Krzysztof BILLEWICZ
POLITECHNIKA WROCŁAWSKA, INSTYTUT ENERGOELEKTRYKI
ul. Wybrzeże Wyspiańskiego 27, 50-370 Wrocław

Doświadczenia wykorzystania technologii Cloud computing w systemie AMR

Dr inż. Krzysztof BILLEWICZ

Adiunkt w Instytucie Energoelektryki Politechniki Wrocławskiej. Wcześniej pracował 3 lata w Instytucie Automatyki Systemów Energetycznych oraz 6 lat w firmie WINUEL SA Grupa Sygnity. Autor ponad 50 publikacji naukowych oraz monografii pt. Smart Metering. Inteligentny system pomiarowy, wydanej w 2012 roku przez Wydawnictwo Naukowe PWN.

e-mail: Krzysztof.Billewicz@pwr.wroc.pl

Streszczenie

Cloud computing jest to model przetwarzania danych, oparty na korzystaniu z zasobów komputerowych dostarczonych przez zewnętrzne przedsiębiorstwa lub działy firmy za pośrednictwem sieci. W artykule zostaną przedstawione doświadczenia z kilkuletniego funkcjonowania systemu AMR (ang. Automated Meters Reading) bazującego na rozwiązaniu chmury prywatnej.

Słowa kluczowe: przetwarzanie w chmurze, outsourcing, bezpieczeństwo, inteligentny system pomiarowy, system AMR.

Experiences using the cloud computing technology in the AMR

Abstract

This paper describes many types of public cloud computing and problem with cloud computing security. Cloud computing is the use of computing resources that are delivered as a service over a network. Cloud computing relies on sharing of resources to achieve coherence and economies of scale similar. The paper presents the several years' experience of the AMR (Automated Meters Reading) system operation based on a private cloud. AMR projects are successfully used by numerous local and national utilities but it was one of the first projects based on cloud technology. This system AMR was implemented in a utility company. The computer system has been working commercially since 2008. Users have to connect to server using Remote Desktop Connection. It was a new solution for the users. They were accustomed to the fact that all the programs they had installed on own PC. The past experience show that the cloud computing is a very forward-looking technology which can be used in systems AMR/AMI (Advanced Metering Infrastructure).

Keywords: cloud computing, outsourcing, security, smart metering, AMR system.

1. Wprowadzenie

Kryzys dopadł bardzo wiele przedsiębiorstw. W wielu z nich dosłownie liczy się każdy grosz. Dlatego podejmuje się różne działania zmierzające do ograniczenia kosztów funkcjonowania. Oszczędności, realizowane w racjonalny sposób, to często najtańszy sposób na ograniczenie kosztów funkcjonowania lub zwiększenia zysków. Nierzadko dużo łatwiejszy niż wypracowanie przychodów pieniężnych np. w wyniku sprzedaży dobra lub usługi.

Dzisiejszy biznes nie istnieje bez IT. W tym artykule poruszono zagadnienie oszczędności wynikających ze zmiany sposobu korzystania z usług informatycznych. Dzięki tej zmianie z jednej strony można z ograniczyć koszty wynikające z konieczności utrzymania liczniejszego personelu wsparcia informatycznego w przedsiębiorstwie, z drugiej jednak strony prowadzi to do uzależnienia od firmy świadczącej usługę tzw. przetwarzania w chmurze. Rodzi to nowe wyzwania w zakresie bezpieczeństwa danych oraz niezawodności świadczenia konkretnych usług – funkcjonowania systemu umożliwiającego zdalny odczyt liczników AMR (ang. *Automated Meters Reading*).

2. Historia

Od paru lat w przedsiębiorstwach dystrybucyjnych energii wdrażane są systemy pomiarowo-rozliczeniowe bazujące na tzw. przetwarzaniu danych w chmurze (ang. *cloud computing*). Samo to pojęcie oznacza technologie dostępne od kilkunastu lat, tylko obecnie zgrupowane razem z innymi i nazwane wspólnym określeniem *cloud computing*.

Przetwarzanie lub udostępnianie danych na komputerze znajdującym się kilkadziesiąt kilometrów od użytkownika nie jest żadną nowością. To, że użytkownik, nie wiedział nawet, w jakim mieście znajduje się komputer, z którego zasobów lub mocy przeliczeniowych korzystał, również nie jest zaskakujące. Szybkość przesyłania danych spowodowała, że fizyczna lokalizacja serwera w zasadzie przestała mieć znaczenie.

Rozwiązania takie powszechnie były stosowane do umieszczania na zdalnych serwerach ogólnodostępnych stron www. Dzięki temu użytkownik nie musiał:

- posiadać odpowiedniego oprogramowania na swoim komputerze,
- mieć go stale włączony,
- stale go monitorować,
- obawiać się ataku hakerskiego.

Klient pełnienie tych zadań powierzy innej firmie i będzie płacił za świadczenie takich usług.

Technologie komputerowe jednak dalej rozwijały się. Stworzono programy, które udawały komputer z systemem operacyjnym tzw. wirtualne maszyny. Dzięki temu na jednym komputerze można było uruchomić kilka systemów operacyjnych i programów pracujących na nich zupełnie niezależnie od siebie. Dodatkowa zaleta była taka, że system operacyjny wraz z jego konfiguracją, zainstalowanymi na nim programami i zasobami danych był zapisany jako plik, który mógł być powielany, kopiowany, przesyłany, archiwizowany i otwierany w środowisku wirtualnej maszyny. Teraz użytkownik mógł dowolnie zmieniać konfigurację takiego środowiska, zawsze jednak pozostawał plik początkowy, w którym wszystko było prawidłowo zainstalowane. Niezależnie od działań podjętych przez użytkownika oraz działań wirusów itp. można było bezproblemowo przywrócić pierwotną prawidłową konfigurację dowolną ilość razy.

3. Outsourcing

Pojęcie *outsourcing* jest skrótem od angielskiego *outside-resource-using*, oznaczającym korzystanie z zasobów zewnętrznych. Głównymi powodami korzystania z takich zasobów są: redukcja i kontrola kosztów operacyjnych, uzyskanie w elastyczny sposób dostępu do mocy produkcyjnych najlepszej jakości, zwłaszcza takich, jakimi przedsiębiorstwo nie dysponuje, dostęp do większej wiedzy, talentów i doświadczenia, możliwość skoncentrowania się na podstawowej działalności, którą firma wykonuje dość sprawnie i niewchodzenie w dziedziny, w których przedsiębiorstwo pozbawione jest doświadczenia i kompetencji. Strategia outsourcingu najczęściej jest stosowana w obszarach: informatyki, operacji pomocniczych np. rachunkowości, marketingu oraz logistyki (np. leasing). Outsourcing umożliwia przedsiębiorstwom płacenie za usługi, których potrzebują, tylko wtedy, gdy ich potrzebują. Zmniejsza to także konieczność zatrudniania i szkolenia wykwalifikowanych pracowników. Czasami wykorzystuje się świadczenie usług przez pracowników i przedsiębiorstwa z innych krajów, które są gotowe wykonać tę samą usługę np. o

połowę tajniej. Jednak z punktu widzenia pracowników w kraju, takie działanie jest związane z przekazaniem kontroli nad procesem pracy podmiotowi zewnętrznemu w innym kraju. W takim przypadku nie tylko ten podmiot otrzymuje wynagrodzenie za wykonaną pracę, ale również zdobywa kompetencje, referencje i doświadczenie. W przypadku popularności korzystania z usług outsourcingu pracownicy tracą siłę przetargową i łatwiej dla korporacji jest ich zwolnić i zlecić wykonywanie swojej pracy za granicą. Outsourcing może również wiązać się z wykorzystaniem siły roboczej w krajach o niskich kosztach pracy i niskich stawkach podatku dochodowego lub innych rozwiązań stosowanych w tzw. rajach podatkowych.

Najpoważniejszymi zagrożeniami outsourcingu są:
- uzyskanie mniejszych obniżek kosztów niż planowane i spodziewane,
- pogorszenie jakości świadczenia usług w stosunku do jakości dotychczas wykonywanych samodzielnie,
- brak powodzenia w wypracowaniu właściwej relacji z zewnętrznym dostawcą usług,
- spory i konflikty pomiędzy klientem, a dostawcą usług dotyczące wysokości wynagrodzenia oraz jakości świadczonych usług,
- możliwość uzależnienia się od dostawcy usług,
- problemy z zachowaniem wysokiej jakości w przypadku dużego udziału obcych komponentów,
- możliwość poniesienia strat wynikających z nierzetelności i niesolidności kooperantów,
- negatywne stosunki z częścią załogi pracowniczej wynikające z redukcji personelu,
- ryzyko wzrostu kosztów.

Zalety outsourcing usług IT są następujące:
- zwiększenie niezawodności pracy systemów informatycznych prowadzące do zwiększenia produktywności i zysków,
- obniżenie kosztów – zmniejszenie lub całkowite pozbycie się działu zajmującego się systemami informatycznymi – zazwyczaj jest to wysoko wynagradzany personel, ponieważ w przypadku niskich wynagrodzeń możliwa jest duża rotacja pracowników i problemy firmy z tym związane: poszukiwanie nowych pracowników, szkolenie ich, okresowa praca osób bez doświadczenia itp.
- brak problemów związanych z czasową nieobecnością pracowników działu IT w firmie,

Outsourcing usług IT może być realizowany w oparciu o tzw. przetwarzanie danych w chmurze (ang. *cloud computing*).

4. Definicja przetwarzania w chmurze

Pochodzenie terminu *cloud computing* jest niejasne. Wydaje się jednak, że może on wynikać z praktyki stosowania rysunków, w których w diagramach informatycznych do oznaczenia sieci i systemów łączności, przedstawiano obłoki. Takie chmury były używane, jako metafora, aby przedstawić pewną abstrakcję.

Cloud computing, czyli przetwarzanie w chmurze, chmury obliczeniowe, inaczej rozproszone środowisko obliczeniowe, jest to model przetwarzania danych, oparty na korzystaniu z usług dostarczonych przez zewnętrzne przedsiębiorstwa lub działy firmy. Funkcjonalność jest tu rozumiana jako usługa, która daje użytkownikowi pewną wartość dodaną. Jest ona oferowana przez odpowiednie oprogramowanie wraz z konieczną infrastrukturą. Takie podejście oznacza eliminację konieczności zakupu licencji, instalowania oraz administrowania oprogramowaniem. Klient płaci za użytkowanie określonej usługi, np. za możliwość korzystania z pakietu graficznego. Nie kupuje sprzętu ani oprogramowania.

Termin *cloud computing* jest związany z pojęciem wirtualizacji. Model ten historycznie wiąże się z przetwarzaniem w sieci internetowej, gdzie wiele systemów udostępnia usługi, korzystając z podłączonych zasobów. Różnica jednak polega na tym, że w *cloud computing* ma się do czynienia z podążaniem zasobów za potrzebami usługobiorcy.

Teoretycznie zakłada się, że firmy nie będą musiały utrzymywać własnej, często skomplikowanej i kosztownej infrastruktury informatycznej oraz personelu do jej obsługi i jednocześnie będą mogły podnieść elastyczność i dostępność systemów informatycznych.

Filozofia *cloud computing* polega na przeniesieniu całego ciężaru świadczenia usług IT (danych, oprogramowania lub mocy obliczeniowej) na serwer i umożliwienie stałego dostępu do niego przez komputery klienckie. Dzięki temu bezpieczeństwo świadczenia usług nie zależy od tego, co stanie się z komputerem klienckim. Zalety takiego rozwiązania to:
- zmniejszenie kosztów użytkowania,
- zwiększenie bezpieczeństwa danych,
- rozsądne rozłożenie zasobów obliczeniowych,
- możliwość korzystania z usługi z wielu terminali – stacji roboczych,
- i in.

5. Praktyczny przykład przetwarzania w chmurze

Klient chciałby skorzystać z najnowszej wersji pakietu Corel Draw. Sam ten program jest bardzo drogi, a klient potrzebuje popracować z nim tylko przez krótki okres czasu. W takim przypadku zakup Corela wydaje się niepotrzebną inwestycją. Oczywiście można skorzystać z takiego oprogramowania u znajomego, który posiada ten program. Jednak możliwe jest rozwiązanie tego problemu w inny sposób.

Przedsiębiorstwo IT sprzedawałoby usługę polegającą na czasowym podłączeniu się do serwera, na którym zostałby zainstalowany pakiet Corel Draw. Klient za pośrednictwem usługi terminalowej, czyli pulpitu zdalnego odpłatnie łączyłby się z takim serwerem. Korzystałby z zainstalowanego tam oprogramowania, a następnie kopiowałby na swój komputer efekt końcowy swojej pracy. Oczywiście po pewnym czasie mógłby zmodyfikować taki plik graficzny korzystając z podobnej usługi u tego samego lub innego dostawcy technologii przetwarzania w chmurze.

6. Cechy przetwarzania w chmurze

Przetwarzanie w chmurze wiąże się z pojęciem wirtualizacji. Dzięki temu możliwe jest stosunkowo proste przenoszenie usługi fizycznie z jednego serwera na inny, zwiększanie jego pamięci itp.

Niewątpliwą zaletą jest niezależność lokalizacji takiego serwera. Użytkownicy mogą się do niego połączyć z dowolnego miejsca, gdzie dostępny jest Internet.

Część zasobów komputerów wykorzystywanych jest w bardzo niewielkim stopniu, rzędu 10-20%. Zatem, znacząca większość dostępnych zasobów infrastruktury i sprzętu pozostaje niewykorzystana. Przetwarzanie w chmurze pomaga efektywniej wykorzystać dostępne zasoby np. poprzez uruchomienie i udostępnienie, na jednym serwerze, kilku wirtualnych maszyn, symulujących działanie kilku całkowicie niezależnych komputerów.

Cloud computing ma pięć kluczowych atrybutów, które dają mu pewną przewagę nad podobnymi technologiami [2]:
- współdzielone zasoby (ang. *shared resources*),
- duża skalowalność,
- elastyczność,
- płatność jedynie za wykorzystywane zasoby (ang. *pay as you go*),
- użytkownicy sami określają, jakich zasobów potrzebują.

7. Sposoby realizacji usług przetwarzania w chmurze

Chmura obliczeniowa jest to model przetwarzania danych oparty na użytkowaniu usług dostarczonych przez zewnętrzne organizacje. Funkcjonalność jest tu rozumiana, jako usługa (dająca wartość dodaną użytkownikowi) oferowana przez dane oprogramowanie (oraz konieczną infrastrukturę). Oznacza to eliminację

konieczności zakupu licencji czy konieczności instalowania i administracji oprogramowaniem. Konsument płaci za użytkowanie określonej usługi, np. za możliwość korzystania z arkusza kalkulacyjnego. Nie musi dokonywać zakupu sprzętu ani oprogramowania. Termin „chmura obliczeniowa" związany jest z pojęciem wirtualizacji.

Chmura obliczeniowa to, według jednej z teorii, przeniesienie pewnych zasobów (serwerów, danych, aplikacji) z przedsiębiorstwa lub serwerowni w inne miejsce i to bez względu na to, czy takie przeniesienie będzie dotyczyło tylko sprzętu, czy to będzie maszyna wirtualna, czy to będą dane, czy też cała aplikacja.

Najbardziej rozpowszechnione formy chmury obliczeniowej:

- najstarszą i najprostszą formą usług w „chmurze" jest tzw. kolokacja, która polega udostępnieniu klientowi miejsca w serwerowni, zasilania, klimatyzacji oraz możliwości podłączenia do Internetu. W takim przypadku to sam klient dba i dokonuje zakupu potrzebnego sprzętu, zabezpieczeń (np. firewall), systemu operacyjnego, oprogramowania i aplikacji. W tym rozwiązaniu płaci się jedynie za użyczenie miejsca w serwerowni.
- zapewnienie sprzętu przez dostawcę IaaS (ang. *Infrastructure as a Service*), czasem nazywane HaaS (ang. *Host as a Service*) jest bardziej zaawansowanym rozwiązaniem usługi chmurowej. Dostawca udostępnia sprzęt i dodatkowo czasem również zabezpieczenia. Klient musi dostarczyć system operacyjny, oprogramowanie i potrzebne aplikacje. Pewną formą takich usług są tzw. serwery dedykowane – wtedy płaci się za udostępnienie faktycznego sprzętu. Usługodawcy mogą również oferować tzw. maszynę wirtualną – w takim przypadku klient płaci za faktycznie zużytą moc serwerów.
- platforma aplikacyjna, jako usługa PaaS (ang. *Platform as a Service*) jest kolejnym poziomem usługi chmurowej. Tutaj klient nie martwi się o utrzymanie i zarządzanie systemem operacyjnym, tylko zajmuje się pisaniem aplikacji i ich utrzymaniem. Dostawca zapewnia sieci, serwery i pamięci masowe. Usługa PaaS może obejmować rozwiązania do projektowania, rozwijania, testowania i wdrażania, a także różne usługi. Taką usługę zazwyczaj rozlicza się na podstawie zużycia zasobów (czasu procesora, miejsca na dysku, liczby zapytań lub transferu danych).
- oprogramowanie, jako usługa SaaS (ang. *Software as a Service*), czasem nazywane, jako „oprogramowanie na żądanie" (ang. *on-demand software*), jest to rozwiązanie, w którym dostawca zajmuje się zarówno sprzętem, systemem operacyjnym aż do finalnej aplikacji. Zaangażowanie klienta ogranicza się do korzystania z określonej aplikacji i jej funkcjonalności. W takim przypadku zazwyczaj ponosi się opłatę za każdego użytkownika za miesiąc korzystania z aplikacji. Niewątpliwym mankamentem takiego rozwiązania jest to, że klient nie może nic zmienić w takiej aplikacji, ani nie ma wpływu (przynajmniej decydującego) na jej rozwój. SaaS stał się wspólnym modelem dostarczania rozwiązań dla wielu zastosowań biznesowych, w tym dla księgowości, współpracy, zarządzaniem relacjami z klientem CRM (ang. *customer relationship management*), fakturowania
  i in. Warto podkreślić ważność usługi SaaS. W najprostszym wydaniu można założyć, że obecnie zakupione oprogramowanie starzeje się w bardzo szybkim tempie. W przedsiębiorstwach, co pewien czas konieczny byłby zakup nowych wersji systemu operacyjnego, aplikacji biurowych, oprogramowania antywirusowego i innych pomimo tego, że dotychczasowe oprogramowanie nadal działałoby poprawnie. Jednak nowsze stawałoby się standardem. Dlatego również okresowo konieczne byłoby przeinstalowywanie całego systemu operacyjnego na komputerach. Dlatego korzystanie z najbardziej aktualnych wersji oprogramowania „wynajmowanych" przez dostawcę usługi SaaS wydaje się być jak najbardziej racjonalnym działa-

Oprócz najpopularniejszych rozwiązań chmurowych, wymienionych wcześniej, można również wyróżnić:

- Przechowywanie (składowanie), jako usługa STaaS (ang. *Storage as a service*) jest to model biznesowy, w którym duża firma wynajmuje miejsce w infrastrukturze pamięci masowej dla mniejszej firmy lub usługi. STaaS, jako wygodnym sposobem zarządzania kopiami zapasowymi. Podstawową korzyścią, w takim przypadku, jest oszczędność fizycznej przestrzeni magazynowej. Dostawca usługi STaaS zgadza się wynająć przestrzeń pamięci za określony koszt każdego gigabajta wykorzystywanego do przechowywania danych i koszt transferu danych. Jeżeli dane firmowe kiedykolwiek zostałyby uszkodzone lub utracone, administrator sieci może skontaktować się z dostawcą STaaS i poprosić o kopię danych. Storage as a Service jest ogólnie postrzegane jako dobra alternatywa dla małych i średnich przedsiębiorstw, które nie mają wystarczającego kapitału lub personelu technicznego do wdrożenia i utrzymania własnej infrastruktury pamięci masowej. STaaS jest także promowane, jako sposób, dla wszystkich przedsiębiorstw, do ograniczenia ryzyka w przechowywaniu i odzyskiwaniu danych.
- Bezpieczeństwo, jako usługa SECaaS (ang. *Security as a service*) to model outsourcingu zarządzania bezpieczeństwem. Zazwyczaj SECaaS obejmuje takie aplikacje jak dostarczane przez Internet zaktualizowane oprogramowanie antywirusowe. W takim przypadku klient nie musi aktualizować bazy wirusów ani wersji programu swojego oprogramowania antywirusowego – przez Internet otrzymuje najnowszą, najbardziej aktualną wersję.
- Dane, jako usługa DaaS (ang. *Data as a service*), jest podobne jak oprogramowanie, jako usługa SaaS. DaaS opiera się na koncepcji, że produkt, w tym przypadku dane, mogą być dostarczane na żądanie niezależnie od geograficznego lub organizacyjnego oddzielenia dostawcy usługi i konsumentów. Można mówić, że usługa DaaS polega na wynajmowaniu danych, które klient wykorzystuje w realizowanych u siebie procesach biznesowych.
- Procesy biznesowe, jako usługa BPaaS (ang. *Business process as a service*) polega na wykonywaniu przez usługodawcę podstawowych procesów biznesowych dla klienta. BPaaS pozwala przedsiębiorstwom i organizacjom na dostęp do zasobów różnych technologii i usług niezbędnych do realizacji, wdrożenia, szkolenia i zarządzania krytyczną technologią dla korporacji, bez ogromnych nakładów kapitałowych.
- Środowisko testowe, jako usługa TEaaS (ang. *Test environment as a service*), zwane jest również, jako „środowisko testowe na żądanie" (ang. *on-demand test environment*). Takie rozwiązanie zazwyczaj rozliczane jest w ramach miesięcznego lub rocznego abonamentu. Dla firm kłopotliwe wydaje się utrzymanie własnego środowiska testowego. Usługa TEaaS polega na wynajęciu takiego środowiska od innego przedsiębiorstwa.
- Pulpit, jako usługa DaaS (ang. *Desktop as a service*) – umożliwia dostęp do systemu operacyjnego i aplikacji za pośrednictwem pulpitu zdalnego lub innej usługi terminalowej z urządzeń (np. smartfonów), których zdolności sprzętowe są zbyt małe
  i uniemożliwiają uruchomienie takiego oprogramowania. Model pulpit, jako usługa, umożliwia wielu użytkownikom dostęp do wielu zindywidualizowanych pulpitów, znajdujących się na jednym centralnym serwerze. Taki serwer może, ale nie
- API (ang. *Application Programming Interfaces),* czyli interfejs programowania aplikacji, jako usługa APIaaS (ang. *API as a service*), API to ściśle określony zestaw reguł i ich opisów, w jaki programy komunikują się między sobą, definiowany na poziomie kodu źródłowego.

Czasami można również wyróżnić wymieszanie tego, co jest obecnie (czyli serwery w firmie, aplikacje na komputerach) z tym co daje chmura (serwery i aplikacje poza firmą). Takie rozwiązanie nazywa się Software + Services. Ponieważ nie zawsze chmura jest najlepszym rozwiązaniem, może istnieć potrzeba korzystania czasem z klasycznego oprogramowania (ang. *Software*), z drugiej jednak strony możliwość skorzystania z tego na zasadzie usługi (ang. *Service*).

Cloud computing może stanowić zysk netto w kwestii bezpieczeństwa i niezawodności systemu i danych – szczególnie dla małych firm ze starzejącymi się komputerami i danymi przecho-

wywanymi na dyskach twardych, które rzadko, jeżeli w ogóle, tworzą jakąkolwiek kopię zapasową.

Można wyróżnić następujące typy chmur obliczeniowych: prywatne, publiczne, dedykowane i hybrydowe (chmury mieszane – połączenie chmur prywatnych z publicznymi).

Chmura prywatna (ang. *private cloud*) to rodzaj usługi chmury obliczeniowej, w której usługodawcą jest dział IT firmy, w której inne działy są klientami takiej chmury. Przedsiębiorstwo całkowicie kontroluje taką chmurę. W takim przypadku zasoby przedsiębiorstwa znajdują się całkowicie pod zarządem przedsiębiorstwa. Chmury prywatne zazwyczaj mogą być udostępniane w dużych przedsiębiorstwach, które posiadają wystarczające zasoby informatyczne oraz wymagany personel do obsługi takiego przedsięwzięcia. Technicznie, w serwerowni danego przedsiębiorstwa instaluje się oprogramowanie systemowe do zarządzania usługami, obsługi maszyn wirtualnych oraz potrzebne aplikacje.

Chmura publiczna (ang. *public cloud*) to rodzaj usługi chmury obliczeniowej, w której infrastruktura jest własnością pojedynczej organizacji, która sprzedaje usługi cloud skierowane do ogółu społeczeństwa lub konkretnych branż. Chmura publiczna w dużym uproszczeniu polega na dzierżawieniu środowiska i polega na współdzieleniu zasobów (serwera, platformy lub aplikacji) pomiędzy różnych użytkowników. Klient określa, jakie zasoby oraz parametry środowiska interesują go (moc obliczeniowa, pamięć itp.) i za nie płaci. Zamówione zasoby są dostępne „na żądanie" (ang. *on demand*). Przykładowo użytkownicy korzystający z poczty Gmail używają chmury dostarczanej przez firmę Google.

Chmura dedykowana to taka wersja chmury, która nie jest dostępna dla każdego. Zazwyczaj fizycznie wydziela się część centrum danych (ang. *DataCenter*) wyłącznie na potrzeby danego klienta. Takie zasoby w żaden sposób nie są współdzielone. Klient ma stuprocentową pewność, że określone zasoby są przeznaczone tylko i wyłącznie dla niego. Chmura dedykowana jest rozwiązaniem droższym od usług w chmurze publicznej, jednak znacznie tańszym od budowy własnej chmury prywatnej o podobnej funkcjonalności.

Przetwarzanie w chmurze przyczynia się do przekształcenia dotychczasowych kosztów inwestycyjnych w koszty operacyjne. Dzięki temu obniżają się koszty i bariery wejścia na rynek. Infrastruktura zazwyczaj dostarczana jest przez tzw. stronę trzecią.

8. Bezpieczeństwo rozwiązań chmurowych

Bezpieczeństwo rozwiązań chmurowych (ang. *cloud computing security* lub ang. *cloud security*) ewoluuje od pojęć bezpieczeństwa komputerowego, bezpieczeństwa sieci oraz ogólnie pojętego bezpieczeństwa informacji. Odnosi się do szerokiego zestawu polityk, technologii i kontroli, wdrożonych w celu ochrony danych, aplikacji i związanej z nimi infrastruktury w *cloud computing*. Bezpieczeństwa chmury (ang. *cloud security*) nie należy mylić z ofertą oprogramowania zabezpieczającego, które dostępne jest „w chmurze".

Bezpieczeństwo w chmurze można podzielić na dwie podstawowe kategorie:

- problemy bezpieczeństwa napotykane przez przedsiębiorstwa świadczące usługi chmurowe,
- problematyka zapewnienia bezpieczeństwa swoim klientom.

Problematyka bezpieczeństwa chmurowego dotyczy trzech obszarów:

- bezpieczeństwa i prywatności, dotyczy takich zagadnień jak:
  a) system do zarządzania tożsamością, aby każdemu klientowi udostępnić odpowiednią usługę (infrastrukturę),
  b) bezpieczeństwo fizyczne dotyczące ograniczeń w dostępie do serwerów własnych oraz klienta (dostęp taki musi być udokumentowany),
  c) dostępność – dostawcy usług chmurowych muszą zapewnić klientów, że będą oni mieli przewidywalny i regularny dostęp do swoich danych i aplikacji),
  d) bezpieczeństwo aplikacji,
- zapewnienie prywatności – operatorzy i dostawcy rozwiązań chmurowych muszą zapewnić, że wszystkie dane krytyczne (dane osobowe, numery kart kredytowych itp.) są odpowiednio maskowane i tylko autoryzowani klienci mają do nich dostęp w całości, ponadto takie dane jak personalia, cyfrowa tożsamość, wszelkie dane oraz aktywność klientów w chmurze muszą być chronione.
- zgodności (ang. *compliance*), dotyczy to takich obszarów, jak zapewnienie ciągłości biznesowej oraz odzyskiwania danych, aby zapewnić klienta, że usługa będzie utrzymywana i świadczona również w przypadku wystąpienia klęski żywiołowej lub sytuacji awaryjnej oraz, że każda z utraconych danych może zostać odzyskana. Ponadto dostawcy rozwiązań chmurowych muszą współpracować ze swoimi klientami i przechowywać odpowiednio zabezpieczone rejestry (ang. *logs*) tak długo, jak tego oczekuje klient oraz tak, aby były one dostępne do celów kryminalnych. Do tego dochodzą unikalne wymogi jakościowe takie, jak zapewnienie, że po opuszczeniu chmury przez klienta żadne z jego danych nie mogą pozostawać w tym systemie, na którym on pracował, ani nawet w tym samym centrum danych.
- kwestie prawne i umowne dotyczą takich zagadnień jak negocjowanie warunków odpowiedzialności związanych z utratą danych, własnością intelektualną oraz końcem świadczenia usługi.

Niebagatelna jest kwestia, co stanie się z plikami i danymi pozostawionymi na zdalnym serwerze po zakończeniu świadczenia usługi *cloud computing*. W przypadku niektórych przedsiębiorstw np. banków lub niektórych typów danych np. tajnych, poufnych, wrażliwych, krytycznych należy zastosować odpowiednie procedury zabezpieczające. Często bowiem jedyną drogą wyjścia dokumentu wewnętrznego z banku jest niszczarka.

W przypadku bezpieczeństwa chmury chodzi o to, aby nieupoważnione osoby trzecie nie miały dostępu do informacji oraz danych związanych ze świadczeniem usługi chmurowej. Istotne jest bowiem zachowanie prywatności i poufności danych przechowywanych w chmurze, zwłaszcza w kwestii dostępu do nich osób niepowołanych. Szczególnie wrażliwa jest kwestia przetwarzania danych poufnych i wrażliwych np. przez sądy, urzędy, banki lub dane handlowe i krytyczne przez firmy. Takie podmioty kończąc przetwarzanie takich danych muszą mieć gwarancję bezpowrotnego ich usunięcia. Oczywiście zdarza się, że podczas przetwarzania danych następuje zarwanie połączenia pomiędzy komputerem roboczym, a serwerem, na którym pozostają poufne dane. W takim przypadku wszelkie pliki i dane zostają tam i mogą dostać się w niepowołane ręce.

Korzystanie z takich usług jak przetwarzanie w chmurze (ang. *cloud computing*) oraz outsourcing, oprócz niewątpliwych zalet takich, jak większa efektywność, dostęp do bardziej wykwalifikowanego personelu, niż dostępny jest w przedsiębiorstwie, wiążą się z niebezpieczeństwem pewnego uzależnienia od zewnętrznych dostawców usług chmurowych, co należy również brać pod uwagę. Wiąże się to również z niebezpieczeństwem uzależnienia od innych firm np. dostawców usług informatycznych (zapewniających dostęp do sieci internetowej) zarówno przedsiębiorstwa zamawiającego, jak również usługodawców. Jeżeli wykorzystuje się zasoby dostępne w przedsiębiorstwie również można mówić o pewnym stopniu uzależnienia, natomiast występuje ono w mniejszym stopniu.

Jeżeli aplikacje zainstalowane są na stacji roboczej to w przypadku jej uszkodzenia niemożliwa jest praca z aplikacją. W tym przypadku korzystanie z aplikacji uzależnione jest od stanu technicznego własnej stacji roboczej albo od jej możliwości obliczeniowych. W przypadku wykorzystywania *cloud computing* zmienia się niezawodność świadczenia usług. Istnieje możliwość podłączenia się do zasobów zdalnych z wykorzystaniem usług terminalowych (pulpitu zdalnego) z bardzo wielu komputerów podłączonych do Internetu (oczywiście pula komputerów, z których można podłączyć się do usługi może być dowolnie zawężona).

Ponieważ usługi *cloud computing* udostępniane są za pośrednictwem sieci, są one podatne na ataki w takich sieciach. Można wyróżnić następujące ataki [1]:

- odmowa usługi (ang. *denial of service*),
- nasłuch – w podsłuchanych pakietach napastnik może przechwycić poufne dane,
- skanowanie portów w komputerze – przykładowo port 80 zawsze jest otwarty, ponieważ jest on wykorzystywany przez serwer www,
- stosowanie wstrzykiwania nieprawidłowych poleceń SQL, przykładowo przeglądanie, jaką składnię mają polecenia z WHERE, a następnie wpuszczanie podobnych, z zapisem WHERE 1=1, czyli z zawsze spełnionym warunkiem; w taki sposób można wykasować lub zmodyfikować wszystkie dane w jakiejś tabeli w bazie danych.

Ponadto problemem może być niezabezpieczone lub niekompletne usunięcie danych – konieczne jest należyte i terminowe kasowanie danych. Nie ma większego problemu, jeżeli takie dane pozostają na serwerach dedykowanych, natomiast problem pojawia się w przypadku zasobów współdzielonych.

Wadą usług chmurowych jest uzależnienie klienta od takich usług oraz możliwość ich niedostępności w przypadku przestojów serwera.

Niektóre osoby obawiają się, że dostawcy usług chmurowych nie będą w stanie poradzić sobie w przypadku zamówień na dużą skalę oraz że infrastruktura dostawcy może nie być do tego dostosowana [2].

9. Uzasadnienie zasadności stosowania technologii chmurowych

Nasuwa się proste pytanie, po co komplikować infrastrukturę informatyczną przedsiębiorstwa i korzystać z usług *cloud computing*. Otóż żaden komputer (i dane na nim zgromadzone) podłączony do Internetu nie jest bezpieczny nawet, jeżeli „połączony" jest za pośrednictwem technologii bezprzewodowej. Zatem aby chronić zasoby firmowe w przedsiębiorstwach potrzeba jest zatrudnienia odpowiednio wysoko wykwalifikowanego administratora sieci specjalizującego się w zabezpieczaniu takich zasobów przed atakami. Oczywiście wynagrodzenie takiego pracownika zazwyczaj jest bardzo wysokie, ponadto w czasie, kiedy jest on na urlopie lub zwolnieniu lekarskim nikt nie chroni formowej sieci informatycznej. Ponadto taki pracownik może po jakimś czasie zmienić pracę i ujawnić pewne dane.

Dodatkowo, co pewien czas zmieniają się systemy operacyjne, programy pakietu biurowego: arkusza kalkulacyjnego, edytora tekstów, baz danych itp. Zatem cyklicznie, co pewien czas, zachodzi konieczność zakupu nowych wersji oprogramowania mimo, że stare działają prawidłowo.

10. Opis systemu AMR

W jednym koncernie energetycznym w Polsce został wdrożony centralny system pomiarowo-rozliczeniowy typu AMR, bazujący na technologii platforma aplikacyjna, jako usługa PaaS (ang. *Platform as a Service*), pracującej, jako chmura prywatna (ang. *Private Cloud*).

System AMR składał się z serwera bazodanowego z oprogramowaniem ORACLE, serwera aplikacyjnego, serwerów akwizycyjnych (pracujących, jako wirtualne maszyny po kilka na jednym komputerze) oraz kilkunastu stacji roboczych, czyli komputerów poszczególnych pracowników, którzy mogli łączyć się do serwera aplikacyjnego. Na serwerze aplikacyjnym zostało zainstalowane oprogramowanie klienckie umożliwiające pracę z systemem AMR. Do serwera tego łączyli się użytkownicy z miejscowości odległych do okolo 120 km od jego lokalizacji. Każdy z pracowników mógł zalogować się tam za pośrednictwem terminalu (pulpitu zdalnego).

System służył do odczytu kilkuset elektronicznych liczników energii elektrycznej, mierzących energię:

- przepływającą przez punkty graniczne: dostarczaną od PSE oraz wymienianą z sąsiednimi przedsiębiorstwami dystrybucyjnymi,
- zużywaną przez klientów zakwalifikowanych, jako wielki odbiór,
- zużywaną przez odbiorców, którzy zmienili sprzedawcę energii,
- z niektórych punktów sieciowych, aby możliwe było bilansowanie niektórych fragmentów sieci elektroenergetycznej.

System również generował wymagane raporty rozliczeniowe. System również dokonywał rozliczeń ilościowych za energię, wyznaczał wartość poszczególnych składników taryfowych, a następnie takie dane eksportował do systemu billingowego.

11. Doświadczenia wykorzystania systemu AMR z przetwarzaniem w chmurze

Na początku zauważono, że system nie jest przystosowany do jednoczesnej pracy kilku użytkowników. Konieczne okazały się zatem modyfikacje niektórych aplikacji. Kolejnym zagadnieniem było uporządkowanie plików z logami, czyli z informacjami, w jaki sposób każdy z użytkowników korzystał z aplikacji.

Konieczna była zmiana funkcjonowania modyfikowania podobnych danych przez dwóch użytkowników jednocześnie. Okazało się, że niektóre z aplikacji uniemożliwiały jednoczesne np. dodawanie liczników energii w tym samym czasie, przez kilku użytkowników. Zmiany wprowadzone przez jednego kasowały to, co wprowadził drugi.

Dla pracowników nowością było korzystanie z aplikacji za pośrednictwem pulpitu zdalnego. Usługa zdalnego pulpitu umożliwiała mapowanie, czyli dostęp do własnych dysków przez osobę, która zalogowała się do serwera aplikacyjnego w jej sesji, czyli dyski takie nie były widoczne przez osobę równocześnie zalogowaną, jako inny użytkownik. Umożliwiała również kopiowanie zawartości schowka. Pomimo tych zalet pracownicy narzekali, że nie można było w prosty sposób skopiować danych z wygenerowanego raportu i wkleić do własnego arkusza kalkulacyjnego – kopiowanie schowka za pośrednictwem pulpitu zdalnego trwało dość długo. Oczywiście raport taki można było zapisać na dysk sieciowy i otworzyć na własnej stacji roboczej, ale było to utrudnienie w stosunku do wcześniejszego rozwiązania.

Czasami podczas awarii sieci komputerowej w koncernie energetycznym zwracano uwagę, że nie można było pulpitem zdalnym połączyć się z serwerem aplikacyjnym i pracować z systemem pomiarowo-rozliczeniowym. W takim przypadku dane i dokumenty stają się całkowicie niedostępne. Niemożliwa jest realizacja żadnych procesów biznesowych, do wspierania których został przeznaczony system AMR. Zapominano jednak, że jeżeli wcześniej aplikacje byłyby zainstalowane na każdej stacji roboczej i występowała awaria sieci komputerowej, to i tak nie można byłoby podłączyć się do bazy danych i pracować z aplikacją.

Obciążenie serwera aplikacyjnego i całego systemu pomiarowo-rozliczeniowego zmieniało się w różnych dniach miesiąca. Największe było na początku każdego miesiąca, kiedy konieczne było odczytanie i przetworzenie wszystkich danych pomiarowych z poprzedniego miesiąca, a następnie wystawienie takich danych do systemu bilingowego. Pomimo znacznego obciążenia nie zauważono problemów z pracą z aplikacją za pośrednictwem usługi terminalowej. Czasami takie rozwiązanie okazywało się lepsze, ponieważ wcześniej, kiedy aplikacje znajdowały się na stacjach roboczych czasami traciły łączność z bazą danych i konieczne było ich restartowanie.

Niewątpliwą zaletą takiego rozwiązania była łatwość naprawy stwierdzonych usterek oprogramowania. Wdrażany system pomiarowo-rozliczeniowy posiadał tzw. błędy młodości, których było niemało, stąd ogromną korzyścią okazała się konieczność instalowania poprawek tylko na jednym komputerze – serwerze aplikacyjnym. Wcześniej, pomimo zastosowaniu mechanizmu automatycznego podstawiania poprawek tzw. LiveUpdate, czasami oka-

zywało się, że użytkownicy przed tą operacją musieli zamykać wszystkie aplikacje, następnie niekiedy niektórzy z nich mieli okrojone uprawnienia użytkownika dla systemów operacyjnych i proste podstawienie plików lub zarejestrowanie bibliotek w systemie operacyjnym okazywało się nie lada wyzwaniem. Konieczny był wtedy udział dodatkowych administratorów, restartowanie komputerów z nowymi ustawieniami użytkownika lub logowanie się na konto administratora. Było to bardzo czasochłonne i pracochłonne. Nierzadko podstawienie nowej wersji aplikacji na kilkunastu stacjach roboczych zajmowało wiele godzin pracy inżyniera systemowego, czasami również i innych użytkowników. Czasami zapominano o niektórych stacjach roboczych, lub podstawienie nie było możliwe, ponieważ użytkownika nie było w pracy. W konsekwencji zdarzało się, że występowały błędy, ponieważ do bazy danych łączyły się aplikacje w kilku różnych wersjach.

Możliwość szybkiej poprawy aplikacji okazała się wielką zaletą. Technologia *cloud computing* jest bardzo pomocną w dalszym rozwoju systemu, ułatwia jego aktualizowanie i panowanie nad takimi aktualizacjami oraz zapewnia wszystkim użytkownikom dostęp do najnowszych wersji oprogramowania.

12. Rozwiązania chmurowe AMR w świecie

W Danii ma zostać wdrożone pierwsze, w tym kraju, rozwiązanie inteligentnego systemu pomiarowego, bazujące na technologii chmurowej, opracowanego przez firmę Echelon. Odpowiednie oprogramowanie będzie codziennie odczytywać profil obciążenia ze 170 tys. inteligentnych liczników energii. Skuteczność odczytu danych w tym systemie wynosi od 99,7% do 100% [3].

Wydaje się, że wybór technologii chmurowej jest kolejnym dowodem na przewidywaną przez niektórych specjalistów migrację przedsiębiorstw użyteczności i małych przedsiębiorstw w stronę rozwiązań hostowanych. Mniejsze przedsiębiorstwa po prostu nie mają wystarczającej siły roboczej, aby uruchamiać centra danych. Jeżeli zatem potrzebują bardzo zaawansowanego oprogramowania, będą musiały je zdobyć i korzystać z niego poprzez usługi chmurowe, gdzie sprzedawca takiego rozwiązania uzyska efekt skali sprzedając swoje usługi dla wielu przedsiębiorstw.

13. Wnioski

Technologia *cloud computing* jest bardzo ciekawym, przyszłościowym rozwiązaniem. Oczywiście nowe rozwiązanie niesie za sobą również nowe wyzwania w zakresie niezawodności świadczenia takiej usługi, zapewnienia jej bezpieczeństwa oraz poufności przetwarzanych tam danych.

Obecny projekt wdrożeniowy związany z wykorzystaniem rozwiązań chmurowych okazał się korzystny. Było to jedno z pierwszych wdrożeń tego typu przez dostawcę rozwiązań IT, ale pokazało ono wiele korzyści płynących z takiego rozwiązania. Przetwarzanie w chmurze okazuje się perspektywicznym rozwiązaniem, oczywiście również niosącym za sobą różne zagrożenia.

14. Literatura

[1] Danish Jamil, Hassan Zaki: Cloud computing security. International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 4 April 2011, ISSN: 0975-5462.

[2] Carlin S., Curran K.: Cloud computing security. 14 International Journal of Ambient Computing and Intelligence, 3(1), 14-19, January-March 2011.

[3] Denmark's First Cloud-Based Smart Grid Solution Relies on Echelon Control Networking Technology. Business Wire, 31 August 2011, http://www.businesswire.com/news/home/20110831005602/en/Denmark%25E2%2580%2599s-Cloud-Based-Smart-Grid-Solution-Relies-Echelon&usg=ALkJrhgCfEifanuHiW_W4J1DYJYyFg9mqA

otrzymano / received: 31.10.2012
przyjęto do druku / accepted: 03.12.2012 *artykuł recenzowany / revised paper*

INFORMACJE

Nowa inicjatywa PAK

Na stronie internetowej Wydawnictwa PAK został utworzony dział: **Niepewność wyników pomiarów** w którym są zamieszczane aktualne informacje dotyczące problemów teoretycznych i praktycznych związanych z szacowaniem niepewności wyników pomiarów. W dziale znajdują się:

- aktualne informacje o publikacjach dotyczących niepewności wyników,
- informacje o przedsięwzięciach naukowo–technicznych i edukacyjnych, o tematyce związanej z niepewnością,
- dokumenty dotyczące niepewności,
- pytania do ekspertów (FAQs).

Zapraszamy:

- autorów opublikowanych prac dotyczących niepewności o nadsyłanie tekstów do zamieszczenia w tym dziale,
- organizatorów przedsięwzięć naukowo – technicznych lub edukacyjnych do nadsyłania informacji o imprezach planowanych lub odbytych,
- zainteresowanych zagadnieniami szczegółowymi do nadsyłania pytań do ekspertów.

Materiały mogą mieć formę plików lub linków do źródeł. Warunkiem zamieszczenia w tym dziale strony internetowej PAK materiałów lub linków jest przysłanie do redakcji PAK pocztą zwykłą zgody właściciela praw autorskich na takie rozpowszechnienie. Zamieszczanie i pobieranie materiałów i informacji w tym dziale strony internetowej jest bezpłatne. Redakcja PAK będzie nadzorować zawartość działu, ale za szczegółowe treści merytoryczne odpowiadają autorzy nadsyłanych materiałów.

Tadeusz SKUBIS
Redaktor naczelny Wydawnictwa PAK