Raport Forum Technologii Bankowych
przy Związku Banków Polskich

CLOUD COMPUTING
w sektorze finansowym

Autorzy

Ewa Dybka
Dariusz Falkowski
Robert Gajda
Maciej Gawroński
Martyna Kubiak
Wojciech Małek
Przemysław Mazurkiewicz
Piotr Piskorz
Janusz Zawiła-Niedźwiecki
Michał Zgajewski
(przewodniczący zespołu autorskiego)

FORUM TECHNOLOGII BANKOWYCH

ZWIĄZEK BANKÓW POLSKICH

Obserwując rozwój technologii i jej ewolucję, ilość przetwarzanych, kumulowanych i gromadzonych danych, można stwierdzić, że „chmura" to przyszłość. Cloud computing dynamicznie rozwija się na świecie, plany Komisji Europejskiej zmierzają do upowszechnienia tej usługi, a dostawcy zapewniają wysoki poziom bezpieczeństwa. Jednak bezpieczeństwo usług w chmurze budzi największą obawę, w szczególnościa dla sektora finansowego.

Każda nowa technologia, w tym również wspominany model dostarczania usług, wiąże się z wieloma korzyściami, ale również z pewnymi zagrożeniami. Należy pamiętać, że dane o klientach polskich banków będę przetwarzane poza siedzibą banku, często również poza granicami kraju. Dlatego istotne jest przygotowanie właściwych przepisów prawa, które zagwarantują ochronę danych osobowych oraz informacji objętych tajemnicą bankową. Ważne są identyfikacja zagrożeń i aktywne im przeciwdziałanie. Pojawia się coraz więcej publikacji i dokumentów dotyczących implementacji tego rozwiązania oraz kwestii ochrony danych i prywatności, mających na celu przyczynienie się do zmniejszenia zagrożeń związanych z wykorzystaniem usług przetwarzania w chmurze.

Mając na uwadze istniejące wątpliwości, Grupa Forum Technologii Bankowych przy Związku Banków Polskich ds. Cloud computing, wychodząc naprzeciw oczekiwaniom bankowców, opracowała dokument poświęcony zagadnieniu chmury obliczeniowej w sektorze finansowym.

Przedstawiona publikacja ma charakter edukacyjny i jej priorytetem jest pomoc w przygotowaniu kierunków prac i rozwoju związanego z wdrożeniem „chmury" w bankach.

Autorzy

Spis treści

Wstęp

Cel dokumentu

Niniejszy raport dotyczy zastosowania przetwarzania w chmurze[1] (*Cloud computing*) w sektorze finansowym. Został opracowany w celu uporządkowania wiedzy o zagadnieniu chmury obliczeniowej oraz o uwarunkowaniach stosowania takiej formy usług informatycznych. W zamierzeniu autorów, raport ma otwierać dyskusję o przetwarzaniu w chmurze w instytucjach sektora finansowego w Polsce.

Mamy nadzieję, że raport ten spotka się z zainteresowaniem i odzewem jego adresatów. W miarę potrzeb raport może być aktualizowany i uzupełniany.

Adresaci

Podstawowymi adresatami raportu są menedżerowie podmiotów sektora finansowego, a zwłaszcza odpowiedzialni za obszary: finanse, kreowanie produktów i sprzedaż, ryzyko operacyjne, aspekty prawne, usługi i technologie informatyczne.

Raport przydatny będzie również osobom odpowiedzialnym za nadzór nad sektorem finansowym, jak i każdemu, kto będzie chciał poszerzyć lub zweryfikować swoją wiedzę o przetwarzaniu w chmurze.

Raport jest opublikowany na stronie internetowej Związku Banków Polskich.

Rozpowszechnianie i odpowiedzialność za rekomendacje

Zaproszeni przez ZBP do pracy nad raportem, eksperci dołożyli staranności, aby na miarę ich wiedzy, obowiązujących przepisów oraz dostępnych norm i standardów, zapewnić odpowiedni poziom niniejszemu dokumentowi.

Raport może być rozpowszechniany w całości lub we fragmentach (w tym cytowany), pod następującymi warunkami:

- należy podawać następujący tytuł raportu: *Raport Forum Technologii Bankowych przy Związku Banków Polskich – Cloud computing w sektorze finansowym*;
- należy podawać wszystkich autorów raportu;
- bez odrębnej zgody FTB ZBP nie można pobierać wynagrodzenia za rozpowszechnianie raportu.

[1] Pojęcie to wzięło się z tradycji rysowania na schematach informatycznych łączności internetowej jako chmury.

Słownik pojęć

Definicje

API – (*application program interface*) interfejs programowy aplikacji – sposób komunikacji programu komputerowego z innym programem komputerowym.

BPaaS – (*business process as a service*) usługa polegająca na obsłudze procesu biznesowego klienta za pomocą oprogramowania udostępnianego zdalnie. Przeważnie jest dostarczana łącznie z usługami IaaS, PaaS oraz SaaS.
Sposób, w jaki określa się przyszły najbardziej wyrafinowany z punktu widzenia użytkownika model usług przetwarzania w chmurze polegający na tym, iż korzysta się z dostępu do w pełni oprzyrządowanego procesu biznesowego dostępnego na zasadach chmury.

Chmura hybrydowa – przetwarzanie w chmurze łączące zasoby chmury prywatnej i publicznej.

Chmura prywatna – współdzielone z innymi użytkownikami zasoby, które są dynamicznie dostarczane na wyłączny użytek jednej organizacji.

Chmura publiczna – współdzielone z innymi użytkownikami zasoby, które są dynamicznie dostarczane przez zewnętrznego dostawcę za pomocą Internetu.

Cloud computing – model świadczenia usług przetwarzania danych, pozwalający na dostęp na żądanie, przez sieć, do dzielonej puli zasobów IT (sieciowych, serwerowych, pamięci masowych, aplikacji i usług). Eksperci firmy Gartner definiują Cloud computing jako: „rodzaj przetwarzania, gdzie za pomocą Internetu wielu użytkowników otrzymuje skalowalne i elastyczne usługi IT”[2].

DaaS – (*data center as a service*) usługa polegająca na zdalnym dostarczaniu pełnej funkcjonalności ośrodka komputerowego. Termin rzadko spotykany, obecnie zastąpiony pojęciem chmury prywatnej.

FaaS – (*framework as a service*) usługa polegająca na zdalnym dostarczaniu klientowi zbioru (tzw. szkieletu) narzędzi do samodzielnego opracowywania przez klienta dedykowanych rozwiązań. Jest to środowisko, które przylega do SaaS i pozwala na rozszerzanie gotowych funkcjonalności aplikacji udostępnianej w SaaS. Podobnie jak w środowisku PaaS, w ramach FaaS można korzystać jedynie z języków i API dostarczanych przez FaaS.

Funkcja biznesowa – pojedyncza aktywność lub grupa jednorodnych aktywności biznesowych, które spełniają ważną i precyzyjnie określoną rolę zdefiniowaną lub wynikającą ze strategii przedsiębiorstwa.

Grid – system integrujący i zarządzający zasobami będącymi pod kontrolą różnych domen/ośrodków/podmiotów połączonych siecią komputerową.

Host – komputer podłączony do sieci komputerowej używającej protokołu komunikacyjnego TCP/IP, posiadający adres IP. Jeżeli użytkownik komputera łączy się z siecią komputerową, to karta sieciowa lub modem jego komputera otrzymuje adres IP i wtedy staje się hostem. W tym znaczeniu host jest dowolną maszyną, uczestniczącą w wymianie danych za pośrednictwem sieci komputerowej, np. przez Internet.

[2] http://www.gartner.com/technology/research/cloud-computing/index.jsp

Inshoring (lub Onshoring, Backshoring) (*inshore outsourcing*) – (jest przeciwieństwem offshoringu) outsourcing procesów biznesowych przedsiębiorstwa na obszarze kraju.

IaaS – (*infrastructure as a service*) usługa polegająca na zdalnym dostarczaniu klientowi niezbędnych zasobów technicznych oraz usług utrzymania (serwisowania) i administrowania nimi.

Insourcing – (jest przeciwieństwem outsourcingu) przekazanie procesów lub działań biznesowych jednostki, realizowanych w ramach działalności gospodarczej przez zewnętrznych usługodawców/dostawców, do wewnętrznej, wyodrębnionej i wyspecjalizowanej komórki organizacyjnej.

Offshoring (*offshore outsourcing*) – (jest przeciwieństwem inshoringu) przeniesienie wybranych procesów biznesowych przedsiębiorstwa poza granicę kraju przy zachowaniu tej samej grupy klientów.

Outsourcing (*outside-resource-using*) – korzystanie z zasobów zewnętrznych. Koncepcja pochodzi od Henry Forda, który stwierdził, że „Jeśli jest coś, czego nie potrafimy zrobić wydajniej, taniej i lepiej niż konkurenci, nie ma sensu, żebyśmy to robili, i powinniśmy zatrudnić do wykonania tej pracy kogoś, kto zrobi to lepiej niż my".

P2V – (*private to virtual*) – zastąpienie fizycznej infrastruktury informatycznej infrastrukturą wirtualną, a ściślej – przeniesienie oprogramowania systemowego, aplikacyjnego i danych z urządzeń fizycznych na ich wirtualne odpowiedniki.

PaaS – (*platform as a service*) usługa polegająca na zdalnym dostarczaniu klientowi niezbędnych systemów operacyjnych i narzędzi systemowych oraz usług utrzymania (serwisowania) i administrowania nimi jako bazy do przetwarzania aplikacji dedykowanych klienta. Z reguły usługa PaaS jest dostarczana łącznie z usługą IaaS.

Plik ISO – format zapisu danych dysków optycznych.

Proces biznesowy – seria powiązanych ze sobą działań lub zadań, które rozwiązują określony problem gospodarczy lub prowadzą do osiągnięcia określonego efektu gospodarczego.

Przetwarzanie w chmurze – patrz Cloud computing.

SaaS – (*software as a service*) usługa polegająca na zdalnym dostarczaniu klientowi przetwarzania potrzebnych mu aplikacji (uniwersalnych lub dedykowanych) oraz usług utrzymania (serwisowania) i administrowania nimi. Z reguły usługa SaaS jest dostarczana łącznie z usługami IaaS oraz PaaS.

Skrypty – programy napisane w językach skryptowych – wykonywane są wewnątrz pewnej aplikacji, w odróżnieniu od programów („normalnych", nieskryptowych), które wykonują się niezależnie od innych aplikacji.

Sourcing – kompleksowa strategia przedsiębiorstwa definiująca, w jaki sposób i przez kogo obsługiwane będą poszczególne procesy biznesowe, bądź obszary funkcjonalne firmy.

XaaS – (*anything as a service*) rzadko używane określenie odnoszące się do zdalnego dostarczania wszelkiego rodzaju usług (aplikacja, platforma, infrastruktura, telekomunikacja).

Wirtualizacja – parametryczne generowanie w pojedynczym komputerze fizycznym wielu komputerów umownych (wirtualnych) lub w pojedynczej sieci wielu sieci umownych (wirtualnych). Komputery wirtualne zachowują cechy użytkowe komputera fizycznego, natomiast ich użytkownicy mogą korzystać z możliwości separowania swoich zadań i danych.

Skróty

AML	Anti–money-laundering
API	Application Program Interface
BIK SA	Biuro Informacji Kredytowej
BPaaS	Business process as a Service
CAPEM	Capital Expenditures (nakłady inwestycyjne)
DaaS	Data center as a Service
DRP	Disaster Recovery Plan
FaaS	Framework as a Service
FTB	Forum Technologii Bankowych ZBP
GIODO	Generalny Inspektor Ochrony Danych Osobowych
IaaS	Infrastructure as a Service
NIST	National Institute of Standards and Technology
OPEX	Operational Expenditures
PaaS	Platform as a Service
PB	Ustawa Prawo Bankowe
PCI	Peripheral Component Interconnect
RBE	Rada Bankowości Elektronicznej ZBP
RBL	Real-time Blackhole List
ROE	Return on Investment
SaaS	Software as a Service
SAS70	Statement on Auditing Standards No. 70
S/MIME	Secure/Multipurpose Internet Mail Extensions
SOA	Service Oriented Architecture
SSL	Secure Sockets Layer
TCO	Total Cost of Ownership
TLS	Transport Layer Security
UE	Unia Europejska
XaaS	Anything as a Service
ZBP	Związek Banków Polskich

1. Charakterystyka przetwarzania w chmurze

Istotą przetwarzania w chmurze nie jest samo posługiwanie się technologią teleinformatyczną, czyli zasobami sprzętowymi i oprogramowaniem, ale nowy model ich pozyskiwania jako usługi. Najczęściej podaje się definicję NIST (National Institute of Standards and Technology).

Przetwarzanie w chmurze to model świadczenia usług przetwarzania danych, pozwalający na dostęp na żądanie, przez sieć, do dzielonej puli zasobów (sieciowych, serwerowych, pamięci masowych, aplikacji i usług). Zasoby te mogą być zamawiane przez klientów i w odpowiedni sposób konfigurowane w zależności od potrzeb użytkowników oraz dostarczane na żądanie i udostępniane przy minimalnym zaangażowaniu odbiorcy usługi.

W zależności od rodzaju pozyskiwanych zasobów rozróżnia się obecnie trzy podstawowe modele usługi przetwarzania w chmurze:

- infrastructure as a service
- platform as a service
- software as a service

Infrastructure as a service (IaaS) polega na korzystaniu za pośrednictwem sieci, w tym Internetu, ze sprzętu informatycznego (hardware). Takim sprzętem jest predefiniowany wirtualny serwer lub poszczególne jego komponenty, dobierane przez klienta według bieżącej potrzeby, tj.:

- procesor, rozumiany jako udostępnienie zakresu mocy przetwarzania wyrażonej w GHz,
- pamięć operacyjna RAM, o pojemności wyrażonej np. w GB,
- pamięć dyskowa, o pojemności wyrażonej np. w GB.

Korzystając z techniki wirtualizacji serwerów, użytkownik usługi może zbudować strukturę wielopoziomową, połączoną analogicznie wirtualnymi sieciami (VLAN). Na tak przygotowanej infrastrukturze usługobiorca może zainstalować własne oprogramowanie systemowe, bazodanowe oraz aplikacje biznesowe.

Platform as a service (PaaS) posiada funkcjonalność IaaS rozbudowaną do poziomu systemów operacyjnych i baz danych, dostarczając gotowe środowisko do tworzenia, instalowania, przetwarzania i uruchamiania własnych aplikacji biznesowych.

Software as a service (SaaS) – w tym modelu użytkownik otrzymuje ciągły dostęp do aplikacji informatycznych, a płaci jedynie za faktyczne z nich korzystanie. Dostęp do nich uzyskuje tak samo jak w modelach PaaS i SaaS, ale inaczej niż w ich przypadku, wykorzystywane oprogramowanie należy do dostawcy i on też odpowiada za jego aktualizację oraz bezawaryjne działanie.

Rodzaje trybów eksploatacji zasobów w chmurze:

- Chmura publiczna – współdzielone z innymi użytkownikami zasoby są dynamicznie dostarczane przez zewnętrznego dostawcę za pośrednictwem Internetu. Zasoby te mogą należeć do wielu dostawców. Klienci korzystają z nich w trybie samoobsługi.

- Chmura prywatna – jest to infrastruktura dostarczana na wyłączny użytek jednej organizacji, zawierającej różnych biznesowych użytkowników (na podstawie definicji NIST).
- Chmura dedykowana – rodzaj chmury prywatnej, będącej w dyspozycji ograniczonej grupy podmiotów prywatnych.
- Chmura hybrydowa – chmura łącząca zasoby chmury prywatnej i publicznej, gdzie publiczne zasoby są wykorzystywane np. w celach backupowych lub w chwilach zwiększonego zapotrzebowania na moc przetwarzania.

Usługa przetwarzania w chmurze stwarza wrażenie możliwości korzystania z nieskończonych zasobów dostępnych na żądanie. Pozwala pozbyć się dylematu, czy uda się obsłużyć wszystkich użytkowników; co będzie, gdy ich liczba wzrośnie; ile zgromadzić urządzeń poszczególnych rodzajów lub jak skalować aplikację. Usługa przetwarzania w chmurze odpowiada za obsługę dowolnie zmieniającego się obciążenia, a opłaty ponoszone są dokładnie za stopień wykorzystania zasobów. To właśnie sedno przełomu wnoszonego do gospodarki przez przetwarzanie w chmurze. Dzięki niemu moc obliczeniowa staje się ogólnodostępnym zasobem, potencjalnie – usługą komunalną, jak np. dostarczanie prądu czy wody do mieszkań.

2. Koncepcja przetwarzania w chmurze

Po raz pierwszy pojęcie Cloud computing (przetwarzanie w chmurze) użyto w 1996 r. w artykule S.E. Gilleta i M. Kapora *The Self-governing Internet: Coordination by Design* (MIT Press). I co ciekawe, dzisiejsze rozumienie tego pojęcia jest dokładnie zgodne z zamierzeniem prekursorów.

Współczesna koncepcja przetwarzania w chmurze jako najnowocześniejsza forma usługi outsourcingu informatycznego kształtuje się mniej więcej od 2005 r. Pozyskiwanie zasobów teleinformatycznych w modelu przetwarzania w chmurze umożliwiły trwające od lat 60. XX wieku:

- zmiany dotyczące modeli przetwarzania od samodzielnych jednostek do przetwarzania w sieciach,
- wzrost mocy obliczeniowych pojedynczych serwerów oraz całych centrów danych,
- zwiększenie przepustowości sieci,
- przeniesienie idei wirtualizacji z maszyn *mainframe* na całość zasobów IT.

Z perspektywy usług, elastyczne ukształtowanie środowiska IT umożliwiło – obok rozwoju idei przetwarzania w chmurze – także wprowadzenie modelu SOA (Service Oriented Architecture), co technicznie polegało na przeniesieniu konwencji komunikacji typu „przeglądarka" z relacji człowiek – maszyna na relację maszyna – maszyna.

Te zmiany techniczne mają swoje konsekwencje organizacyjne, biznesowe i prawne.

Outsourcing

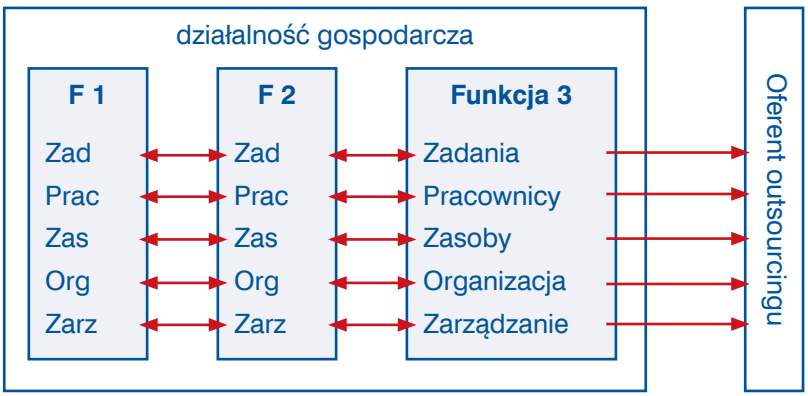
Outsourcing, który w zakresie teleinformatyki występuje równolegle do przetwarzania w chmurze, a docelowo zapewne w dużej mierze ustąpi mu miejsca,

funkcjonalnie realizuje taką samą usługę. Dalej pokazujemy istotę usługi outsourcingu, aby przybliżyć mechanizm usługi przetwarzania w chmurze.

Outsourcing jest jedną z form organizowania działalności gospodarczej. Jego wprowadzanie jest zwykle związane z reorganizacją dotychczasowego sposobu prowadzenia działalności. Wybrane funkcje lub procesy (dla wygody w dalszym opisie pozostaniemy przy określeniu funkcja[3]) są wydzielane z dotychczasowej organizacji i przekazywane do realizacji innemu podmiotowi. Długoterminowym celem jest zwiększenie efektywności działania organizacji. Powierzona funkcja ma być realizowana korzystniej, niż miało to miejsce dotąd. Niemniej jednak w okresie przejściowym, jaki towarzyszy przekazywaniu wybranej funkcji, przychodzi zmierzyć się z poważną zmianą[4]. Trzeba ją postrzegać w ujęciu operacyjnym (organizacyjnym) oraz formalnym (prawnym). Należy podkreślić, że outsourcing polega na oddawaniu w usługę samych czynności operacyjnych, natomiast nie przenosi odpowiedzialności prawnej ze zlecającego na usługodawcę.

Outsourcing może dotyczyć: pojedynczych funkcji, procesów biznesowych lub obszarów działalności. Pozostaniemy przy wariancie outsourcingu funkcji, bowiem pozostałe podlegają takim samym zasadom. W celu realizacji funkcji, organizacja powinna spełniać następujące warunki (patrz też rys. 1):

- znać szczegółowo istotę działań (zadań) składających się na funkcję,
- dysponować kadrą pracowników o właściwych kwalifikacjach,
- zgromadzić niezbędne zasoby materialne, finansowe i informacyjne,
- określić prawidłową organizację wykonywania zadań,
- określić zasady kierowania realizacją zadań.



Rysunek 1. Mechanizm wydzielania funkcji powierzanych w outsourcing

Źródło: opracowanie własne na podstawie [Trocki, 2001].

Oznacza to, że – podejmując decyzję o oddaniu wybranej funkcji w outsourcing – organizacja uznaje, że – mimo starannego zorganizowania wykonywania funkcji – zewnętrzny usługodawca będzie efektywniejszy lub tańszy. Podstawowym celem

[3] Funkcja jest innym pojęciem pojęcia niż proces biznesowy, ale w niniejszym opracowaniu, które referuje ogólną ideę outsourcingu, ta różnica nie jest istotna.

[4] Koncentrujemy się na zagadnieniu powierzania funkcji biznesowo i organizacyjnie ważnych, a więc nie takich, które są popularnie oddawane w outsourcing, jak sprzątanie czy ochrona.

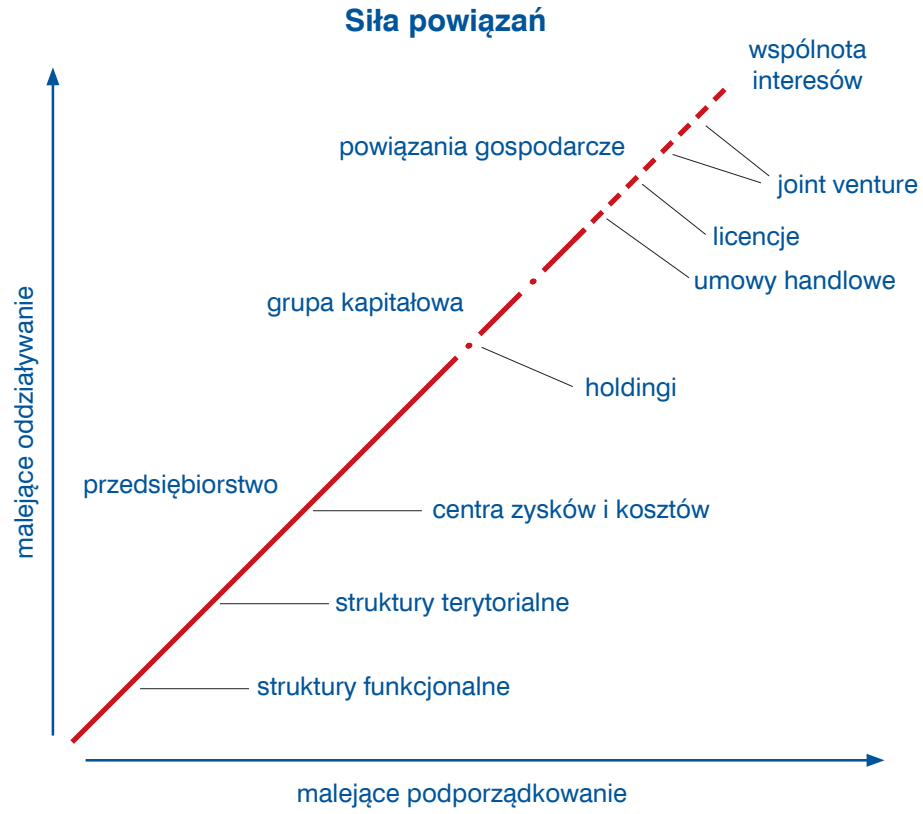
oddania funkcji w outsourcing było bowiem zawsze podnoszenie rentowności, co uzyskuje się przez:

- skupienie się na wybranej działalności podstawowej,
- wykorzystanie cudzych kompetencji, wyższych niż własne.

Wobec tego, przechodząc do formuły powierzenia funkcji w outsourcing, należy zreorganizować następujące powiązania:

- zadaniowe,
- personalne,
- majątkowe,
- organizacyjne,
- zarządcze.

Powiązania te są silniejsze dla struktur funkcjonalnych i scentralizowanych, a słabsze dla struktur opartych na centrach zysków/kosztów oraz terytorialnych (por. rys. 2).



Rysunek 2. Siła powiązań funkcjonalnych.

Źródło: [Trocki, 2001].

Z tego zaś wynika, że najtrudniej jest oddawać w outsourcing funkcje, które są silnie powiązane z innymi funkcjami, np. usługi IT, a najłatwiej te, które są najsłabiej powiązane, np. sprzątanie (por. rys. 3).

Rysunek 3. Podatność funkcji na powierzenie w outsourcing

Źródło: [Trocki, 2001].

Idea outsourcingu nie jest nowa. Słynne jest powiedzenie Henry Forda, że „Jeśli jest coś, czego nie potrafimy zrobić wydajniej, taniej i lepiej niż konkurenci, nie ma sensu, żebyśmy to robili i powinniśmy zatrudnić do wykonania tej pracy kogoś, kto zrobi to lepiej niż my". Ale tak naprawdę, outsourcing jest jeszcze starszy, bo wynika przecież ze specjalizacji i podziału czynników produkcji charakterystycznego dla wszelkiej działalności przemysłowej, a jeszcze wcześniejszej – rzemieślniczej.

Skrótowa historia ewolucji outsourcingu jest następująca:

- podział pracy (do początku XX w.),
- metoda obniżania kosztów (do lat 60. XX w.),
- zmniejszanie ryzyka zmian technologicznych,
- koncentracja na działalności kluczowej,
- strategiczny wybór sposobu funkcjonowania.

Współcześnie można już mówić o następujących, wykształconych celach outsourcingu:

- strategiczne:
  - koncentracja na podstawowym biznesie,
  - zwiększanie swobody i elastyczności działalności,

- zwiększanie efektywności,
- dostęp do *know-how*;

➤ rynkowe:

- poprawa konkurencyjności,
- zwiększenie skali działalności,
- dywersyfikacja lub koncentracja działalności;

➤ ekonomiczne:

- zwiększenie przychodów,
- redukcja kosztów,
- poprawa rentowności,
- ograniczanie ryzyka ekonomicznego;

➤ organizacyjne:

- „odchudzenie" struktury,
- uproszczenie procedur organizacyjnych,
- usprawnienie działania;

➤ motywacyjne:

- obiektywizacja wyników ekonomicznych,
- upowszechnienie myślenia ekonomicznego,
- rozwój przedsiębiorczości,
- wzrost motywacji.

Przygotowanie rozwiązania outsourcingowego może być skomplikowanym i długotrwałym procesem, który jest projektem samym w sobie. Jego ramowa struktura jest następująca:

➤ pomysł (inicjatywa),

➤ analiza celowości (analiza „*make-or-buy*"),

➤ analiza możliwości,

➤ decyzja,

➤ wybór partnera,

➤ opis SLA,

➤ negocjowanie umowy,

➤ reorganizacja wewnętrzna,

➤ wdrożenie.

W ujęciu prawnym outsourcing dzieli się na kontraktowy i kapitałowy. Outsourcing kontraktowy jest typową relacją między niezależnymi podmiotami, z których jeden przekazuje fragment działalności w outsourcing drugiemu. Outsourcing kapitałowy polega na specjalizacji działalności w ramach grupy kapitałowej, np. na zasadzie tworzenia centrów zarządzania kosztami.

Relacje prawne między stronami usługi outsourcingu są zbliżone do tych, które dotyczą usługi przetwarzania w chmurze. Te zaś zostały omówione w rozdziale 6 oraz w załączonej analizie prawnej Kancelarii Bird&Bird. Szczególnie istotne w relacji outsourcingowej jest to, że przekazujący oddaje w usługę tylko działanie właściwe dla danej funkcji, natomiast nie może przekazać odpowiedzialności biznesowej wobec swych kontrahentów. Z kolei przyjmujący nie może poprzestać tylko na własnym doświadczeniu w danej dziedzinie działania. Musi stosować obowiązujące prawo i przyjęte już przez przekazującego standardy dobrych praktyk oraz poddawać się kontrolom i audytom w takim samym zakresie jak przekazujący.

Gwarantowaną jakość świadczonych usług zapewniają załączniki do umów outsourcingowych, tzw. klauzule/opisy/wymagania poziomu usługi, zwane SLA (*service level agreement*). Mają one za zadanie, na tyle precyzyjne zdefiniowanie potrzeb i wymagań klienta, możliwości i ograniczeń usługodawcy oraz okoliczności zewnętrznych, aby w konkretnej sytuacji (potencjalnie spornej) możliwa była jednoznaczna [Tak – Nie] ocena wywiązania się z umowy przez usługodawcę.

W odniesieniu do hasła SLA możemy napotkać:

- „teorię w nauce o zarządzaniu”,
- podejście prawne,
- podejście organizacyjne,
- podejście techniczne.

Typowa struktura opisu wymagań SLA jest następująca:

- zdefiniowanie usług,
- zarządzanie skutecznością wykonania (wspólne oceny okresowe),
- rozwiązywanie problemów (w tym dokumentowanie),
- obowiązki usługobiorcy,
- szkody, odpowiedzialność, siła wyższa,
- bezpieczeństwo, poufność, audyt,
- ciągłość działania,
- rozliczenia,
- rozwiązywanie umowy.

Z kolei przykładowe wskaźniki oceny usługi, które służą rozstrzyganiu kwestii, czy usługa jest prawidłowo (dostatecznie dobrze) świadczona, są następujące:

- gwarantowany czas reakcji (np. 4 h od zgłoszenia),
- gwarantowany czas naprawy (np. 12 h od zgłoszenia),
- gwarantowany czas świadczenia usługi (np. 99,95% w skali roku),
- średni czas obsługi zgłoszenia,
- procent zgłoszeń obsłużonych w zadanym czasie (np. 80% w 20 s),
- procent zgłoszeń obsłużonych jednym kontaktem.

Aspekty prawne – regulacje i standardy w Polsce i UE

Cloud computing jest zjawiskiem nowym. Nie wydano jeszcze przepisów wprost dotyczących przetwarzania w chmurze ani w Polsce, ani w innych państwach (według wiedzy autorów raportu). Nad strategią Unii Europejskiej względem Cloud computingu pracuje Komisja Europejska. Wprowadzanie przepisów krajowych nie nastąpi wcześniej niż po uzgodnieniu tej strategii i jej wydaniu przez Komisję. Dotychczas Komisja Europejska wydała tylko raport, publicznie konsultowany, dotyczący chmury[5]. Spodziewane są kolejne dokumenty.

Mimo że nie ma przepisów wprost odwołujących się do przetwarzania w chmurze, można wdrażać tego typu rozwiązanie na bazie istniejących przepisów, gdyż w zasadzie przetwarzanie w chmurze jest prawnie uregulowane. W Polsce, jak i za granicą, istnieją bowiem regulacje określające warunki przetwarzania określonych kategorii informacji oraz określające wymagania w przypadku powierzenia tych informacji podmiotom trzecim (podwykonawcom). Kategorie informacji, których przetwarzanie podlega reglamentacji, to na ogół dane osobowe oraz inne dane prawnie chronione (w szczególności tajemnica bankowa, szereg kategorii danych objętych tajemnicą zawodową, tajemnica państwowa). Regulacje dotyczące powierzenia czynności innym podmiotom opierają się co do zasady na nauce i standardach zapewnienia bezpieczeństwa informacji oraz ciągłości działania.

Możliwie wyczerpujący przegląd regulacji, stosowanych do usługi przetwarzania w chmurze skierowanej do podmiotów polskiego sektora finansowego, został zawarty w załączniku do niniejszego raportu pt. *Cloud computing w sektorze finansowym. Regulacje i standardy*. Pierwsza wersja tego prawnego raportu o przetwarzaniu w chmurze została opublikowana w listopadzie 2011 r. Dalej przedstawiamy więc tylko ogólny zarys tematyki prawnej, w kwestiach szczegółowych odsyłając do załącznika i wspomnianego raportu prawnego.

Regulacje mające zastosowanie do przetwarzania chmurowego dotyczą co do zasady dwóch zagadnień:

- przetwarzania danych,
- wykorzystania do tego podmiotów zewnętrznych.

Są to przede wszystkim przepisy ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych oraz przepisy dotyczące outsourcingu w sektorze finansowym:

- ustawa z 29 sierpnia 1997 r. – Prawo bankowe,
- ustawa z 19 sierpnia 2011 r. o usługach płatniczych,
- ustawa z 27 maja 2004 r. o funduszach inwestycyjnych,
- ustawa z 28 sierpnia 1997 r. o organizacji i funkcjonowaniu funduszy emerytalnych,
- ustawa z 29 lipca 2005 r. o obrocie instrumentami finansowymi,
- ustawa z 22 maja 2003 r. o działalności ubezpieczeniowej.

Z punktu widzenia ochrony danych osobowych, co do zasady, przetwarzanie w chmurze stanowi powierzenie przetwarzania danych osobowych innemu pod-

[5] http://ec.europa.eu/information_society/activities/cloudcomputing/docs/ccconsultationfinalreport.pdf

miotowi lub sieci podmiotów. Pociąga to za sobą wymóg zapewnienia sobie przez klienta kontroli nad sposobem przetwarzania danych przez dostawcę Cloud computingu, prawa audytu usługi i usługodawcy, wiedzy o położeniu danych, braku możliwości wykorzystywania przez dostawcę danych mu powierzonych w innym celu niż dla należytego wykonania usługi przetwarzania[6].

Regulacje usługi outsourcingu w sektorze finansowym wychodzą z tych samych założeń co przepisy o ochronie danych osobowych, koncentrując się jednak na nieco innych aspektach bezpieczeństwa informacji. Regulacje sektora finansowego, zasadniczo dzielą czynności faktyczne (a więc i operacje przetwarzania danych) na istotne dla ciągłego i niezakłóconego działania instytucji i na pozostałe. Regulowane są tylko czynności faktyczne (zwane też operacyjnymi) istotne dla działania instytucji (żargonowo zwane też krytycznymi). W przypadku czynności i procesów krytycznych, regulacje opierają się na następujących założeniach:

- jednoznaczna odpowiedzialność,
- adekwatne bezpieczeństwo informacji,
- stosowna do krytyczności zdolność zapewnienia ciągłości działania,
- systematyczne monitorowanie ryzyka.

Wszystkie wspomniane akty prawne koncentrują się na zapewnieniu bezpieczeństwa informacji, kontroli nad informacją i ryzykiem związanym z jej przetwarzaniem lub powierzeniem jej przetwarzania innemu podmiotowi.

W sektorze finansowym pojawia się również podstawowa obecnie w Polsce, zdaniem autorów, bariera rozwoju chmury – wynikająca z Prawa bankowego i kilku innych regulacji tego sektora. Jest to zwłaszcza zakaz wprowadzania ograniczeń odpowiedzialności dostawcy usługi za szkody wyrządzone klientom instytucji. Restrykcja ta jest twórczym rozwinięciem zaleceń regulacji europejskich (takich jak m.in. Markets in Financial Instruments Directive czy Payment Services Directive), zakazujących powoływania się na outsourcing w celu ograniczenia przez instytucję finansową własnej odpowiedzialności względem klientów. Rozwinięcie wprowadzone przez polskiego ustawodawcę wykracza nie tylko poza wymogi aktów unijnych, ale i poza ich cel. Polska regulacja jest także egzotyczna na tle regulacji innych krajów Unii Europejskiej.

Zainteresowanych szczegółową wiedzą o regulacjach dotyczących przetwarzania w chmurze w polskim sektorze finansowym odsyłamy do wspomnianego raportu prawnego *Cloud computing w sektorze finansowym. Regulacje i standardy*, którego drugie wydanie zostało dołączone do niniejszego dokumentu. Zainteresowani międzynarodową perspektywą Cloud computingu mogą znaleźć coraz więcej publikacji na ten temat[7].

---

[6] W zakresie przetwarzania danych osobowych w chmurze istnieje pewna nowość w interpretacji, czyli wydane 24 kwietnia 2012 r. *Memorandum z Sopotu* – wspólne stanowisko opracowane przez tzw. Grupę Berlińską (międzynarodowe ciało doradcze grupujące regulatorów oraz ekspertów z zakresu danych osobowych), gdzie wskazano konkretne rodzaje ryzyka związane z przetwarzaniem w chmurze, ale zawarto również zalecenia i szereg proponowanych dobrych praktyk. Dokument jest dostępny na stronie: http://www.giodo.gov.pl/data/filemanager_pl/dif/m_s_pl.pdf

[7] Na przykład [Shaw, 2011].

Aspekty organizacyjne i zarządcze

Zasadniczo przetwarzanie w chmurze polega na:

- swobodnej dostępności puli zasobów,
- wirtualizacji jako efektywnym wykorzystaniu infrastruktury,
- elastycznym i dynamicznym skalowaniu (bez wydatków inwestycyjnych),
- automatycznym kształtowaniu środowiska przetwarzania,
- proporcjonalności kosztów do wykorzystania zasobów.

Swobodna dostępność puli zasobów

Niezależnie od przetwarzania w chmurze, już od lat stopniowo odchodzi się od modelu samodzielnego utrzymywania zasobów IT, korzystając z outsourcingu teleinformatycznego w różnych modelach tej usługi (hosting, kolokacja itd.). Proces ten ma istotne konsekwencje ekonomiczne. Główne konsekwencje to przenoszenie ciężaru kosztów z inwestycyjnych (Capex) na rzecz operacyjnych (Opex). Następnym skutkiem jest potencjalna redukcja kosztów operacyjnych związanych z działaniem infrastruktury. Zmniejszanie kosztów inwestycyjnych obniża barierę podejmowania przedsięwzięć opartych na znaczącym wykorzystywaniu teleinformatyki.

Rysunek 4. Koszty Capex i Opex w modelach usług IT (liczby pokazują proporcje)

Źródło: [Mateos, Rosenberg, 2011].

Różnica w kosztach wynika z tego, że przetwarzanie w chmurze zapewnia o wiele lepszą ich strukturę. Najważniejszym powodem jest zjawisko skali – zasoby (moc obliczeniowa, przestrzeń dyskowa, zużywana energia, przepustowość sieci) oferowane są hurtowo, co ma ten sam skutek jak w przypadku oferty handlowej sieci handlowych w porównaniu z ofertą tradycyjnych sklepów.

Przetwarzanie w chmurze jest też swoistą analogią techniki „just-in-time" w zarządzaniu produkcją, która pozwala minimalizować, a czasem wykluczać tworzenie kosztochłonnych zapasów.

Wirtualizacja jako efektywne wykorzystanie infrastruktury

Wirtualizacja ma kluczowe znaczenie dla przetwarzania w chmurze, bowiem umożliwia najbardziej efektywne wykorzystywanie głównego zasobu infrastruktury

teleinformatycznej, jakim jest serwer fizyczny, który w tym trybie wykorzystywania jest dzielony na wiele serwerów umownych (wirtualnych). Każdy z serwerów wirtualnych, z perspektywy użytkownika, działa jak normalny fizyczny serwer z systemem operacyjnym i pełnym zestawem aplikacji. Serwery wirtualne tworzą pulę zasobów dostępnych na życzenie użytkownika.

Koncepcja ta jest bardzo stara i pochodzi jeszcze z epoki komputerów klasy mainframe, ale w ostatnim dziesięcioleciu została wzmocniona technologią komputerów wielordzeniowych.

Elastyczne i dynamiczne skalowanie

Wirtualizacja daje tę możliwość, że aplikacje użytkownika mogą elastycznie używać to większą, to mniejszą pulę zasobów, zależnie od bieżących i zmieniających się wymagań biznesowych/operacyjnych. Elastyczność wyraża się w dynamicznym skalowaniu, tj. dynamicznym udostępnianiu właściwej ilości zasobów, odpowiednio do bieżącego zapotrzebowania. Przecież niemal każda firma miewa okresy zwiększonego zapotrzebowania na zasoby przetwarzania i jeśli zapewnia je we własnym zakresie, to zmuszona jest utrzymywać zasoby nadmiarowe wobec zapotrzebowania przeciętnego, co generuje zbędne koszty. Korzystanie z przetwarzania w chmurze pozwala unikać takich nieproduktywnych kosztów.

Automatyczne kształtowanie środowiska przetwarzania

Aplikacja obsługująca potrzeby użytkownika, działająca w ramach przetwarzania w chmurze może pozyskiwać lub zwalniać zasoby (instancje) w miarę potrzeb. Dynamiczne przydzielanie zasobów odbywa się automatycznie („w biegu").

Proporcjonalność kosztów do wykorzystania zasobów

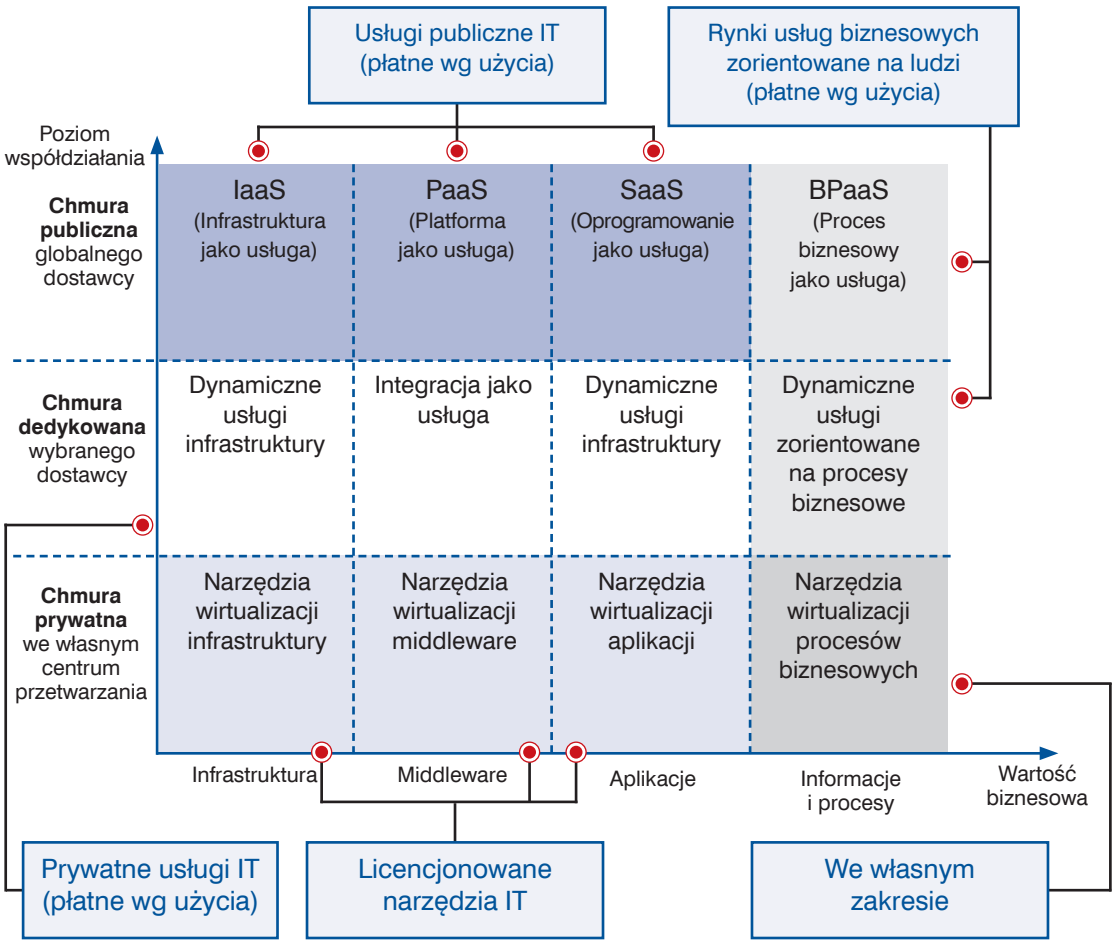
Możliwość dynamicznego skalowania zasobów znajduje odzwierciedlenie w opłatach, które są z zasady proporcjonalne do stopnia wykorzystywania zasobów. Ma więc miejsce przekształcenie kosztów stałych (typowym przykładem jest amortyzacja) w koszty zmienne. Prowadzi to do znamiennych konsekwencji:

- usuwa barierę inwestycyjną w przypadku nowych przedsięwzięć, które można rozpoczynać bez dużych nakładów wstępnych na teleinformatykę,
- udostępnia narzędzia teleinformatyczne, dotąd bardzo kosztowne, podmiotom o mniejszym potencjale finansowym,
- skraca czas wdrożenia narzędzi teleinformatycznych.

3. Zakres modelu przetwarzania w chmurze

Taksonomia przetwarzania w chmurze

Kompleksowe spojrzenie na stopień powierzenia usług do przetwarzania w chmurze oraz zakres korzyści biznesowych z tego czerpanych prowadzą do klasyfikacji przedstawionej na rysunku 5.

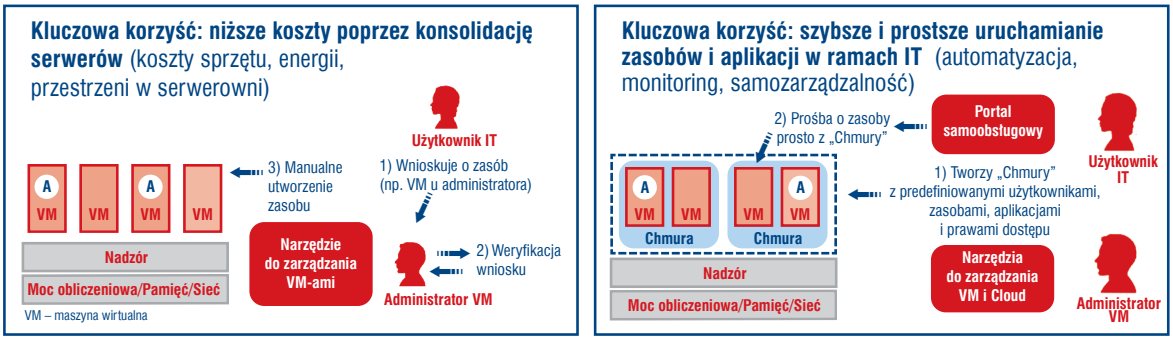


Rysunek 5. Taksonomia przetwarzania w chmurze

Źródło: [Forrester, 2010].

Chmura prywatna

Wirtualizacja serwerów jest pierwszym krokiem w kierunku budowy chmury prywatnej. Pozwala lepiej wykorzystać posiadane zasoby sprzętowe oraz pomaga szybciej dostosowywać złożone systemy informatyczne do zmieniających się wymagań biznesowych firmy. Takie przekształcenie określa się terminem konsolidacja.



Rysunek 6. Kluczowe korzyści przetwarzania w chmurze

Źródło: Microsoft Sp. z o.o.

Tabela 1. Różnice między wirtualizacją a chmurą prywatną

Wirtualizacja	Chmura prywatna
➤ Pozwala użytkownikom optymalizować stosowanie zasobów (wykorzystując jeden serwer, umożliwia uruchomienie w nim dodatkowych, wirtualnych maszyn) ➤ Administrator serwera wirtualnego odpowiada za jego bieżące utrzymanie (np. aktualizację, konfigurację, bezpieczeństwo) ➤ Istnieje możliwość monitorowania zużycia takich zasobów ➤ Wprost nie pozwala na samoobsługowe uruchamianie dodatkowych zasobów ➤ Wirtualizacja to infrastruktura	➤ Automatycznie uruchamia lub zwalnia zasoby (w zależności od potrzeb użytkowników i obciążenia) ➤ Oferuje automatyczne i centralne zarządzanie zasobami w puli (np. rozwiązywanie konfliktów czy zapewnienie ciągłości działania) ➤ Możliwa jest automatyka w zarządzaniu aktualizacjami, poprawkami itp. ➤ Umożliwia samoobsługowe podejście do natychmiastowego uruchamiania i wyłączania zasobów ➤ Chmura prywatna to sposób dostarczania zasobów i usług

Projekt konsolidacji serwerów, oparty na ich wirtualizacji, składa się z następujących etapów:

- wytypowanie serwerów fizycznych do wirtualizacji,
- wybór platformy wirtualizacyjnej oraz wyskalowanie docelowych hostów,
- konwersja P2V (*private to virtual*) wybranych serwerów,
- stabilizacja systemów.

Etap 1. Wybór systemów do konsolidacji

Wybór systemów do konsolidacji oraz wyskalowanie hostów należy poprzedzić zebraniem danych o charakterystyce obciążeń wszystkich serwerów. W ramach procesu zbierania informacji mierzone jest obciążenie procesorów, pamięci, kanałów dyskowych oraz sieciowych. Na podstawie zestawienia danych można podjąć decyzję o wyborze konkretnych maszyn, unikając ryzyka przeciążenia docelowych hostów wirtualizacyjnych. Powyższą analizę mogą wesprzeć odpowiednie narzędzia aplikacyjne, które pozwalają np. na zdalny pomiar obciążeń wybranych serwerów oraz wspomagają proces podejmowania decyzji o doborze serwerów do konsolidacji. Przy użyciu narzędzi dostarczających informacji na temat systemów heterogenicznych (np. MS Windows Server, HP-UX, Sun Solaris, Red Hat Enterprise Linux, Novell SUSE Linux Enterprise Server, IBM AIX) możliwe jest monitorowanie pełnego zestawu parametrów obciążeń, zarówno systemów fizycznych, jak i wirtualnych. Ostrzegają one także o potencjalnych awariach oraz pomagają usunąć te, które już wystąpiły.

Etap 2. Wybór platformy wirtualizacyjnej

W kolejnym etapie należy podjąć decyzję o wyborze platformy wirtualizacyjnej. Możliwy jest wybór między dedykowanymi rozwiązaniami komercyjnymi, rozwiązaniami oferowanymi w cenie systemu operacyjnego, a także niszowymi rozwiązaniami bezpłatnymi.

Etap 3. Konwersja środowisk fizycznych na wirtualne

Proces konwersji jest również wspierany narzędziowo. Należy wskazać serwery fizyczne i rozpocząć proces ich konwersji. Następnie należy zapisać informacje o konfiguracji sprzętu oraz skopiować zawartość dysków z maszyny fizycznej do hosta wirtualnego. Po skompletowaniu wszystkich elementów (dyski, konfiguracja) następuje utworzenie w pełni funkcjonalnej maszyny wirtualnej. Procesowi konwersji towarzyszy często efekt optymalizacji, co oznacza zmniejszenie zasobów wirtualnych przy jednoczesnym utrzymaniu odpowiedniej wydajności. Narzędzia wspierające proces konwersji pozostają przydatne także później – do zarządzania środowiskiem zwirtualizowanym. Często możliwe jest także zarządzanie zwirtualizowanymi środowiskami heterogenicznymi, pochodzącymi od różnych dostawców (np. VMware, Microsoft).

Etap 4. Stabilizacja systemów

Po zakończeniu procesu konwersji P2V (*private to virtual*) ważne jest uwzględnienie nowego elementu – platformy wirtualizacyjnej – w systemie monitorującym usługi świadczone przez centrum przetwarzania. W celu pełnego i zintegrowanego monitoringu warstwy fizycznej i wirtualnej warto zaimplementować dedykowane narzędzia, pozwalające na utworzenie jednolitego modelu usług, obejmującego wszystkie elementy rozwiązania w systemach heterogenicznych (sprzęt, platforma wirtualizacyjna, systemy wirtualne, aplikacje serwerowe). Dostarczą one bieżących informacji o obciążeniu poszczególnych elementów oraz będą ostrzegać o potencjalnych awariach. Powiązane z narzędziami bazy wiedzy, ułatwią rozwiązywanie pojawiających się problemów.

Chmura prywatna

Cechą, która wyróżnia chmurę prywatną od wirtualizacji, jest pełna automatyzacja we wszystkich warstwach: systemu, sprzętu, wirtualizatora, systemów operacyjnych i logiki biznesowej aplikacji. W tej ostatniej najczęściej pojawiają się problemy ze skalowalnością czy awariami i najtrudniej je rozwiązać. Wtedy ujawniaja się przewaga chmury prywatnej. Na podstawie pełnej wiedzy o strukturze i bieżących parametrach pracy systemu, daje ona możliwość szybkiego rozwiązania problemu.

Zaawansowane mechanizmy automatyki, obejmujące wszystkie warstwy przetwarzania, różnią chmury od systemów hostingowych. Jeśli np. system monitoringu uzna, że serwer obsługujący strony internetowe osiągnął już limit wydajności, może uruchomić kolejną instancję takiego serwera i zintegrować go z już działającym systemem, usuwając automatycznie wąskie gardło aplikacji.

Od wirtualizacji do chmury prywatnej

Pierwszym etapem przygotowania chmury prywatnej jest opracowanie spójnego systemu zarządzania tożsamością. System ten będzie autoryzował wszystkie kolejne działania usługi realizowane w ramach chmury.

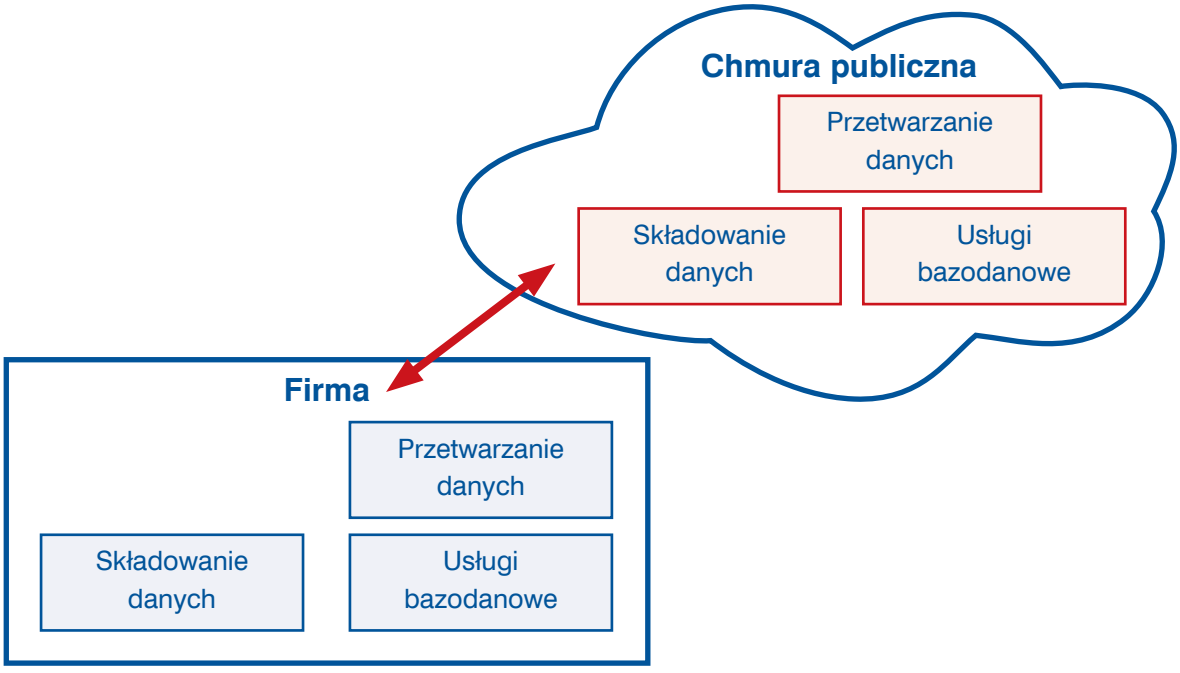
Zbudowane środowisko wirtualne stanowi fundament do działania chmury prywatnej pozwalającej świadczyć zaawansowane usługi (IaaS, PaaS, SaaS). Dzięki narzędziom do zarządzania maszynami wirtualnymi można łatwo je przenosić, korzystać z podpowiedzi, co zrobić z niedociążonym lub przeciążonym serwerem,

stosować wbudowane biblioteki z obrazami systemów, plikami ISO czy skryptami. Można wówczas na podstawie zdefiniowanych reguł dodawać lub zabierać zasoby. Wzbogacenie warstwy zarządzania o dodatkowy portal samoobsługowy pozwala pracownikom firmy na samodzielną obsługę w zakresie rezerwacji zasobów niezbędnych do realizacji celów biznesowych. Użytkownik może sam określać, ile maszyn, instancji baz danych, procesorów czy pamięci operacyjnej potrzebuje.

Kluczem do poprawnego działania chmury prywatnej jest możliwość stałego i dogłębnego monitorowania i raportowania wszystkich jej warstw i procesów, jakie w niej zachodzą. Ponieważ docelowo chmura prywatna utrzymuje wiele złożonych usług, warto wyposażyć ją w mechanizmy zaawansowanej automatyki, która pozwoli zintegrować wszystkie heterogeniczne komponenty chmury i realizować sekwencje czynności administracyjnych, rozwiązując automatycznie pojawiające się problemy.

Przetwarzanie w chmurze publicznej

Chmurę publiczną najprościej definiuje się, jako usługę dostępną przez łącza internetowe, świadczoną przez firmę niezależną od podmiotu korzystającego z usługi. Określenie „publiczna" nie oznacza, że jest to usługa darmowa, ani również, że dane klienta są dostępne publicznie.



Rysunek 7. Model przetwarzania w chmurze publicznej

Źródło: opracowanie własne.

Usługa w chmurze publicznej musi realizować następujące zadania:

- identyfikacja – usługa musi jednoznacznie uwierzytelniać użytkownika;

- uwierzytelnianie sfederowane – usługa powinna umożliwiać integrację z istniejącymi w firmie mechanizmami uwierzytelniania użytkowników, pozwalając na użycie mechanizmu jednokrotnego logowania;
- bezpieczeństwo (w tym prywatność danych) – dostęp do usługi musi następować w sposób bezpieczny, z użyciem mechanizmów uniemożliwiających przechwycenie bądź podejrzenie danych klienta;
- lokalizacja danych – z uwagi na wymagania regulatora, dane powinny znajdować się na terenie Europejskiego Obszaru Gospodarczego[8] i klient powinien mieć możliwość monitorowania ich przepływu; jeśli dane miałyby być przetwarzane poza obszarem UE, potrzebne byłyby dodatkowe uzgodnienia kontraktowe z dostawcą chmury oraz zezwolenia administracyjne (nadzorcy danych);
- monitorowanie usługi – dostawca powinien dostarczyć narzędzia służące monitorowaniu dostępności usług, które pozwalają na rozliczanie się z klientem z dotrzymania założonego SLA.

Potencjalne obszary, w których wykorzystanie chmury publicznej ma sens ekonomiczny i technologiczny dla przedsiębiorstwa to np.:

- kopie zapasowe i składowanie danych archiwalnych,
- dodatkowa moc przetwarzania do obsłużenia zwiększonego i tymczasowego zapotrzebowania, związanego z obciążeniem systemów komputerowych,
- aplikacje przystosowane do modelu SaaS (poczta, systemy CRM, komunikacja itp.),
- współdzielenie danych w bazach bądź plikach z firmami kooperującymi.

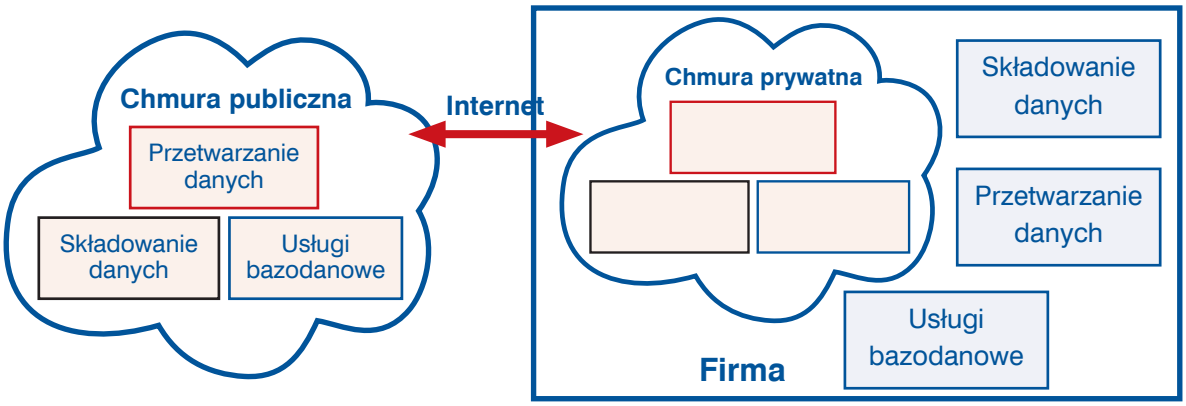
Decydując się na pełne „wejście w chmurę", organizacja nie ponosi kosztów zakupu i utrzymania rozbudowanej infrastruktury informatycznej. Należy jednak wziąć pod uwagę jakość i parametry świadczonej usługi, która będzie, w pewnym stopniu, determinowała działalność operacyjną przedsiębiorstwa.

Przetwarzanie w chmurze – model hybrydowy

Jednym z typowych przypadków połączenia chmury publicznej z chmurą prywatną (chmura hybrydowa) jest sytuacja, w której organizacja na potrzeby kluczowych aplikacji biznesowych, zbudowała chmurę prywatną, natomiast część niekrytycznych aplikacji jest dostarczana z zewnątrz w postaci usługi z chmury publicznej. Może to również dotyczyć sytuacji, w których organizacja, ze względów związanych z obowiązującym prawem, wewnętrznymi regulacjami bądź z innych względów, nie może w pełni skorzystać z modelu chmury publicznej. Niemniej jednak ma możliwość wydzielenia części swojej infrastruktury i aplikacji oraz zbudowania usług IT, wykorzystując model hybrydowy.

Niezależnie od wybranego modelu funkcjonowania, z punktu widzenia użytkownika końcowego, sposób dostarczenia aplikacji jest przezroczysty.

[8] Lub na innych obszarach, na których ochrona danych została uznana przez Komisję Europejską za adekwatną. Więcej w raporcie *Cloud computing w sektorze finansowym. Regulacje i standardy*.



Rysunek 8. Model hybrydowy przetwarzania w chmurze

Źródło: opracowanie własne.

Wymagania stawiane dostawcy usług w chmurze hybrydowej są takie same jak w przypadku chmury publicznej. Model chmury hybrydowej jest praktycznym sposobem przechodzenia do pełnego przetwarzania w chmurze, gdyż ze względu na istniejącą infrastrukturę, poniesione inwestycje, jak również wypracowane praktyki zarządzania procesami IT, konieczne jest zastosowanie takiego modelu, który aktywnie włączy wszystkie elementy systemu i wytworzy spójną całość. Nie do przecenienia są również dotychczasowe przyzwyczajenia związane z korzystaniem z infrastruktury i aplikacji. W związku z tym model hybrydowy pozwala na łatwiejszą adaptację przetwarzania w chmurze oraz pełniejsze wykorzystanie jego zalet i korzyści.

Scenariusze wykorzystania modelu hybrydowego są analogiczne jak w przypadku chmury publicznej. Krytycznym elementem spinającym obydwa środowiska może stać się infrastruktura rozproszonego uwierzytelniania użytkowników (np. Active Directory) bądź „szyna danych".

Wyzwania bezpieczeństwa

Dokonując wyboru zewnętrznego dostawcy usług, brane są pod uwagę takie parametry, jak: bezpieczeństwo, ochrona danych, ochrona prywatności oraz prawa własności. Istotne jest zwrócenie uwagi na całościowe zabezpieczenie usług na wielu poziomach, w tym:

- warstwy fizycznej w centrach danych: fizyczne środki kontroli dostępu, nadzór kamer, kontrola dostępu;
- warstwy logicznej: izolacja danych, bezpieczeństwo obsługiwanych aplikacji, usługi infrastrukturalne, poziom sieci, zarządzanie tożsamością i dostępem.

Bezpieczeństwo fizyczne

Prawidłowe fizyczne zabezpieczenie środowiska przechowywania danych klientów powinno być realizowane następująco. Kontrola dostępu jest przeprowadzana za pomocą wielopoziomowej weryfikacji zabezpieczeń. Fizyczne sprawdzanie zabezpieczeń odbywa się w centrach obliczeniowych, a usługi są świadczone

przez ośrodki obliczeniowe klasy korporacyjnej, które zapewniają ciągłość ich realizacji na podstawie umów dotyczących poziomu usług (SLA). W ośrodkach obliczeniowych, zgodnie ze standardami branżowymi, realizowane są wymienione dalej zadania.

- Kontrola zapewniająca dostęp fizyczny wyłącznie dla osób upoważnionych. Dostęp jest ograniczony na podstawie funkcji służbowej tak, aby wyłącznie uprawnieni pracownicy mogli zarządzać aplikacjami i usługami klientów. Autoryzacja dostępu fizycznego jest wdrażana przy pomocy szeregu procesów uwierzytelniania i zabezpieczeń: kart identyfikacyjnych, kart inteligentnych, skanerów biometrycznych, lokalnych służb ochrony, ciągłego nadzoru kamer oraz uwierzytelniania podwójnego w celu uzyskania fizycznego dostępu do centrum obliczeniowego.
- Gwarantowanie rezerwowego źródła zasilania, w tym dwóch oddzielnych źródeł zasilania w każdym centrum danych, akumulatorowego zasilania rezerwowego i zespołów prądnicowych z silnikami wysokoprężnymi (wraz z umowami na dostawę alternatywnych rodzajów paliwa).
- Kontrola warunków klimatycznych w celu zapewnienia optymalnej temperatury i wilgotności powietrza dla funkcjonowania sprzętu.
- Kontrola skutków klęsk żywiołowych, w tym wzmocnione regały na wypadek wstrząsów sejsmicznych, tam gdzie to konieczne, oraz systemy przeciwpożarowe i gaśnicze.
- Monitoring fizyczny, włącznie z czujnikami ruchu, zabezpieczeniem dostępu 24 godziny na dobę, nadzorem z kamer i alarmami naruszenia zabezpieczeń.
- Zapewnienie bezpiecznej struktury i obsługi sieci, które w centrach obliczeniowych są zaprojektowane w taki sposób, aby tworzyć szereg oddzielnych segmentów w ramach każdego ośrodka.

Bezpieczeństwo logiczne

Bezpieczeństwo logiczne usług jest tak samo istotne, jak bezpieczeństwo fizyczne. Jest ono zapewnione dzięki następującym kluczowym funkcjom:

- rozdzieleniu danych,
- bezpieczeństwu aplikacji zdalnych.

Przechowywanie i przetwarzanie danych podlega segregacji logicznej klientów tej samej usługi, dzięki strukturom logicznym danych oraz dzięki funkcjom opracowanym specjalnie w celu wspierania procesów tworzenia, zarządzania i zabezpieczenia środowisk wielodostępnych. Dzięki architekturze bezpieczeństwa obsługi wielu podmiotów, dane klientów przechowywane w obliczeniowych centrach, współużytkowanych przez wielu klientów, są zabezpieczone przed dostępem lub naruszeniem ich bezpieczeństwa przez inne organizacje.

Wysoki poziom ochrony aplikacji zdalnych, znajdujących się w ośrodkach obliczeniowych, zapewniany jest dzięki niezawodnym funkcjom bezpieczeństwa oraz funkcjom kontroli dostępu. Są to m.in.:

- obsługa komunikacji uwierzytelnionej i zaszyfrowanej, co ułatwia identyfikację uczestników procesu komunikacji i ochronę przed manipulacją wiadomościami;

- obsługa technologii szyfrowania w wiadomościach e-mail (np. S/MIME);
- ograniczenie przekazywania wiadomości w celu zredukowania liczby wiadomości niepożądanych i spamu;
- listy adresów blokowanych w czasie rzeczywistym (RBL) oraz listy bezpieczne w celu wyeliminowania wiadomości przychodzących ze znanych źródeł spamu;
- elastyczność zasad dotyczących urządzeń w celu zabezpieczenia komunikacji z urządzeniami mobilnymi (w rodzaju blokad PIN oraz czyszczenia zdalnego lub lokalnego);
- ochrona przed oprogramowaniem złośliwym (*malware*) przez wdrożenie wielowarstwowego oprogramowania antywirusowego w systemach operacyjnych serwerów, systemach wiadomości;
- zabezpieczenie infrastruktury usług w chmurze, co odbywa się dzięki:
  - interfejsom użytkownika z konfiguracją ustawień bezpieczeństwa, które mogą być poddawane filtrowaniu wg uprawnień grupowych, co zapewnia wyświetlanie dostępnych funkcji wyłącznie dla akcji, łączy i treści, do których użytkownicy posiadają uprawnienia dostępu,
  - administracji wielopoziomowej z zastosowaniem modelu administracji trzypoziomowej, w ramach którego rozdzielane są zadania i formaty administracyjne na podstawie autoryzacji dostępu w zależności od roli użytkownika i poziomu autoryzacji dostępu do funkcji administracyjnych,
  - skanowaniu bezpieczeństwa środowiska w celu wykrycia luk w zabezpieczeniach i błędów konfiguracji,
  - systemom wykrywania nieautoryzowanego dostępu, w taki sposób, że zaawansowane silniki korelacji analizują te dane, aby bezzwłocznie powiadamiać personel o próbach nawiązania połączenia, które zostały zaklasyfikowane jako podejrzane;
- zabezpieczenia na poziomie sieci, m.in. funkcje związane z wysokim poziomem zabezpieczeń połączeń internetowych, np.:
  - połączenia umożliwiające klientom dostęp do usług świadczonych przez Internet są nawiązywane z lokalizacji użytkownika, która jest wyposażona w dostęp do sieci, i następnie kierowane do ośrodka obliczeniowego; połączenia nawiązywane między klientami a ośrodkami obliczeniowymi są szyfrowane przy pomocy funkcji zgodnej ze standardem branżowym Transport Layer Security (TLS)/Secure Sockets Layer (SSL); zastosowanie TLS/SSL pozwala na nawiązanie bezpiecznego połączenia między wyszukiwarką a serwerem, aby podwyższyć poziom ochrony poufności danych i integralności połączenia między komputerem użytkownika a centrum danych,
  - sieć nadmiarowa, która zapewnia możliwość pracy awaryjnej oraz dostępność sieci na poziomie blisko 100%,
  - wszystkie połączenia zdalne, nawiązywane przez personel operacyjny są realizowane przy pomocy usług pulpitu zdalnego;
- zarządzanie tożsamością i dostępem; dostęp do systemów, przez które realizowane są usługi, jest kontrolowany dzięki:

- kontroli dostępu na poziomie personelu: udostępnianie systemów teleinformatycznych, na których przechowywane są dane klientów, personelowi ośrodków obliczeniowych podlega ścisłej kontroli,
- kontroli dostępu bazującej na zasadzie rozdzielenia obowiązków i nadawania minimalnych przywilejów;

➤ ograniczenie funkcjonalności serwerów przez wyłączenie usług nieistotnych;

➤ logowanie i nadzór;

➤ ograniczony dostęp do usług;

➤ nadzorowanie treści;

➤ ograniczenie funkcjonalności serwerów;

➤ lepsza ochrona sesji dzięki SSL/TLS.

4. Analiza SWOT przetwarzania w chmurze

Tabela 2. Analiza SWOT

	S					**W**		
	Elastyczność doboru technologii	Koszty	Skalowalność technologiczna	Szybkość wdrożenia nowych usług	Koncentracja na własnych kluczowych kompetencjach	Poziom dojrzałości rozwiązań	Kompatybilność rozwiązań technologicznych	Złożoność migracji
PUBLIC HYBRID PRIVATE	wysoka wysoka średnia	niskie średnie wysokie	wysoka wysoka średnia	wysoka średnia niska	wysoka średnia średnia	średni niski wysoki	średnia średnia średnia	średnia średnia niska
	O					**T**		
	Przewidywalność kosztów	Elastyczność biznesowa	Ryzyko biznesowe	Zwiększenie efektywności IT	Mobilność biznesowa	Zagrożenia związane z bezpieczeństwem	Zagrożenia związane z obowiązującymi regulacjami	Bariera mentalna
PUBLIC HYBRID PRIVATE	wysoka średnia średnia	wysoka wysoka średnia	niskie średnie wysokie	duże średnie średnie	wysoka średnia niska	niskie niskie niskie	średnie średnie najniższe	wysoka średnia niska

Źródło:opracowanie własne.

Mocne strony

➤ szybkość uzyskania dostępu do usługi,

➤ możliwość samoobsługi,

➤ opłata jedynie za wykorzystane zasoby,

➤ możliwość korzystania z wybranych opcji usługi,

➤ możliwość wykorzystania zasobów zewnętrznych,

➤ możliwość ścisłej kontroli zgodności z SLA,

➤ w przypadku chmury publicznej brak konieczności utrzymywania wewnętrznych zasobów infrastrukturalnych i ludzkich,

➤ ograniczenie kosztów operacyjnych i inwestycyjnych,

➤ możliwość koncentracji IT na kluczowych kompetencjach zespołu.

Słabe strony

- dojrzałość rozwiązań w przypadku chmury publicznej i hybrydowej,
- w przypadku korzystania z usług różnych dostawców, zarówno usług w chmurze, jak i elementów technologicznych (sprzęt, różne wirtualizatory, systemy operacyjne), możliwe problemy z kompatybilnością,
- potencjalnie większa złożoność migracji do chmury publicznej i hybrydowej,
- uzależnienie od wybranego zewnętrznego dostawcy w przypadku chmury publicznej i hybrydowej.

Szanse

- możliwość zachowania dużej kontroli nad ponoszonymi kosztami, szczególnie w przypadku chmury publicznej,
- duża skalowalność biznesowa, możliwość rozszerzenia o dodatkowe zasoby w przypadku zewnętrznego zapotrzebowania,
- możliwość bardzo szybkiego tworzenia nowych usług, dostawy nowych aplikacji i infrastruktury, co przekłada się na zdecydowanie większą elastyczność biznesową,
- zmniejszenie ryzyka biznesowego w zakresie przyspieszenia dostawy nowych aplikacji i usług oraz mobilności biznesowej,
- znaczne zwiększenie efektywności działań IT,
- możliwość reorganizacji prowadzenia działalności biznesowej pod kątem wykorzystania przetwarzania w chmurze.

Zagrożenia

- potencjalnie większe poczucie zagrożenia w przypadku chmury publicznej i hybrydowej,
- potencjalna niejednoznaczność w interpretacji obowiązujących regulacji,
- bariera mentalna związana z przeniesieniem aplikacji i danych do chmury (np. obawa przed mniejszą kontrolą nad sposobem przetwarzania danych, obawa przed uzależnieniem od jednego dostawcy).

5. Korzyści z wykorzystania modelu przetwarzania w chmurze w sektorze finansowym

Przetwarzanie danych w chmurze to nowe możliwości, dzięki którym organizacja bardziej elastycznie i efektywnie kosztowo wykorzystuje swoje zasoby. Korzyści można podzielić na trzy grupy:

- korzyści techniczne,
- korzyści finansowe,
- korzyści organizacyjne.

Korzyści techniczne

➤ Elastyczne wykorzystanie mocy obliczeniowej.

Profile dobowego zapotrzebowania na moc obliczeniową są różne dla różnych aplikacji. Systemy wsparcia sprzedaży są najbardziej obciążone w ciągu dnia, szczególnie w godzinach popołudniowych. Systemy odpowiedzialne za przetwarzanie transakcji, naliczanie odsetek i inne procesy zakończenia dnia, pracują głównie w godzinach nocnych. Systemy sprawozdawcze i raportowe przetwarzają dane w nocy i wcześnie rano, a w zakresie analiz *ad hoc* w ciągu dnia, raczej w godzinach rannych. W przypadku tradycyjnej architektury obliczeniowej z dedykowanymi dla każdej aplikacji serwerami, moc obliczeniowa dużych i drogich komputerów przez większość czasu nie jest wykorzystywana. W chmurze obliczeniowej współdzielone zasoby są udostępnione tym aplikacjom, które tego w danym momencie najbardziej potrzebują. Dzięki temu:

- wzrasta dostępność zasobów obliczeniowych dla każdej aplikacji,
- ograniczone są inwestycje w sprzęt komputerowy przy jednoczesnym zmniejszeniu czasu wykonywania obliczeń,
- alokowana jest moc obliczeniowa dla tych aplikacji, które w danej chwili najbardziej jej wymagają,
- uzyskiwany jest stały poziom dostępu do usług niezależnie od liczby użytkowników (tzw. skalowalność),
- powstaje możliwość szybkiego pozyskania dodatkowej, zewnętrznej mocy obliczeniowej.

Moc obliczeniowa w modelu przetwarzania w chmurze upodabnia się do energii elektrycznej, czyli do zasobu o określonych parametrach, który można pobrać z zewnątrz za uzgodnioną wcześniej opłatą. Również w przypadku obliczeń zaczyna być możliwe uruchomienie posiadanych maszyn (czyli oprogramowania) za pomocą pozyskanej niejako z „gniazdka" energii (obliczeń w chmurze). W przypadku wykorzystania chmury płacimy tylko za to, z czego korzystamy.

➤ Dostęp do najnowszych wersji oprogramowania (automatyczne upgrade'y) – SaaS.

Łatwy dostęp do najnowszych technologii. Za aktualizację oprogramowania, rozwój infrastruktury (chmury) z wykorzystaniem najnowszych technologii i trendów technologicznych odpowiedzialny jest dostawca usługi.

Korzyści finansowe

➤ Niższe wydatki inwestycyjne i utrzymaniowe – brak konieczności inwestycji w sprzęt i brak kosztów początkowych instalacji i uruchomienia.

Przetwarzanie w chmurze pozwala również zmniejszyć koszty związane z zakupem licencji na oprogramowanie. Rezygnacja z posiadania własnej infrastruktury obliczeniowej (częściowa lub całkowita) pozwala na ograniczenie wydatków inwestycyjnych związanych z budową i wyposażeniem serwerowni komputerowych.

Oczywiście w zamian wzrastają koszty operacyjne, gdyż dostawca usługi musi mieć środki na organizację i utrzymanie chmury obliczeniowej. Ze względu na

ekonomię skali oraz lepsze wykorzystanie zasobów, koszty te powinny być jednak niższe niż całkowite koszty (TCO) ponoszone indywidualnie. Ponadto, w przypadku gdy w wyniku zmiany warunków rynkowych lub decyzji biznesowych nagle zmienia się zapotrzebowanie na moc obliczeniową, możliwe jest równie szybkie pozyskanie dodatkowej lub zwolnienie zbędnej mocy.

- Krótszy *time–to-market*, co oznacza możliwość szybszego wprowadzenia produktu na rynek i uzyskania korzyści finansowych.

W przypadku zastosowania chmury, organizacja nie musi martwić się o serwery, oprogramowanie i jego aktualizację oraz integrację, dzięki czemu można budować aplikacje znacznie szybciej i mniej kosztownie. Zastosowana architektura oraz sama koncepcja działania chmury wspiera nie tylko szybką i prostą implementację i integrację nowych aplikacji, ale również modyfikacje i wdrożenia nowych funkcjonalności w działających już systemach. Dzięki zastosowaniu przetwarzania w chmurze budowa aplikacji (lub wdrażanie nowych rozwiązań) jest pięciokrotnie szybsza i o połowę tańsza od zastosowania tradycyjnego podejścia, np. platformy .NET.

- Minimalizacja aktywów niepracujących, zwiększenie ROE.
- Przewidywalność kosztów i przywiązanie kosztów do przychodów.

Wykorzystanie chmury obliczeniowej powoduje radykalne zmniejszenie kosztów stałych IT i przeniesienie znacznej ich części do kosztów zmiennych. Koszty zmienne zaś znacznie prościej można powiązać z odpowiadającymi im przychodami, w efekcie łatwiejsza jest ocena rentowności produktów.

Ponoszenie kosztów związanych z rzeczywistym wykorzystaniem usług znacząco obniża ryzyko finansowe prowadzenia działalności. W przypadku standardowego podejścia, organizacja zmuszona jest ponosić koszty związane z inwestowaniem w infrastrukturę IT (serwery, aplikacje, utrzymanie). Sprzęt taki nigdy nie jest przez cały czas wykorzystany w 100%, dodatkowo z zakupionego sprzętu ciężko jest zrezygnować. W przypadku chmury w dowolnym momencie możemy zmniejszyć koszty związane z przetwarzaniem w chmurze, rezygnując z tego, co w danej chwili jest zbędne.

Korzyści organizacyjne

- Ograniczenie zaplecza w postaci zasobów (firmy zewnętrzne, IT).

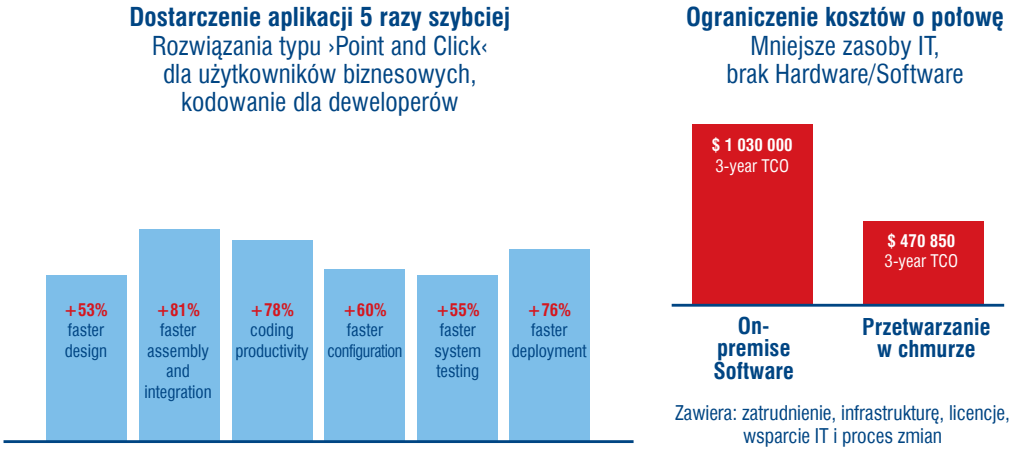
Szybsza implementacja i podniesienie sprawności działania, dzięki skróceniu czasu wdrożenia nowych aplikacji biznesowych i rozwiązań informatycznych, sprawia, że organizacja jest bardziej elastyczna i otwarta na wprowadzanie nowych rozwiązań.

- Przeniesienie punktu ciężkości ryzyka związanego z infrastrukturą informatyczną na dostawcę usługi.

To dostawca odpowiada za bezawaryjność działania usługi oraz bezpieczeństwo danych. Do dostawcy należy m.in.:

- sporządzanie zapasowych kopii danych,
- zapewnienie serwerów zapasowych i przeniesienie na nie działania aplikacji w przypadku awarii serwerów podstawowych,

- zapewnienie alternatywnych źródeł zasilania,
- zabezpieczenie fizyczne infrastruktury IT przed dostępem osób nieuprawnionych.



Rysunek 9. Korzyści z implementacji chmury obliczeniowej

Źródło: IDC White Paper, „Force com Cloud Platform Drivers Huge Time to Market and Cost Savings", Doc #219965, September, 2009.

➤ Podniesienie jakości usług i poziomu SLA.

Zwykle aplikacje w usłudze przetwarzania w chmurze działają bardziej niezawodnie. Dzieje się tak dlatego, że u dostawców tych usług pracuje personel bardziej wyspecjalizowany, zmiany otrzymywane od producentów są wnikliwiej sprawdzane, poprawki do aplikacji są sprawniej instalowane. Dostawca utrzymuje mniejszą różnorodność środowisk, co skutkuje mniejszą liczbą występujących błędów. Oferowane poziomy dostępności usługi na ogół przekraczają poziom 99,9%. Procesy/usługi są ustandaryzowane i uproszczone.

➤ Łatwiejszy dostęp do aplikacji dla pracowników mobilnych, zgodnie z zasadami bezpieczeństwa w banku.

Dla aplikacji, należących do usług działających w chmurze, w przypadku odpowiedniej konfiguracji, możliwe jest zalogowanie się z dowolnego miejsca na Ziemi. Dostępne jest dodatkowe wsparcie i aplikacje umożliwiające korzystanie z urządzeń mobilnych (dedykowane aplikacje na smartfony i tablety). Pracownicy mają dostęp i korzystają z ustandaryzowanych funkcjonalności systemu (standaryzacja konfiguracji, usług).

➤ Zmiana modelu zarządzania ryzykiem.

Dzięki zastosowaniu przetwarzania w chmurze ciężar ryzyka zostaje rozłożony również na dostawcę usługi. Zgodnie z opisanymi już wcześniej zasadami funkcjonowania chmury to dostawca odpowiada za zapewnienie ciągłości i bezbłędności działania aplikacji będących w chmurze.

Paradoksalnie, zważywszy na obawy dotyczące bezpieczeństwa i ciągłości działania, dodatkowymi korzyściami, należącymi do trzech wymienionych grup, są te dotyczące bezpieczeństwa przetwarzanych danych.

Tabela 3. Porównanie różnic tradycyjnego podejścia do infrastruktury IT z przetwarzaniem w chmurze

Obszar	Tradycyjne podejście do infrastruktury IT	Przetwarzanie w chmurze
Wykorzystanie zasobów	Niski poziom wykorzystania dostępnych zasobów (10–20%)	Wysoki poziom wykorzystania dostępnych zasobów (75–90%)
Dostawa sprzętu, aplikacji, usług	Tygodnie	Minuty
Wdrożenie zmian	Miesiące	Dni/Godziny
Rezerwacja zasobów i usług	Tygodnie	Minuty
Zwolnienie zasobów i usług	Tygodnie	Minuty
Konfiguracja nowych serwerów, usług	Dni/Tygodnie	Minuty/Godziny
Model opłat	Jednorazowe opłaty (sprzęt, usługa) + opłaty okresowe (licencje, wsparcie)	Opłata za rzeczywiste wykorzystanie zasobów

6. Bariery i ograniczenia

Ograniczenia i bariery dla rozwoju przetwarzania w chmurze lub korzystania z tego modelu usług informatycznych, szczególnie w sektorze finansowym, mają mieszaną naturę. Połączenie obaw, ograniczeń mentalnych czy niechęci do zmiany po stronie potencjalnych usługobiorców, jak i obaw co do zarządzalności usług, problemów z zarządzaniem wielonarodowym, zgodności z wymogami (*compliance*) po stronie dostawców usług, spowalnia wykorzystanie przetwarzania w chmurze, w tym w szczególności właśnie przez silnie regulowany sektor finansowy. Dotyczy to głównie rynku polskiego, który w dalszym ciągu ma najbardziej rygorystyczne w Europie przepisy dotyczące outsourcingu w sektorze bankowym oraz najbardziej sformalizowane przepisy dotyczące ochrony danych osobowych.

Poniżej rekapitulujemy obawy i zagrożenia dotyczące korzystania z przetwarzania w chmurze przedstawione autorom raportu przez menedżerów działów informatycznych banków.

Bariery regulacyjne

Realną barierą regulacyjną w szerszym stosowaniu Cloud computingu w sektorze finansowym mogą być zakazy ograniczeń odpowiedzialności dla dostawców usług („insorurcerów" wg terminologii ZBP) mające zastosowanie w stosunku do usług krytycznych (np. przetwarzania danych objętych tajemnicą bankową). Ten regulacyjny rygor pozostaje egzotyczny dla dostawców spoza Polski. Równocześnie może on zniechęcać instytucje finansowe do powierzania swoich procesów wspólnym dostawcom (insourcerom), w obawie przed „zakażeniem" w razie ewentualnego konfliktu między ich dostawcą chmury a innym usługobiorcą (odbiorcą chmury). Problem ten wiąże się z zagadnieniem upadłości dostawcy chmury,

który nie musi przecież być operatorem czy właścicielem poszczególnych centrów przetwarzania danych wchodzących w skład chmury.

Wyzwaniem regulacyjnym, zarówno krajowym, unijnym, jak i globalnym jest terytorialne podejście do ochrony danych osobowych i informacji. Brak pełnej unifikacji przepisów na terenie Unii Europejskiej, wielość regulatorów, z których każdy ma inne podejście i inaczej interpretuje prawo (brak stałości interpretacji jest też mniejszym lub większym, ale stałym problemem wszystkich regulatorów) jest barierą dla rozwoju. Część wymogów regulacyjnych, jak np.: pełne usuwanie danych nawet z kopii zapasowych, jest technologicznie trudna do spełnienia. Inne wymogi, jak możliwość kontroli dostawcy usługi przetwarzania danych przez powierzającego dane czy konieczność ujawnienia lokalizacji centrów przetwarzania danych, nie są chętnie akceptowane przez międzynarodowych dostawców, którzy traktują je na ogół jako utrudnienia w pracy lub zagrożenia dla bezpieczeństwa danych.

Wśród barier regulacyjnych wymienia się też brak regulacji wprost odnoszących się do Cloud computingu. Równocześnie jednak są głosy przeciwne, wskazujące na to, że istnieją regulacje dotyczące powierzania podmiotom zewnętrznym przetwarzania danych, a zatem że w istocie Cloud computing jest już uregulowany.

Przedstawiciele działów technologicznych banków wyrażają także oczekiwania skierowane do prawników, aby ci „rozsądzili", czy przetwarzanie chmurowe generuje ryzyko dla przetwarzanych danych. Bez względu na to, czy trafnie zostali określeni adresaci tego postulatu, wskazuje on, że istnieje potrzeba niezależnych analiz merytorycznych i porównawczej oceny bezpieczeństwa aktualnych rozwiązań stosowanych przez banki z rozwiązaniami w modelu Cloud computingu.

Koszt zmiany

Praktycznym problemem w przejściu do chmury jest koszt finansowy, organizacyjny, mentalny i ludzki zmiany.

Migracja do chmury jest wysiłkiem organizacyjnym, który wymaga sfinansowania oraz skutecznego przeprowadzenia. Tego typu bariera nie jest oczywiście swoista dla Cloud computingu, dotyczy każdej zmiany organizacyjnej czy technologicznej.

Problemem księgowym mogą być także niezamortyzowane nakłady na własną infrastrukturę. Rezygnacja z wykorzystywania infrastruktury przed jej księgowym okresem przydatności zaburza założenia finansowe, na podstawie których czyniono na nią nakłady. Nawet w przypadku gdy decyzja o „przejściu w chmurę" generuje istotne oszczędności, zrozumiała może być niechęć do takiego *ex post* „podważenia" sensowności wcześniejszych wydatków.

Co ciekawe, przedstawiciele banków wskazywali na to, że polskie banki charakteryzują się stosunkowo wysokimi kosztami działania, w tym kosztami informatyki. Wskazywano, że zwiększenie kosztów operacyjnych (Opex) nie byłoby pożądane, ponieważ pogarszałoby obraz rentowności działania banku, który podjąłby taką zmianę.

Koszt ludzki zmiany to konieczność restrukturyzacji wewnętrznego zespołu informatycznego. Wewnętrzne działy IT częściowo słusznie postrzegają dostawców zewnętrznych jako zagrożenie własnej egzystencji. Przejście na rozwiązania

chmurowe wymuszać może restrukturyzację w działach IT – zmniejszenie ich stanu osobowego, co zmienia nieco wymagania w stosunku do szefów tych działów. Jak wskazują indagowani przedstawiciele banków: „W sytuacji, w której bank posiada już infrastrukturę IT i decyduje się na skorzystanie z usług przetwarzania w chmurze, pozostaje do rozstrzygnięcia, co zrobić z niezamortyzowaną częścią infrastruktury oraz z utrzymującym ją zespołem?".

Oddzielnym zagadnieniem są koszty wyjścia z modelu. Bardzo trudno je obecnie oszacować i nie chodzi tu jedynie o bezpośrednie nakłady na odtworzenie infrastruktury, ale o efekty pośrednie i negatywny wpływ takiego powrotu na otoczenie i procesy biznesowe.

Zaufanie

Ograniczeniem rozwoju modelu chmury jest niski poziom zaufania służb wewnętrznych instytucji finansowych do tego sposobu funkcjonowania. Pomimo szybkiej utraty wartości technologii informatycznych i ich starzenia się, występuje dotychczas przeświadczenie, iż posiadanie zasobów IT jest „pewniejsze" niż korzystanie z zewnętrznych usług.

Ostrożnościowe podejście znalazło swoje odbicie w obowiązujących regulacjach prawnych, spotęgowanych przez interpretacje stosowane wewnętrznie w instytucjach. Jak wskazuje przedstawiciel działu informatyki jednego z banków: „Trudno nie odnieść wrażenia, iż np. regulacja dotycząca tzw. czynności faktycznych, utraciła swój pierwotny cel i stała się barierą dla świadczenia przez podmioty zewnętrzne zaawansowanych usług IT w bankach. Szczególnie iż często wewnętrzne interpretacje tych przepisów i wytyczne audytorów są bardziej konserwatywne niż stanowisko KNF".

Jak wskazują banki, standardy kontraktowe proponowane przez dostawców chmury, ograniczające ich kontraktową odpowiedzialność, nie zwiększają zaufania do oferowanych usług.

Transparentność oferty dostawców chmury

Deficyt zaufania dotyczy również promowanej oferty usługodawców. Nośność przekazu dotyczącego nowych rozwiązań technologicznych znacznie zmalała. Obecnie potencjalni odbiorcy usługi Cloud computing deklarują, że są w dużej mierze „uodpornieni" na komunikat marketingowy, że będzie „jeszcze lepiej", i podchodzą do niego z ostrożnością, traktując koncepcję przetwarzania w chmurze jako kolejną odsłonę outsourcingu usług IT ubranego w nowe szaty. Wyrażane są obawy, że Cloud computing powielać będzie błędy klasycznego outsourcingu, nie dając znaczących widocznych korzyści.

Obawa przed pogorszeniem stanu istniejącego

Indagowani przedstawiciele banków wyrażają także obawę przed powierzeniem swoich procesów podmiotom zewnętrznym, zwracając uwagę na strategiczną rolę IT w zarządzaniu kapitałem informacyjnym i w usprawnianiu procesów biznesowych. Wskazują także na wątpliwości, czy przy szczegółowych, wielowątkowych regulacjach i „niesprzyjającym zmianom klimacie" banki będą zdolne

do skupienia się jedynie na wąsko pojętej działalności bankowej – co dopiero mogłoby zmienić ich obecny model funkcjonowania.

Wśród obaw przed wdrożeniem modelu przetwarzania w chmurze wymienia się też – nie zawsze pozytywne – doświadczenia outsourcingu, takie jak utrata elastyczności działania, szybkości reakcji, braku efektywności kosztowej.

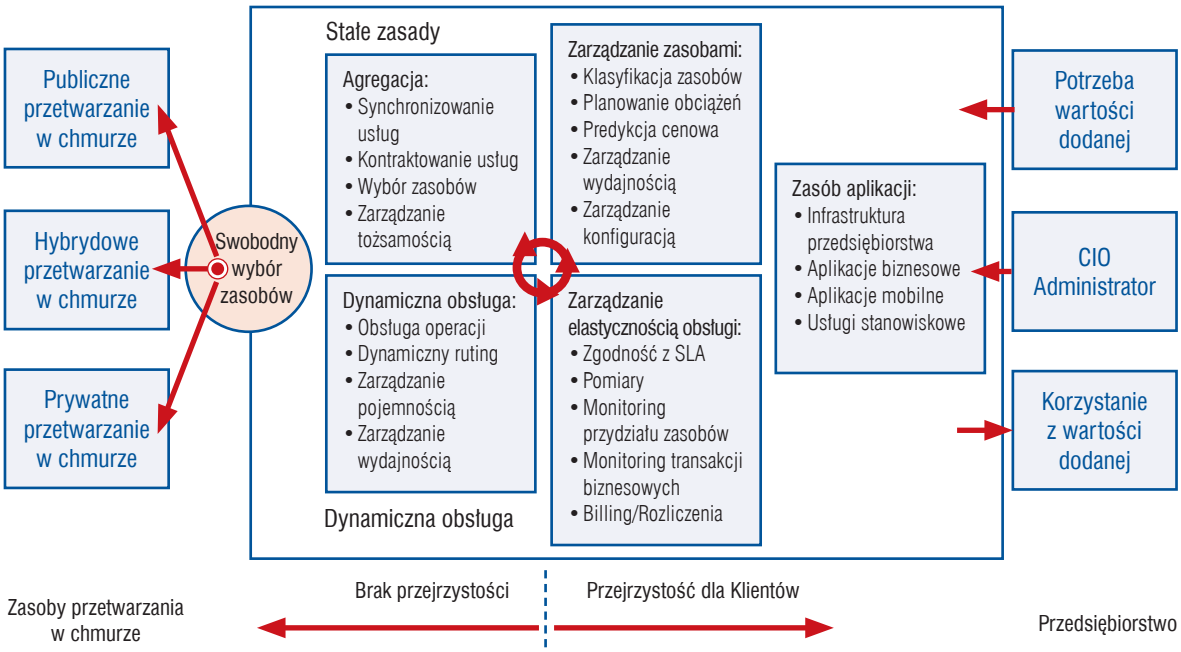
Oczekiwanie na pionierów

Powszechne jest też oczekiwanie na zrealizowane projekty migracji do chmury, na podstawie których będzie można ocenić efektywność modelu przetwarzania w chmurze oraz zoptymalizować jego operacyjne aspekty, tzw. efekt „wygrzania się" nowości, jaką wciąż w opinii wielu jest model przetwarzania w chmurze.

Koszt wyjścia

Przedstawiciele banków wskazują na potencjalny problem z rezygnacją z usług danego dostawcy, zmianą dostawcy lub insource'owaniem (odtworzeniem infrastruktury). Ryzyko *vendor lock-in* jest wymieniane wśród istotniejszych zagrożeń, także ze względu na potencjalne trudności z przeniesieniem usługi między dostawcami, związane z brakiem standardów branżowych i różnicami między platformami.

7. Możliwości wykorzystania modelu przetwarzania w chmurze



Rysunek 10. Ewolucja korzystania z przetwarzania w chmurze w kierunku bezpośrednich korzyści użytkowników

Źródło: [Belissent, Wisłowski, 2011].

Dobre praktyki

Przed skorzystaniem z usługi przetwarzania w chmurze konieczne są dokładne analizy, które pozwolą odpowiedzieć na postawione niżej pytania oraz pomogą wybrać najlepsze rozwiązanie odpowiadające wymaganiom i charakterystyce działania danej organizacji.

1) Konieczne jest przeprowadzenie dokładnych analiz wewnątrz organizacji, dzięki którym otrzyma się:
   - aktualny obraz działania firmy,
   - obraz infrastruktury IT (architektura, software, hardware),
   - sugestie wskazujące, które elementy firmy „przenieść" do chmury,
   - informacje o tym, jakie dostępne na rynku rozwiązania będą najodpowiedniejsze dla oczekiwań i wymagań firmy.
2) Konieczna jest też analiza rynku, dzięki której będzie wiadomo:
   - z jakich rozwiązań możemy skorzystać,
   - których dostawców należy brać pod uwagę.
3) Działania, które muszą być podjęte, by dobrze przygotować się do wejścia w usługę przetwarzania w chmurze:
   - należy zdecydować, które procesy biznesowe mają być wspierane przez usługi teleinformatyczne, aby zdefiniować ich katalog,
   - dla każdej zdefiniowanej usługi należy opisać wymagania określające jej dostępność, sposób działania, bezpieczeństwo danych,
   - należy określić i uzgodnić, które z usług należy przetwarzać wewnętrznie, a które mogę być obsługiwane przez firmy zewnętrzne,
   - należy zmierzyć aktualny, wewnętrzny nakład pracy/zasobów niezbędny do dostarczania usługi na obecnym poziomie,
   - należy przyjrzeć się obecnej infrastrukturze pod kątem możliwości poprawienia, uproszczenia, racjonalizacji i standaryzacji działania procesu,
   - należy znaleźć odpowiedniego dostawcę rozwiązań przetwarzania w chmurze dla usług, które mogą być przekazane na zewnątrz.
4) Gdy zostanie już podjęta decyzja o przejściu do usługi przetwarzania w chmurze i określi się grupę potencjalnych dostawców, należy zadać następujące pytania:

Czy dany dostawca:

- Jest w stanie zaprezentować referencje udanego wdrożenia podobnego rozwiązania informatycznego?
- Oferuje bezpłatne wersje testowe proponowanego rozwiązania?
- Dostarcza umowy typu SLA (*service level agreement*) i czy może zaprezentować historię dostępności i niezawodności dostarczanych usług? Co w przypadku niewywiązania się przez dostawcę z zapisów SLA?
- Ma sposób działania/realizowania usługi, który jest przejrzysty, i czy dostawca daje możliwość wglądu w sposób realizowania usługi?

- Posiada Disaster Recovery Plan (DRP)? Czy był on przetestowany? Czy DRP działa?
- Jakie są możliwości i polityka ochrony danych przetwarzanych przez usługę, ochrony zarówno fizycznej, jak i proceduralnej? Jak usługa jest zabezpieczona, zgodnie z jakimi standardami (PCI, SAS70, HIPPA, NIST)? Jak dostawca ma zamiar zapewnić dodatkowe obostrzenia związane z bezpieczeństwem przetwarzania danych, wynikające z charakteru prowadzonego biznesu (np. banki)?
- Czy możliwa jest łatwa konfiguracja, modyfikacja i dostosowanie usługi do zmieniającego się biznesu?

Funkcjonalne obszary zastosowań

Istnieje już wiele rozwiązań wspierających przetwarzanie w chmurze. Z uwagi na ciągły ich rozwój i rosnącą liczbę udanych wdrożeń, zakres możliwych zastosowań przetwarzania w chmurze ciągle poszerza się. Poniżej zostały wskazane ciekawsze z możliwych zastosowań. Opisane funkcjonalne obszary zastosowań mogą być realizowane w każdym z trzech wymienionych wcześniej modeli przetwarzania w chmurze (IaaS, PaaS, SaaS), w zależności od potrzeb i specyfiki działalności organizacji.

Obsługa klientów oraz zarządzanie relacjami z klientami

Jest to najbardziej oczywisty i najczęściej stosowany obszar funkcjonalny, w którym możliwe jest zastosowanie przetwarzania w chmurze. Na rynku działa wielu dostawców specjalizujących się w aplikacjach wspomagających obsługę klienta, dostarczających zaawansowane, łatwo konfigurowalne i modyfikowalne zgodnie z potrzebami klienta rozwiązania. Zastosowanie usług wspierających obsługę CallCenter lub aplikacji typu CRM (Customer Relationship Management) pozwala na poprawienie i uproszczenie procesów związanych z obsługą klienta. Wymiernymi korzyściami wynikającymi w zastosowania przetwarzania w chmurze w tym zakresie funkcjonalnym są:

- podniesienie wydajności pracy/obsługi agentów,
- skrócenie czasu obsługi klienta,
- zwiększenie liczby obsługiwanych klientów,
- pełna i aktualna wiedza na temat klienta (historia kontaktów, informacje na temat posiadanych przez klienta produktów, opłat, tzw. „widok 360” dla każdego klienta),
- zmniejszenie liczby reklamacji,
- zwiększenie lojalności i zaangażowania klienta.

Sprzedaż

Wykorzystanie usługi przetwarzania w chmurze w procesach sprzedażowych (np. sprzedaż pośrednia kredytów samochodowych z wykorzystaniem dealerów lub sprzedaż bezpośrednia produktów bankowych za pośrednictwem przedsta-

wicieli bankowych) skutkuje zwiększeniem efektywności i wydajności sprzedawców. Doradcy klienta, sprzedawcy, specjaliści ds. produktów mają dostęp do jednego miejsca, w którym znajduje się aktualna informacja na temat oferty sprzedażowej. Proces sprzedaży jest wystandaryzowany.

Wymierne efekty to zwiększenie sprzedaży netto oraz dochodowości. Dzięki analizie danych klienta oraz posiadanych przez niego produktów, opiekunowie klienta mogą zaproponować produkt, który odpowiada jego potrzebom.

Dobrym rozwiązaniem jest integracja rozwiązania sprzedażowego z rozwiązaniami wspomagającymi klasy CRM (opisanymi we wcześniejszym akapicie).

Marketing

Przygotowywanie ofert i planowanie kampanii marketingowych to kolejny obszar funkcjonalny, który może zostać przeniesiony do usługi przetwarzania w chmurze. Jedno miejsce, w którym specjaliści ds. marketingu mogą mieć dostęp do aktualnych danych klientów i produktów nabytych przez tych klientów, produktów oferowanych przez bank oraz analiz i raportów sprzedażowych czy produktowych, jest typowym do zastosowania rozwiązaniem wykorzystującym przetwarzanie w chmurze. Klasyczne już jest przenoszenie do przetwarzania w chmurze aplikacji wspierających mailing do klientów oraz baz marketingowych.

HR (*Human Resources*)

Przeniesienie narzędzi i aplikacji służących do zarządzania zasobami ludzkimi do usługi przetwarzania w chmurze, pozwala na integrację narzędzi i usług wspomagających HR z portalami specjalizującymi się w wyszukiwaniu pracowników oraz portalami społecznościowymi. Możliwy też jest własny portal lub aplikacja rekrutacyjna działająca w chmurze.

Przykładowe rozwiązania z sektora bankowego

Jednym z rozwiązań, które jest wykorzystywane przez banki w modelu usługi przetwarzania w chmurze, jest aplikacja do wykrywania operacji „prania brudnych pieniędzy" (AML – *anti-money-laundering*). Podstawą działania tego rozwiązania są dane o transakcjach.

Poniżej przykładowe wdrożenia tego systemu.

- Aplikacja została zainstalowana w siedzibie banku w Luksemburgu i w modelu chmury prywatnej udostępniana jest organizacjom zależnym w Austrii i Luksemburgu. W ten sposób powstała jedna instalacja, a końcowi użytkownicy przez dedykowany kanał mają swobodny dostęp do pełnej funkcjonalności narzędzia. U podstaw wyboru tego modelu leżał niższy koszt wdrożenia rozwiązania dla całej grupy oraz fakt, że banki zależne nie posiadają praktycznie własnych zespołów IT, wszystko jest scentralizowane w firmie „matce".
- Z kolei bank z Jersey korzysta z modelu chmury hybrydowej. Część aplikacji pozyskuje z centrali banku w Londynie, natomiast moduł do przeciwdziałania „praniu brudnych pieniędzy" pozyskuje od zewnętrznego dostawcy w modelu przetwarzania w chmurze. Centrum outsourcingowe jest zlokalizowane na

wyspie Jersey i obsługuje 80% lokalnych instytucji finansowych. O takim modelu zadecydował koszt obsługi infrastruktury teleinformatycznej oraz fakt, że bank nie posiada departamentu IT.

- Lokalny dostawca zasobów teleinformatycznych w modelu przetwarzania w chmurze z Zurychu oferuje pakiet rozwiązań dla banków, w tym wspomnianą aplikację. Do korzystania z takiego modelu skłoniła banki cena i pełna obsługa infrastruktury za niewielki koszt w porównaniu z kosztem stworzenia własnego rozwiązania. Pakiet startowy, to poziom mniej więcej 70–90% rocznego kosztu pojedynczego pracownika IT, natomiast roczne utrzymanie to poziom 25% takiego kosztu.

- Bank of America zauważył, że wielu z jego obecnych oraz potencjalnych klientów szuka informacji i odpowiedzi na nurtujące ich pytania na forach oraz portalach społecznościowych. Klienci dopytywali się np. jak bank prezentuje się na tle konkurencji, jakie są stopy procentowe, na co należy uważać. Dzięki wdrożeniu aplikacji wspierającej wymianę danych, BofA dołączył do rozmów portalowych. Agenci dostali narzędzie, dzięki któremu mogli na bieżąco odpowiadać na pojawiające się wątki w dyskusji.
  Obecnie bank na jednym z portali społecznościowych odpowiada na ponad 1100 wpisów dziennie i ma ponad 6000 aktywnych użytkowników.

- W Banku SunTrust wdrożono pięć linii biznesowych korzystających z wielu systemów działających w tle. Chciał on się wyróżnić przez dostarczanie spersonalizowanych usług, przy jednoczesnej poprawie wydajności swoich doradców oraz uruchomieniu nowego strumienia przychodów i maksymalizacji cross-sellingu. Dotąd bank nie był w stanie uzyskać spójnego obrazu klienta na podstawie informacji z wykorzystywanych systemów. Dodatkowo metody sprzedażowe, które bank wprowadził, nie były wspierane przez narzędzia informatyczne.
  Po upewnieniu się, że rozwiązanie zaproponowane przez dostawcę spełnia wymogi bezpieczeństwa, wydajności oraz niezawodności, bank skorzystał z zaproponowanego rozwiązania przetwarzania w chmurze, polegającego na udostępnieniu w ten sposób wybranych systemów hurtowni danych banku. Powstało rozwiązanie, w którym dostępna jest pełna i aktualna informacja na temat klienta i jego relacji z bankiem. W ciągu dwóch lat bank zwiększył przychody ze sprzedaży. Podniesiona została produktywność sprzedawców oraz skrócony czas wdrożenia nowego sprzedawcy (z miesięcy do dni).

8. Przyszłość przetwarzania w chmurze

Przetwarzanie w chmurze jest prawdopodobnie największą rewolucją, jakiej doświadczała w swej historii informatyka, i z pewnością stanie się powszechnie dostępną usługą. Zresztą przetwarzanie w chmurze jest już powszechnie wykorzystywanym modelem usługi w sferze Internetu konsumenckiego. Dużo mniej jest jeszcze upowszechnione w sferze biznesu. Niemniej jednak szacuje się[9], że

[9] Pew Internet & American Life Project (2008), Compuware (2010)

w ciągu zaledwie kilku lat korzystanie z przetwarzania w chmurze stanie się powszechne. Doprowadzi do tego:

- standaryzacja przeglądarek i działających w nich aplikacji,
- miniaturyzacja i standaryzacja urządzeń informatycznych,
- dynamiczny rozwój urządzeń mobilnych.

Nie bez znaczenia jest też fakt, że powszechne w sferze konsumenckiej korzystanie z usług i narzędzi opartych na przetwarzaniu w chmurze spowoduje na zasadzie oswojenia i przyzwyczajenia osobistego akceptację tego modelu usługi także w zastosowaniach biznesowych.

Szacuje się, że od 2009 roku rozpoczął się proces stopniowego absorbowania modelu przetwarzania w chmurze w sferze biznesu. Prawdopodobnie będzie on przebiegać stopniowo w zachodzących na siebie fazach:

- wdrożenia w chmurze aplikacji typu *start-up*, niedostatecznej standaryzacji, niedostatecznej konkurencji dostawców usług, obawy o bezpieczeństwo (z tym etapem mamy wciąż do czynienia, choć w fazie dla niego schyłkowej),
- wewnętrznej migracji do chmury prywatnej, ale bez efektu skali, a tym samym bez odpowiednio znaczących oszczędności (ten etap jest już zaawansowany, choć niedostatecznie powszechny),
- dominacji chmury prywatnej, pokonywania bariery mentalnej obawy przed chmurą publiczną (ten etap już się rozpoczął na znaczącą skalę),
- przechodzenia do modelu przetwarzania na żądanie (ocenia się, że potrwa ono przez czas pokoleniowej wymiany menedżerów biznesu, którzy kierują się niestety naturalnym oporem przed nowym).

Prognozy ewolucji przetwarzania w chmurze

- Przetwarzanie w chmurze będzie tańsze, bardziej niezawodne, bezpieczniejsze i prostsze w użyciu.
- Przetwarzanie w chmurze stanie się motorem napędzającym wzrost firm i przewagę konkurencyjną tych, którzy pierwsi przejdą na ten model.
- Koszty dostawców usługi przetwarzania w chmurze będą kształtować się na poziomie ok. 25% kosztów ponoszonych na prowadzenie własnego centrum przetwarzania danych.
- Liderzy rynku wypracują szeroko rozumiane standardy przetwarzania w chmurze. Pojawią się też standardy ISO w tym zakresie.
- Model SaaS będzie się rozwijać, podobnie jego usługi na bazie powstających i doskonalonych standardów.

Prognozy ewolucji generowania oprogramowania w chmurze

- Szkielety aplikacji (a*pplication framework*) — takie jak obecnie Ruby on Rails, Apache Struts, Adobe Flex, PHP, Python – odegrają istotną rolę w upowszechnianiu przetwarzania w chmurze.

- Warstwa logiki aplikacji i warstwa danych będą najczęściej powierzane do przetwarzania w chmurze.
- Mechanizmy składowania danych czeka radykalna ewolucja związana przede wszystkim z danymi nieustrukturyzowanymi oraz skalowaniem baz danych.
- Usługi zabezpieczania dopracują się dedykowanych rozwiązań związanych z przetwarzaniem w chmurze.
- Firmy prowadzące biznes oparty na udostępnianiu komercyjnym rozległych repozytoriów danych przygotują dedykowane rozwiązania oferujące ich usługi w modelu przetwarzania w chmurze.
- Aplikacje wykorzystujące inne istniejące usługi (*mashup*) upowszechnią korzystanie z przetwarzania w chmurze, co zostanie dodatkowo wsparte dedykowanymi do tego celu narzędziami programistycznymi.
- Modele PaaS i FaaS staną się dominującym sposobem wytwarzania aplikacji.
- Posiadanie infrastruktury oraz narzędzi teleinformatycznych przestanie być barierą zawodową, co zwiększy konkurencję.

Wnioski

Dostępność mocy obliczeniowej

W dzisiejszych czasach moc obliczeniowa staje się coraz bardziej dostępna.

Powszechność wiedzy

Zagadnienia ściśle technologiczne (jak np. zapewnianie bezpieczeństwa danych, przetwarzania wielkich wolumenów), jak i zagadnienia organizacyjne (np. procesy HR, organizacja poczty elektronicznej) standaryzują się. Standardy zaś są podstawą upowszechniania się wiedzy o możliwych zastosowaniach.

Implikacje ekonomiczne

Postęp techniki przetwarzania w chmurze zmierza w kierunku porównywalnym do dostarczania prądu, gazu, wody. Podobnie jak w przypadku energii elektrycznej zadziała ekonomia skali jak i możliwości optymalizacji parametrów samej usługi. Spowoduje to jej powszechność i obniżanie kosztów.

Przejściowe bariery

Problemy ze standaryzacją, wymienialnością, zaufaniem, kontrolą nad danymi, różnicami w systemach prawnych z czasem zostaną pokonane.

Pola konkurencji

Przedsiębiorcy, w tym instytucje finansowe, w dalszym ciągu będą rozwijać wewnętrzne kompetencje informatyczne i zatrzymywać dla siebie te elementy systemów informatycznych, których rozwiązania ucieleśniają ich przewagę konkurencyjną. Dlatego właśnie najwięksi najpóźniej lub najmniej skorzystają na nowym modelu korzystania z zasobów teleinformatycznych, gdyż już dysponują istotną skalowalnością i kompetencją wewnątrz własnych organizacji.

W obliczu konkurencji zewnętrznej, wewnętrzne działy IT wzmocnią nacisk na efektywność i zadowolenie biznesowego użytkownika (czy to wewnętrznego, czy też klienta). To jednak nie zmieni ogólnego trendu, jakim jest powszechność przetwarzania w chmurze.

Miejsce polskiego sektora finansowego

Mniej lub bardziej świadomie wypracowaną decyzją będzie to, gdzie w tym postępie technologiczno-biznesowym znajdzie się polski sektor finansowy. Czy opłaca się być w awangardzie, czy lepiej być tzw. *followerem*, czy też należy zachować daleko posuniętą ostrożność i plasować się raczej w ariergardzie postępu. Ważne, by odpowiedź na te pytania i konsekwentne nastawienie regulacyjne, nadzorcze i sektorowe względem przetwarzania w chmurze zostały określone w sposób świadomy i z perspektywy bilansu zalet i wad przetwarzania w chmurze z punktu widzenia polskiego sektora finansowego i całej polskiej gospodarki, a więc jako przypadkowy wynik zagregowanych postaw poszczególnych opiniotwórczych osób – od entuzjastów do mocnych sceptyków.

Stanowisko Unii Europejskiej

Najlepszym podsumowaniem naszego Raportu jest dokument Komisji Europejskiej pod tytułem *Unleashing the Potential of Cloud Computing in Europe* („Wykorzystanie potencjału chmury obliczeniowej w Europie")[10] datowany na 27 września 2012 roku i adresowany do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Społeczno-Ekonomicznego i Komitetów Regionów. W dokumencie tym Komisja Europejska jednoznacznie wskazuje na Cloud computing jako zjawisko technologiczno-biznesowe, umożliwiające skokową akcelerację wzrostu ekonomicznego w Europie (czytaj: „tam na świecie, gdzie zdecydują się z niego skorzystać").

KE nie ma wątpliwości co do korzyści płynących z Cloud computingu i co do logicznej nieuchronności korzystania z niego. KE wskazuje trzy główne wyzwania, którym trzeba sprostać, aby w pełni „uwolnić potencjał chmury":

- standaryzacja technologiczna (interoperacyjność i transparentność jakościowa – zapewniana przez certyfikację);
- standaryzacja kontraktowa (określenie pewnego standardowego poziomu i zestawu zobowiązań dostawców chmury, względem którego będzie można pozycjonować ofertę poszczególnych dostawców oraz oceniać tę ofertę w skali „minimum/wystarczająco/bogato");
- przełamanie „oporu materii" – ubrane przez KE w dyplomatyczną ofertę stworzenia wspólnoty zamówień na Cloud computing w sektorze publicznym, nawet do stopnia transgranicznego.

Na koniec zwracamy uwagę Czytelnika, że Komisja Europejska nie zastanawia się już nad pytaniem, czy korzystanie z Cloud computingu ma sens. KE autorytatywnie stwierdza, że sens ten jest nieuchronny, z czym zgadzają się autorzy niniejszego raportu.

[10] http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf – odnośnik wg stanu z daty 06.11.2012 r.

Uwagi końcowe

Wszystkich, którzy zapoznali się z tym raportem, zachęcamy do dyskusji i przekazywania uwag na jego temat. W miarę sił, środków i potrzeb, możliwe że powstaną kolejne wersje raportu, uwzględniające rozwój praktyki i myśli dotyczącej przetwarzania w chmurze. A być może w niedługim czasie powszechność zastosowań tego modelu usług sprawi, że takie opracowania jak niniejsze będą zupełnie zbędne.

Współcześnie zmiany gospodarcze i technologiczne zachodzą tak szybko, że publikacja ich dotycząca od dnia jej ogłoszenia sukcesywnie się dezaktualizuje. Toteż zachęcamy Czytelników do reakcji na jej ukazanie się przez zgłaszanie uwag do wspólnej pracy nad jej kolejnymi wersjami.

Źródła

Belissent J., **Wisłowski L.** [2011], *Czy z tej chmury będzie deszcz? Globalne trendy IT w obszarze przetwarzania w chmurze*, ForresterResearch.

Cellary W. [2010], *Co dalej w technice informatycznej?* [w:] Zawiła-Niedźwiecki J., Rostek K., Gąsiorkiewicz A. (red.) *Informatyka gospodarcza,* C.H. Beck.

Gawroński M. [2012], *Cloud computing w sektorze finansowym. Regulacje i standardy*, Kancelaria Bird&Bird.

Gillet S.E., **Kapor M.** [1997], *The Self-governing Internet: Coordination by Design,* MIT Press.

Erl T. [2007], *SOA Principles of Service Design,* Prentice Hall.

IDC White Paper [2009], *Force com Cloud Platform Drivers Huge Time to Market and Cost Savings*, doc #219965.

Łapiński K., **Wyżnikiewicz B.** [2011], *Cloud computing – wpływ na konkurencyjność przedsiębiorstw i gospodarkę Polski (raport)*, Instytut Badań nad Gospodarka Rynkową.

Mateos A., **Rosenberg J.** [2011], *Chmura obliczeniowa,* Helion.

Nowicka K. [2011], *Outsourcing a funkcjonowanie przedsiębiorstwa – rola modelu cloud computing*, „Przegląd Organizacji" nr 11.

Poniatowska-Jaksch M. [2012], *Modele biznesu w epoce Network economy*, [w:] M. Duczkowska-Piasecka (red.), *Model biznesu w zarządzaniu przedsiębiorstwem*, Wydawnictwo SGH.

Shaw T.I. [2011], *Cloud Computing for Lawyers and Executives*, wyd. Autonomous Legal & Technology Publishing.

Sobińska M. [2010], *Zarządzanie usługami outsourcingowymi* [w:] Zawiła-Niedźwiecki J., Rostek K., Gąsiorkiewicz A. (red.) *Informatyka gospodarcza,* C.H. Beck.

Sosinsky B. [2011], *Cloud computing Bible,* Wiley Publishing.

The Evolution of Cloud Computing Markets [2010], Forrester Research.

Trocki M. [2011], *Outsourcing,* PWE.

http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf

O autorach

Profesor Remigiusz W. Kaszubski

(1970–2012)

Raport jest poświęcony pamięci tragicznie zmarłego Prof. Remigiusza Kaszubskiego. Profesor aktywnie działał w obszarze rozwoju nowoczesnych technologii i był osobiście zaangażowany w prace Forum. Zgodnie z zamierzeniami Grupy FTB ds. Cloud computing i autorów raportu, raport miał być wydany pod redakcją Profesora.

Profesor Remigiusz Kaszubski był człowiekiem odnoszącym sukcesy w sferze zawodowej i naukowej. Wyróżniał się nie tylko najwyższym profesjonalizmem, ale także szczególną konsekwencją i ambicją w realizacji celów. Entuzjazm i zaangażowanie Profesora Kaszubskiego pozwalały z niebywałą łatwością integrować środowisko bankowe wokół wspólnych projektów. Z powodzeniem wdrażał koncepcję innowacyjnej bankowości, służącej rozwojowi nowoczesnego państwa. Dzięki wielkiemu zaangażowaniu Remigiusza Kaszubskiego w działania wielu organizacji, polski system bankowy, a w szczególności system bankowości elektronicznej, jest jednym z najnowocześniejszych, najbezpieczeniejszych i najlepiej funkcjonujących systemów w Europie.

Prof. Remigiusz Kaszubski był osobą szczególnie ważną w historii Związku Banków Polskich. Był inicjatorem, pomysłodawcą i współtwórcą podmiotów, które wydatnie przyczyniły się do poprawy funkcjonowania sektora bankowego. Kierując pracami Rady Wydawców Kart Bankowych, zbudował Forum Przeciwdziałania Przestępstwom Kartowym, następnie reaktywował działania Rady Bankowości Elektronicznej, w ramach której zainicjował prace Forum Technologii Bankowych oraz Forum Bezpieczeństwa Transakcji Elektronicznych. Przyczynił się do powołania Komitetu Agentów Rozliczeniowych. Ostatnim ważnym projektem, który realizował był Program SEPA Polska.

Profesor Kaszubski z charakterystyczną dla siebie życzliwością i cierpliwością odnosił się do wszystkich z którymi współpracował. W naszej pamięci pozostanie na zawsze jako osoba ciepła, niezwykle otwarta wobec innych, służąca zawsze dobrym słowem i radą.

Ewa Dybka

IMPAQ Polska, Sales Director – Banking

Na początku swojej kariery poznawała struktury bankowości, a od 2006 roku aktywnie działa na rynku IT, zdobywając szerokie doświadczenie zarówno u największych producentów IT na świecie, jak i u integratorów w Polsce. W IMPAQ Polska odpowiada za Sektor Bankowości.
Absolwentka Szkoły Głównej Handlowej w Warszawie na kierunku Metody Ilościowe i Systemy Informacyjne w Ekonomii ze specjalizacją Informatyka Gospodarcza.

Dariusz Falkowski

Outbox Sp. z o.o., Dyrektor Handlowy Pionu usług dla sektora finansowego

Ponad 20-letnie doświadczenie w dziedzinie zarządzania sprzedażą dedykowanych systemów informatycznych dla sektora komercyjnego, publicznego i finansowego. Od ukończenia studiów pracował w departamentach sprzedaży systemów ITC w takich międzynarodowych korporacjach, jak: Alcatel, IBM, Bull, Raindrop IS, Logix.
Magister Ekonomii, absolwent Cybernetki Ekonomicznej Wydziału Ekonomiki Produkcji Uniwersytetu Gdańskiego.

Robert Gajda

Microsoft Polska, Business Development Manager

Posiada ponad 15-letnie doświadczenie w branży IT. W Microsoft Polska odpowiada m.in. za rozwój rynku związanego z obszarem cloud. Absolwent Akademii Górniczo-Hutniczej im. Stanisława Staszica w Krakowie, Wyższej Szkoły Zarządzania i Prawa w Warszawie oraz posiada tytuł MBA University of Illinois.

Maciej Gawroński

Partner zarządzający polskim biurem Bird & Bird

Jest uznanym ekspertem w dziedzinie IT oraz prawa finansowego z niemal 20-letnim doświadczeniem w doradztwie prawnym. Szef praktyki IT. Od 1994 roku doradza przedsiębiorcom. Specjalizuje się w doradztwie prawnym w zakresie IT, fuzji i przejęć, prawie korporacyjnym, bankowym i finansowym, ochronie danych osobowych, własności intelektualnej, negocjacjach handlowych oraz rozwiązywaniu sporów (arbitraż i spory sądowe) szczególnie z obszaru inwestycji budowlanych. Posiada również doświadczenie w zakresie telekomunikacji. Doradzał przy największych wdrożeniach informatycznych w kraju.
Studiował prawo na Uniwersytecie Jagiellońskim i Uniwersytecie w Tours we Francji.

Martyna Kubiak

Od siedmiu lat jest Sekretarzem Forum Technologii Bankowych (FTB) przy Związku Banków Polskich

Specjalizuje się w obszarze gospodarki elektronicznej i nowoczesnych technologii sektora finansowego i publicznego. Pośredniczy we współpracy firm technologicznych oraz banków w zakresie propagowania obrotu bezgotówkowego i implementacji nowoczesnych technologii. Koordynuje prace Grup roboczych FTB ds. biometrii, identyfikacji i uwierzytelnienia, zarządzania ciągłością działania – BCM (Business Continuity Management) oraz Cloud computing, jak również Grupy Rady Bankowości Elektronicznej ds. społeczeństwa informacyjnego i eAdministracji. Przygotowuje i opracowuje statystyki dotyczące rozwoju bankowości elektronicznej w Polsce.
Organizuje szkolenia i konferencje tematyczne FTB w zakresie prowadzenia działalności edukacyjnej FTB, jak również wiele przedsięwzięć związanych z promocją obrotu bezgotówkowego, upowszechnianiem rozwiązań informatycznych, nowoczesnych technologii i bezpieczeństwa bankowości elektronicznej.
Absolwentka Wydziału Prawa na Uniwersytecie Kardynała Stefana Wyszyńskiego oraz studiów podyplomowych Szkoły Głównej Handlowej.

Wojciech Małek

Microsoft Polska, zajmuje się sprzedażą rozwiązań Cloud computing, w szczególności ofertą do pracy grupowej w chmurze – Office 365

Menedżer sprzedaży posiadający ponad 15 lat doświadczenia w branży IT. Pracę rozpoczynał w TP SA, pracował również w firmach Hewlett-Packard, EMC i Teradata. Współpracował z działami IT największych instytucji finansowych w Polsce. Zajmował się projektami związanymi z konsolidacją danych, wirtualizacją, hurtowniami danych i Business Intelligence. Absolwent Wydziału Elektroniki Politechniki Warszawskiej oraz Warszawskiej Szkoły Biznesu.

Przemysław Mazurkiewicz

CompFort Meridian Polska, Dyrektor ds. Rozwoju i Utrzymania

W latach dziewięćdziesiątych administrator systemów w „Gazecie Wyborczej"; redaktor w dodatku Gazety „Biuro i Komputer". Od 1998 roku w CompForcie, kolejno: konsultant, zastępca dyrektora ds. Oprogramowania, Presales & Product Sales Director, Consulting Services Director, Dyrektor Operacyjny OS. Specjalizuje się w rozwiązaniach do zarządzania infrastrukturą, usługami IT oraz bezpieczeństwem informatycznym.

Piotr Piskorz

Outbox Sp. z o.o., Dyrektor Financial Services

Kieruje Departamentem Financial Services, w ramach którego jest architektem strategii, rozwiązań i liderem wdrożeń z dziedziny CRM i szeroko rozumianego Customer Experience, a także rozwiązań chmurowych. Posiada 13-letnie doświadczenie w doradztwie strategicznym i zarządzaniu projektami dla branży bankowości, ubezpieczeń oraz funduszy inwestycyjnych. Przed objęciem stanowiska w Outbox pracował w Accenture, Banku Ochrony Środowiska oraz ING Nationale-Nederlanden Polska.
Absolwent Szkoły Głównej Handlowej, studiów podyplomowych SGH w dziedzinie zarządzania systemami informatycznymi oraz Project Management Institute.

Janusz Zawiła-Niedźwiecki

Naukowiec, dydaktyk i praktyk zarządzania biznesem

W przeszłości – m.in. dyrektor informatyki Giełdy Papierów Wartościowych, członek zarządu i dyrektor zarządzający PZU, kierownik europejskiego projektu Platformy Lokalizacyjnej (część systemu ratownictwa E112). Laureat nagrody „Lider Informatyki" (jako dyrektor IT Giełdy) tygodnika Computerworld w 1998 i 1999 r.
Obecnie – doradca biznesowy, przewodniczący Rady Fundacji im. Prof. K. Bartla, naukowiec i dydaktyk na Wydziale Zarządzania Politechniki Warszawskiej, gościnnie wykładowca Collegium Civitas, Warszawskiego Uniwersytetu Medycznego i Uniwersytetu Ekonomicznego we Wrocławiu. Laureat nagród Ministra Przekształceń Własnościowych i Rektora Politechniki Warszawskiej. Autor przeszło 200 publikacji, redaktor monografii: *Informatyka gospodarcza* (nagroda wydawców ekonomicznych 2011) i *Zarządzanie ryzykiem operacyjnym*. Autor książek: *Bezpieczeństwo systemów informacyjnych* i *Zarządzanie ryzykiem operacyjnym w zapewnianiu ciągłości działania*; członek Polskiej Komisji Akredytacyjnej.
Więcej – www.januszzawilaniedzwiecki.com

Michał Zgajewski

ATM Systemy Informatyczne SA, Dyrektor Działu Sprzedaży do Sektora Finansowego

Menedżer z 8-letnim doświadczeniem w sprzedaży na rynku IT. Członek grupy roboczej konsultujący „Księgę dobrych praktyk w obszarze Zarządzania Ciągłością Działania" oraz przewodniczący grupy roboczej Cloud Computing w ramach Forum Technologii Bankowych przy Związku Banków Polskich. Karierę zawodową rozpoczynał jako analityk ekonomiczny.
Absolwent Wydziału Zarządzania Uniwersytetu Łódzkiego oraz podyplomowych studiów w Szkole Głównej Handlowej.

Redakcja merytoryczna i korekta: edu-Libri
Opracowanie graficzne: GRAFOS
Ilustracja na okładce: Ig0rZh/iStockphoto.com

Wydawnictwo edu-Libri
ul. Zalesie 15, 30-384 Kraków
e-mail: edu-libri@edu-libri.pl
www.edu-libri.pl

edu-Libri

FORUM TECHNOLOGII BANKOWYCH

ZWIĄZEK BANKÓW POLSKICH