA
Uniwersytet Łódzki

ROZWIĄZANIA CLOUD COMPUTING W ADMINISTRACJI PUBLICZNEJ

Wprowadzenie

W dobie informatyzacji działalności administracji publicznej kadra zrządzająca urzędami stoi przed wyzwaniem opracowania strategii informatyzacji urzędu i podjęciem decyzji inwestycyjnych dotyczących technologii i narzędzi informatycznych. Może zdecydować się na zakup i wdrożenie rozwiązań we własnym zakresie lub skorzystać z usług przetwarzania w chmurze. Te ostatnie nie wymagają inwestowania w infrastrukturę informatyczną i pozwalają optymalizować koszty IT przy dostępności usług niezależnie od miejsca dostępu. Decyzja taka powinna zostać podjęta w oparciu o analizę procesów gospodarczych zachodzących w urzędzie, dzięki czemu wybrane rozwiązanie ICT będzie wspierało te procesy, przyczyniając się do polepszenia jakości pracy urzędu.

1. Definicja cloud computing

Cloud computing[1] ma wiele różnych definicji. W sektorze publicznym (np. USA, Niemcy) została przyjęta definicja ustalona przez National Institute of Standards and Technology: „Przetwarzanie w chmurze to takie przetwarzanie, które poprzez dogodny dostęp sieciowy dostarcza współdzielony zestaw konfigurowalnych zasobów przetwarzania, np. dostarcza sieci, serwery, przestrzeń do składowa-

[1] Przetwarzanie w chmurze.

nia danych, oprogramowanie i usługi. Zasoby te są dostarczane szybko (na żądanie) z minimalnym wysiłkiem zarządzania i z minimalnym udziałem dostawcy"[2].

Definicja ta obejmuje pięć kluczowych charakterystyk, trzy modele usług i cztery modele wdrażania, które są ważne dla zrozumienia natury i terminologii chmury.

Przetwarzanie w chmurze ma miejsce wtedy, gdy charakteryzuje się ono takimi cechami jak: samoobsługowe usługi na żądanie, szeroki dostęp do sieci, definiowalna pula zasobów, błyskawiczna elastyczność, mierzalne usługi.

Określone zostały trzy modele świadczenia usług:

1. Infrastruktura jako usługa (IaaS)[3] – polega na udostępnianiu za pośrednictwem Internetu sprzętu, np. miejsca na wirtualnym dysku na przechowywanie danych, miejsca na serwerze na własny system operacyjny, korzystanie z mocy obliczeniowej procesorów.
2. Platforma jako usługa (PaaS)[4] – pozwala użytkownikowi na dostęp nie tylko do sprzętu, ale także do środowiska, w którym może instalować i uruchamiać aplikacje, przy czym elementy infrastruktury udostępniane są jak wirtualny superkomputer, na którym można budować skalowalne aplikacje.
3. Aplikacja jako usługa (SaaS)[5] – jest najbardziej zaawansowanym poziomem, który pozwala użytkownikowi na dostęp do sprzętu, środowiska oraz aplikacji (np. edytorów, poczty elektronicznej, systemów księgowych). Aplikacje te są własnością dostawcy chmury, który odpowiada za ich aktualizacje i bezawaryjne działanie.

Opisane zostały cztery modele wdrażania chmury:

1. Chmura prywatna, infrastruktura jest kontrolowana przez usługobiorcę, który ma fizyczny dostęp do serwerów, magazynów danych z oprogramowaniem tworzącym chmurę.
2. Chmura wspólnotowa, infrastruktura jest własnością kilku organizacji, mających wspólny cel, który ta chmura wspiera. Może być zarządzana przez te organizacje lub przez niezależnego dostawcę.
3. Chmura publiczna, infrastruktura jest własnością dostawcy i mogą z niej korzystać wszyscy.
4. Chmura hybrydowa, jest połączeniem rozwiązań stosowanych w chmurze prywatnej i publicznej. W chmurze prywatnej przetwarzane są dane strategiczne i prawnie chronione, pozostałe dane przesyłane są do chmury publicznej.

---

[2] Def. wg NIST za K. Łapiński, B. Wyżnikiewicz, *Cloud Computing: elastyczność, efektywność, bezpieczeństwo*, raport 2011, s. 9.

[3] Infrastructure as a Service.

[4] Platform as a Service.

[5] Software as a Service.

2. Bezpieczeństwo cloud computing

Tworząc i wykorzystując rozwiązania przetwarzania w chmurze, należy brać pod uwagę szereg ryzyk zagrażających bezpieczeństwu przetwarzania danych, takich jak: użycie w celu przestępczym, niebezpieczne interfejsy i API, wrogie działania wewnątrz chmury obliczeniowej, luki w aplikacjach i mechanizmach, utrata poufności danych lub danych, przechwycenie usługi, ruchu lub konta oraz ryzyko nieznanego poziomu[6]. Znaczenie tych ryzyk uzależnione jest od rodzaju prowadzonego biznesu i wykorzystywanego modelu chmury.

Użycie w celu przestępczym polega na wykorzystaniu nieograniczonej mocy obliczeniowej chmury do działań typu: zdalne ataki DDoS[7], kradzież haseł i kluczy oraz ich łamanie, przechowywanie złośliwego kodu, które ułatwiane jest przez procedury rejestracyjne niewymagające autoryzacji użytkownika.

Interfejsy oprogramowania lub API[8] wykorzystywane są do tworzenia interakcji z usługami cloud computing lub zarządzania nimi. Ich słabe zabezpieczenie zagraża poufności i integralności danych, a także dostępności do nich.

Czynnik ludzki jest najczęściej najsłabszym ogniwem zabezpieczeń systemu. Biorąc pod uwagę fakt, że pracownicy firmy usługodawcy chmury mają dostęp do ważnych danych klientów, co umożliwia im zebranie poufnych danych lub uzyskanie kontroli nad usługami klienta, powinny zostać wprowadzone przejrzyste procedury bezpieczeństwa systemu i powiadamiania o ich łamaniu, a warunki zarządzania zasobami ludzkimi określone w części prawnej kontraktu.

W chmurze korzysta z usług wielu klientów jednocześnie poprzez infrastrukturę, której komponenty nie były zaprojektowane do oferowania w taki sposób zabezpieczonych funkcjonalności. Powstały luki bezpieczeństwa sprzętowego, których wykorzystanie umożliwia włamanie się w operacje innych działających w tej samej chmurze.

Utrata poufności danych lub danych ma wpływ na zaufanie partnerów i klientów firmy, może powodować straty finansowe, naruszać reputację firmy i powodować migrację klientów do konkurencji. Zagrożenia te zwiększają się w przetwarzaniu w chmurze, które jest rozproszone, a ich przyczyny tkwią w słabej autentykacji i autoryzacji, niespójnym użyciu kluczy szyfrujących i programowych, błędach proceduralnych, ryzyku połączeń, ryzyku nadzoru prawnego, zagrożeniu zawodności działania centrów danych czy w nieodpowiedniej procedurze przywracania systemu po awarii.

Największym zagrożeniem przetwarzania danych w chmurze jest przechwycenie konta lub usługi, najczęściej związane z kradzieżą tożsamości, dzięki czemu

---

[6] M. Mejssner, *Raport nr 8*, www.ticons.pl/newsletter/Raport_nr_8.pdf.

[7] Distributed Denial of Service – rozpowszechniona odmowa usługi.

[8] Application Programming Interface.

osoby nieupoważnione uzyskują dostęp do krytycznych obszarów wystawionych usług, narażając je na utratę poufności, integralności lub dostępności. Atakujący może podsłuchiwać transakcje, manipulować danymi czy przekierowywać klientów do niebezpiecznych stron.

Negocjacje i umowy o przetwarzanie w chmurze nie uwzględniają wewnętrznych procedur bezpieczeństwa, zmian konfiguracyjnych, uaktualniania systemu, wprowadzania łat i audytowania, procedur w przypadku incydentu bezpieczeństwa, co powoduje, że klient nie jest w stanie oszacować ryzyka bezpieczeństwa i godzi się na usługi w chmurze z perspektywą ryzyka nieznanego stopnia.

Bezpieczeństwo przetwarzania w chmurze powinno opierać się na najlepszych praktykach i obejmować następujące komponenty[9]:

- budowa programu bezpieczeństwa,
- ochrona danych poufnych,
- implementacja silnych mechanizmów kontroli dostępu i tożsamości,
- aprowizacja i deaprowizacja aplikacji,
- zarządzanie audytem i nadzorem IT,
- zarządzanie podatnościami, testowanie i walidacja.

Bezpieczeństwo przetwarzania w chmurze jest szczególnie istotne dla administracji publicznej, powinno być zgodne z obowiązującym prawem i polityką, zapewniać ochronę danych osobowych.

3. Scenariusze cloud computing dla sektora publicznego

Realizacja usług chmury wymaga zidentyfikowania uczestników, którzy będą korzystać z tych usług lub je dostarczać. W przypadku wykorzystania chmury w administracji publicznej należy rozważyć następujących dodatkowych uczestników[10]:

- Mieszkańcy – korzystają z chmury urzędu, przy czym stosowane powinny być specjalne procedury ochrony danych osobowych. Na przykład obywatel ma prawo do: uzyskania informacji o przechowywanych danych osobowych, z jakich źródeł pochodzą te dane i w jakich celach są one przechowywane; korekty błędnych danych osobowych, autoryzacji przekazania danych osobom trzecim; składania reklamacji w urzędzie odpowiedzialnym za ochronę danych osobowych.
- Firmy – komercyjne instytucje korzystające z chmury, przy czym zasady ochrony danych nie są tak restrykcyjne jak w przypadku danych osobowych.

---

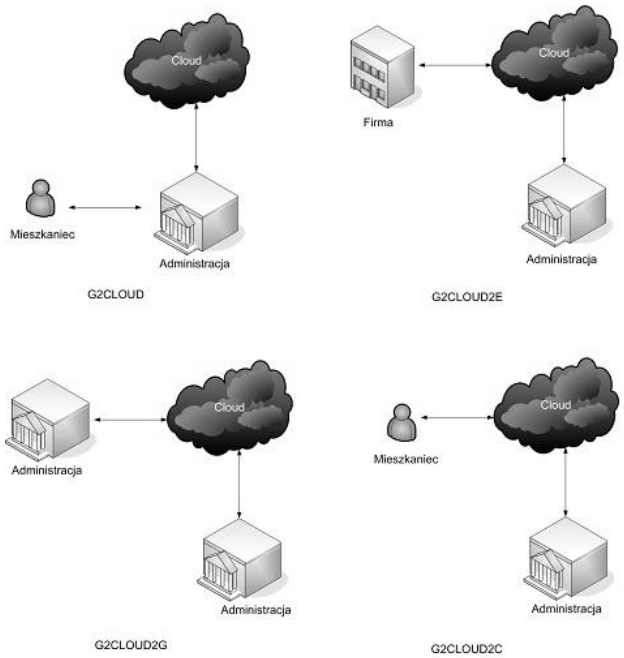
[9] R. Michalski, *Bezpieczeństwo w chmurze – nie taki wilk straszny jak go malują*!, V Zachodniopomorski Konwent Informatyków, Międzywodzie 15.09.2011.

[10] Na podstawie: P. Deussen, K.P. Eckert, L. Strick, D. Witaszek, *Cloud Concepts for the Public Sector in Germany – Uses Cases*, FOKUS, 2011.

- Agencje rządowe – korzystają z usług chmury w celu wsparcia procesów wewnętrznych, przy czym usługi te mogą być świadczone przez prywatnych lub publicznych dostawców. Odpowiedzialność za realizację, wydajność i bezpieczeństwo realizacji podstawowych zadań agencji, tzn. świadczenie usług dla obywateli, spoczywa na samej agencji, a to oznacza, że jest ona odpowiedzialna za monitorowanie i kontrolowanie realizacji procesów u dostawcy chmury.
- Rządowy dostawca chmury – dostawca ten udostępnia usługi w chmurze dla obywateli, firm i innych agencji w imieniu agencji rządowej i może należeć do sektora publicznego lub prywatnego.
- Urzędnik / organ ochrony danych – osoba w instytucji lub instytucja odpowiedzialna za nadzorowanie wdrożenia polityki bezpieczeństwa danych. Dostawcy IT muszą dostarczać temu organowi wyczerpujące informacje dotyczące np. sprzętu i oprogramowania, danych z monitoringu, stosowanych procedur itp.

Rozwiązania chmury dla administracji publicznej powinny brać pod uwagę pewne dodatkowe wymiary np.:

- wdrażany model chmury może być ograniczony w zależności od przyjętego scenariusza użycia dla sektora publicznego;
- tradycyjne modele świadczenia usług wraz z przyszłymi modelami, takimi jak: dane jako usługa, proces jako usługa, wiedza jako usługa itd., pomagają kategoryzować scenariusze użycia oraz techniczne przypadki użycia;
- specyficzne modele biznesowe, takie jak G2Cloud, G2Cloud2E, G2Cloud2C, G2Cloud2G (G = rząd, C = obywatel, E = przedsiębiorstwo), mogą być wykorzystane do dopracowania scenariusza użycia, w którym wystąpią także dodatkowi użytkownicy;
- należy rozróżnić dostawców z sektora publicznego i prywatnego;
- należy rozważyć rolę aktorów zewnętrznych, takich jak np. dostawcy aplikacji chmury, broker płatności, broker usług, przedstawiciel prawny czy dostawca tożsamości chmury;
- powinny być wzięte pod uwagę dodatkowe niefunkcjonalne właściwości usług chmury, takie jak dostępność, wydajność, odporność, rozliczenia, polityka SLA (Service Level Agreement).



Rys. 1. Modele konfiguracji chmury w administracji publicznej

Źródło: P. Deussen P., K.P. Eckert, L. Strick, D. Witaszek, *Cloud Concepts for the Public Sector in Germany – Uses Cases*, FOKUS, 2011, s. 29–30.

Na rysunku 1 przedstawione zostały cztery podstawowe konfiguracje wykorzystania chmury w administracji publicznej.

Model G2Cloud umożliwia redukcję kosztów i konsolidację środowiska IT, taką jak wprowadzenie wspólnych usług, które są katalizatorem dla tego modelu. Obywatele korzystają z usług dostarczanych przez agencję rządową, wiedząc, że niektóre usługi zaplecza są uruchomione w chmurze.

Model G2Cloud2E pozwala na realizację elektronicznych zamówień publicznych, składanie wniosków, przesyłanie zawiadomień, dostęp do jawnych danych, procesów i przepływów pracy między rządem a przedsiębiorstwami.

Model G2Cloud2C obsługuje takie usługi jak elektroniczne wnioski, zawiadomienia, e-udział, e-współpraca, dostęp do jawnych danych, zwrot podatku, skargi.

Model G2Cloud2G stanowi elektroniczne wsparcie dla urzędów, obsługę międzyurzędowych procesów, wspólne repozytoria i systemy informacyjne oraz elektroniczną współpracę agencji sektora publicznego.

Należy zauważyć, że przedstawione powyżej modele realizują usługi, które są przede wszystkim powodem wdrażania systemów e-urzędów, nie wymagają one wprowadzenia rozwiązań chmury, chociaż jej zastosowanie jest korzystne z punktu widzenia technologii i ekonomii.

4. PICTURE jako narzędzie ułatwiające wybór usług chmury

Cloud computing jest rozwiązaniem, które jak każde inne rozwiązanie ICT wymaga oceny jego użyteczności dla danej instytucji. Zatem należy i w tym przypadku przeprowadzić analizę biznesową i wymagań, określić projekt architektury systemu i na tej podstawie podjąć decyzję o potrzebnych komponentach ICT – również tych oferowanych w chmurze. Urzędy administracji publicznej w takich analizach mogą wspomagać się narzędziami informatycznymi, których przykładem jest PICTURE[11].

PICTURE jest narzędziem korzystającym z technologii internetowych, które umożliwia efektywny pomiar oddziaływania technologii informatycznej na procesy gospodarcze zachodzące w administracji publicznej. Składa się z dwóch głównych części: modułu modelowania procesów (*the Process Landscaping Module*) i modułu mierzenia wpływu (*the Impact Measurement Module*).

Moduł modelowania procesów umożliwia utworzenie mapy procesów danej jednostki administracji publicznej, przy czym procesy są modelowane przez bezpośrednich aktorów danego procesu zgodnie z nowatorską notacją modelowania. Modelowanie procesu realizowane jest w oparciu o bloki PBB (*Process Building Blocks*), które określają czynności wykonywane w ramach procesu. Zestaw bloków opracowany został zgodnie z potrzebami administracji publicznej. Dla każdego bloku wprowadza się szereg atrybutów, charakterystycznych dla danego bloku, opisujących szczegółowo daną czynność, np. osoby zaangażowane w tę czynność, przetwarzane w ramach czynności obiekty (dokumenty), czas trwania czynności, liczba tworzonych kopii itp.

Celem modułu pomiaru wpływu jest identyfikacja i pomiar wpływu technologii informacyjnej i komunikacyjnej na procesy zachodzące w urzędach administracji publicznej. Wykorzystana w tym module metodologia skupia się na określeniu korzyści i słabości wpływu ICT na procesy oraz na integracji narzędzi ICT z procesami. Moduł mierzenia wpływu opiera się na analizie zamodelowanych procesów w oparciu o wzorce słabych punktów (*weakness pattern*), które muszą zostać określone w systemie przez eksperta z zakresu analizy procesów i stanowią bazę dla zmierzenia wpływu ICT na procesy. W wyniku przeprowadzonej analizy generowane są raporty, które kadra zarządzająca może wykorzystać w procesie podejmowania decyzji w zakresie IT. Wykorzystana w narzędziu PICTURE metodologia pomiaru wpływu ułatwia odpowiedź na pytanie:

W jakie technologie teleinformatyczne należy inwestować w obszarze administracji publicznej?

---

[11] *Process Identification and Clustering for Transparency In Reorganising Public Administrations*, nr projektu 027717. Projekt realizowany był w ramach 6 Programu Ramowego w latach 2006–2008. Udziałowcem projektu z Polski była Katedra Informatyki Ekonomicznej UŁ.

Jest ona ukierunkowana na wspomaganie kierownictwa urzędów w identyfikacji najbardziej odpowiednich narzędzi ICT z punktu widzenia korzyści tych technologii, które rozpatrywane są w trzech obszarach: poprawa jakości, oszczędność czasu i obniżka kosztów.

Pomiar wpływu technologii ICT na procesy w urzędach administracji publicznej realizowany jest w sześciu etapach:

1. Identyfikacja charakterystyki procesów – polega ona na analizie szczegółowo zamodelowanych procesów (wprowadzone atrybuty PBB i PO), w wyniku której tworzona jest lista charakterystyk procesów.
2. Identyfikacja słabości – obejmuje analizę modeli procesów w oparciu o listę charakterystyk procesów, w wyniku której tworzona jest lista słabości procesów, przy czym kluczowe słabości procesu są określane w oparciu o wzorce słabych punktów.
3. Mapowanie optymalnych narzędzi ICT do słabości – opiera się na analizie listy słabości procesów i profili analizy słabości. W wyniku tej analizy otrzymywana jest mapa optymalnych narzędzi ICT w stosunku do słabości procesów.
4. Identyfikacja korzyści z zastosowania narzędzi ICT – opiera się na liście słabości, optymalnej mapie ICT usuwającej słabości i profilach analizy słabości. W wyniku tej analizy tworzony jest zestaw korzyści, które mogą zostać osiągnięte w wyniku zastosowania narzędzi ICT.
5. Pomiar korzyści z zastosowania ICT – wykorzystuje listę charakterystyk procesów, listę słabości procesów, optymalną mapę ICT i profile analizy słabości. W wyniku analizy uzyskiwane są konkretne dane pomiarowe mierzone w kategoriach jakości, czasu, zasobów.
6. Prezentacja wyników – kończy proces mierzenia wpływu ICT na procesy. Wynikiem analizy tego etapu jest zestaw raportów tworzony według preferencji użytkownika.

Podsumowanie

Zastosowanie rozwiązań przetwarzania w chmurze w administracji publicznej może przynieść wiele korzyści, szczególnie finansowych, ale niesie ze sobą również zagrożenia, w tym przede wszystkim związane z bezpieczeństwem danych i problemami prawnymi. Ich przezwyciężenie wymaga przygotowania dobrej strategii przeniesienia usług informatycznych i danych do chmury. Dostawcy usług w chmurze tworzą specjalne rozwiązania dla administracji, np. Google Apps for Government (korzysta z niej ok. 100 amerykańskich agencji federalnych), Microsoft Business Productivity Online Suit, Microsoft Exchange Online, Microsoft

SharePoint Online. Rozwiązania chmury stosują już administracje publiczne wielu krajów, np. USA, Danii, Anglii, Australii, Kanady.

Decyzja o przejściu na przetwarzanie w chmurze nie powinna być wynikiem zauroczenia pojęciem cloud computing, lecz rzetelnej analizy potrzeb informacyjnych administracji publicznej, która może być wspomagana narzędziami informatycznymi typu PICTURE. Tylko pragmatyczne podejście, którego efektem będzie nabycie rzeczywiście potrzebnych usług i rozwiązań, pozwoli na osiągnięcie oczekiwanych korzyści.

Literatura

1. Deussen P., Eckert K.P., Strick L., Witaszek D., *Cloud Concepts for the Public Sector in Germany – Uses Cases*, FOKUS, 2011.
2. Łapiński K., Wyżnikiewicz B., *Cloud Computing: elastyczność, efektywność, bezpieczeństwo*, raport 2011.
3. Mejssner M., *Raport nr 8*, www.ticons.pl/newsletter/Raport_nr_8.pdf.
4. Michalski R., *Bezpieczeństwo w chmurze – nie taki wilk straszny jak go malują!*, V Zachodniopomorski Konwent Informatyków, Międzywodzie 15.09.2011.
5. Ziemecka M., *PICTURE jako narzędzie wspierające podejmowanie decyzji w zakresie IT w administracji publicznej*, w: *Wybrane problemy budowy aplikacji dla gospodarki elektronicznej*, red. M. Niedźwiedziński, K. Lange-Sadzińska, Łódź 2009.
6. Dokumentacja projektu nr 027717 PICTURE 2006–2009.

CLOUD COMPUTING SOLUTIONS IN THE PUBLIC ADMINISTRATION

Summary

This article describes Cloud Computing in the context of its use by public administrations. Discussed were such issues as the definition of Cloud Computing, its architecture, security and the usage scenarios for the public administrations. There is presented also the tool PICTURE that can support managers in the office in making a decision on the ICT solutions – their own or available in the cloud.

Translated by Małgorzata Ziemecka