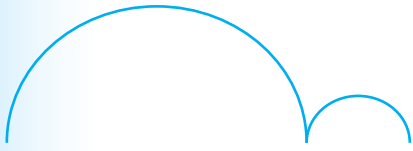


> Projekt

TEZEUSZ

Przeniesienie systemów
archiwalnych banku do
chmury publicznej

OPIS INICJATYWY



SPIS TREŚCI

3

Executive Summary

6

Definicja chmury
obliczeniowej

8

Wyzwania usług chmurowych
na rynku bankowym
w Polsce

10

Cel projektu Tezeusz

12

Wymagania i założenia

15

Architektura rozwiązania

23

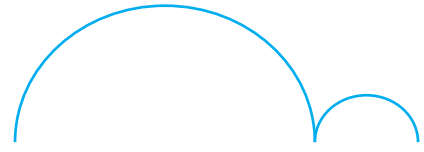
Ryzyka i wyzwania

28

Wnioski

30

Załączniki



EXECUTIVE SUMMARY

W ramach działalności FTB został powołany projekt TEZEUSZ, który miał doprowadzić do odpowiedzi, czy projekt umieszczenia systemów archiwalnych banku w chmurze publicznej – w wariancie najprostszym od strony prawnej/regulacyjnej i jednocześnie maksymalnie opłacalnym dla banku – może być skutecznie zrealizowany przez wybrany bank?

Zakres projektu stanowiło 12 maszyn wirtualnych stanowiących środowisko systemów archiwalnych Banku, do których zostało przedstawionych 18 wymagań i 6 założeń (dot. architektury, dostępności, licencji, utrzymania, lokalizacja danych itd.).

CELE PROJEKTU

1

Przygotowanie dokumentu ze wskazówkami najlepszych praktyk (best practices guidelines) dla scenariusza opisującego powyższy projekt. Cały projekt został oparty o rzeczywiste dane banku Raiffeisen Polska (Bank).

Analiza wykonalności technicznej projektu

- w dwóch rozwiązaniach chmurowych
- Infrastructure-as-a-Service (IaaS) oraz
 - Platform-as-a-Service (PaaS), w dwóch technologiach (Microsoft oraz IBM).

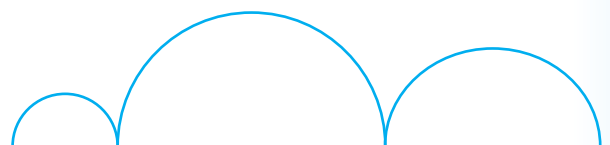
2

3

Analiza ryzyk projektowych.

Wycena kosztów – szacunkowe koszty przechowywania systemów archiwalnych w chmurze publicznej (tj. koszty mocy obliczeniowej, oprogramowania, wsparcia, wprowadzania zmian, warunków płatności, itd.). Wycena bazowała na ogólnie dostępnych danych poszczególnych dostawców usług. Wyceny usług chmurowych zostały przekazane Bankowi i celowo nie zostały włączone do niniejszego dokumentu.

4



WNIOSKI

Na podstawie przeprowadzonych analiz zespół projektowy doszedł do wniosku, że projekt przeniesienia systemów archiwalnych do chmury publicznej, na podstawie posiadanych danych o infrastrukturze Banku, jest:

W Y K O N A L N Y

Wykonalny od strony technicznej – zapewniając odpowiednie SLA dla aplikacji oraz ich wsparcie w trakcie ich utrzymywania.

B E Z P I E C Z N Y

Nie przedstawia istotnych ryzyk operacyjnych, finansowych i informatycznych. Należy tutaj oczywiście przypomnieć o kwestiach interpretacji przepisów wynikających z ustawy Prawo Bankowe, ustawy o Ochronie danych osobowych oraz relacjach z regulatorem (KNF). Decyzje co do działań w tym zakresie są całkowicie po stronie każdego z banków.

O P Ł A C A L N Y

Interesujący finansowo dla Banku. Ze względu na charakter publikacji szczegółowe informacje finansowe (w szczególności obecne koszty utrzymania systemów archiwalnych w Banku) nie są publikowane.

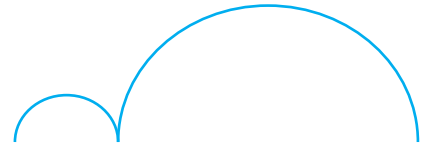
ROZDZIAŁ 2

DEFINICJA CHMURY OBLICZE - NIOWEJ

Światowa organizacja NIST (National Institute of Standards and Technology) w publikacji 800-145 tak definiuje model przetwarzania w chmurze:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>



Wikipedia z kolei definiuje chmurę obliczeniową (ang. cloud computing) jako: „model przetwarzania danych oparty na użytkowaniu usług dostarczonych przez usługodawcę (wewnętrzny dział lub zewnętrzna organizacja). Funkcjonalność jest tu rozumiana jako usługa (dająca wartość dodaną użytkownikowi) oferowana przez dane oprogramowanie (oraz konieczną infrastrukturę). [...] Konsument płaci za użytkowanie określonej usługi, np. za możliwość korzystania z arkusza kalkulacyjnego. Nie musi dokonywać zakupu sprzętu ani oprogramowania.”

Dla celów naszego dokumentu definiujemy chmurę jako rozproszone przetwarzanie funkcjonalności biznesowych i zarządzanie usługami IT, bez troszczenia się o lokalizację fizycznych urządzeń. Chmura publiczna oznaczać będzie, iż zasoby są całkowicie poza Bankowym Centrum Przetwarzania, u dostawcy usługi. Chmura prywatna oznaczać będzie, iż zasoby są rozlokowane w ramach wewnętrznych środowisk IT Banku, a ich dostawcą jest nie firma zewnętrzna, a wewnętrzne działy IT Banku. Chmura hybrydowa, najczęściej spotykana obecnie opcja architektoniczna, oznacza, iż część zasobów jest przetwarzanych w ramach chmury publicznej (u jednego lub kilku dostawców), część przetwarzana jest w ramach wewnętrznych zasobów Banku (chmura prywatna lub tradycyjne niezvirtualizowane zasoby informatyczne) a całość jest zarządzana w jeden spójny sposób. Mimo zbieżności nazw, nie wolno stawiać w zakresie funkcjonalnym znaku równości między chmurą publiczną a chmurą prywatną. Jakkolwiek oba modele mają te same cechy przetwarzania chmurowego, to zakres

oferowanych funkcji dla konsumenta chmury jest znacząco różny.

Przetwarzanie w chmurze w dobie cyfrowej gospodarki jest drogą do innowacyjności i większej elastyczności biznesu. Biznes ten jest coraz mocniej osadzony w technologii, przy jednoczesnej optymalizacji kosztowej (w szczególności inwestycyjnej). Co więcej, chmura potrafi znakomicie skrócić tzw. „time to market” dla projektów, dostarczając usługi wyższego rzędu, tj. Platform-as-a-Services czy Software-as-a-Service. Pośrednio, wykorzystanie tego typu usług może być też odpowiedzią na coraz większy brak rąk do pracy w branży IT (szacuje się, że w Polsce brakuje od 10 000 do 50 000 osób w szeroko rozumianej branży IT).

Kluczowe jest zrozumienie, iż przetwarzanie danych wyszło i wychodzić będzie coraz bardziej z serwerowni Banku. Najpierw Internet (a wraz z nim bankowość internetowa), następnie urządzenia mobilne (i bankowość mobilna) skutecznie te granice IT przesuwają – powodując, iż zbieranie, przetwarzanie, analizowanie danych dzieje się częściowo poza Data Center banku tak czy inaczej. Jest rozproszone i będzie rozproszone coraz bardziej, jeśli uwzględnimy technologie typu „Blockchain”.

Technologie informatyczne (infrastruktura) oraz aplikacje biznesowe czy pojedyncze usługi funkcjonalne mogą być dostarczane na żądanie, tam, gdzie Bank danej funkcjonalności potrzebuje, tyle ile jej potrzebuje, wtedy, kiedy jej potrzebuje i przy zachowaniu określonego SLA, które jest potrzebne – a wszystko w modelu pay-as-you-go (ang).

ROZDZIAŁ 3

WYZWANIA
USŁUG
CHMUROWYCH
NA RYNKU
BANKOWYM
W POLSCE

Rozwiązania chmurowe, ze względu na model cenowy, swoją elastyczność i łatwość w zarządzaniu i powoływaniu, znajdują zastosowanie w wielu obszarach biznesowych.

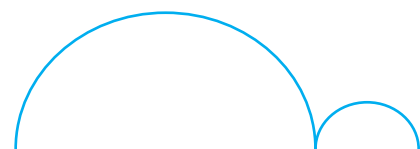
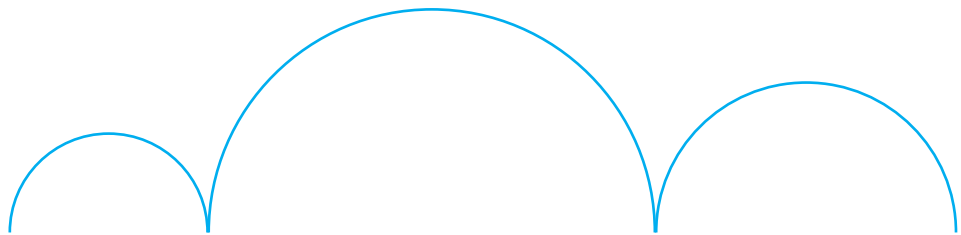
Mimo to, wciąż możemy znaleźć dziedziny gospodarki, w których rozwiązania chmurowe, zwłaszcza w Polsce, nie są jeszcze tak popularne jak w krajach Europy Zachodniej czy w Stanach Zjednoczonych. Należy do nich między innymi sektor bankowy i ubezpieczeniowy.

Przetwarzanie w chmurze stanowi ten obszar informatyki, któremu banki przyglądają się coraz dokładniej. Już w 2011 Związek Banków Polskich (ZBP) opublikował dokument odnoszący się do uwarunkowań technologicznych i prawnych zastosowania chmury publicznej dla polskiego sektora bankowego. Właściwie każda instytucja bankowa zdobyła już w tej kwestii własne doświadczenia dostrzegając potencjalne korzyści - zarówno finansowe jak i organizacyjne. Póki co, nie prowadzi to jednak do realizacji dużych, wkraczających w główną działalność biznesową i masowych projektów wykorzystują-

cych możliwości chmury publicznej. Przyczyny są oczywiście złożone – a największe wyzwania leżą po stronie interpretacji prawa i znalezieniu takiego scenariusza biznesowego, który będzie spełniał jednocześnie trzy ważne wymagania:

- 1.** Będzie prawnie akceptowalny;
- 2.** Zminimalizuje ryzyka systemowe;
- 3.** Zmaksymalizuje wartość biznesową dla banku.

Dostrzegając te potrzeby, ZBP powołał Forum Technologii Bankowych (FTB), którego zadaniem stało się m.in. promowanie i wprowadzanie takich nowoczesnych rozwiązań technologicznych w sektorze bankowym w Polsce. Grupa ta zrzesza liderów w swoich dziedzinach, którzy dzieląc się swym doświadczeniem i wiedzą mogą przyczynić się do dynamicznego rozwoju sektora bankowego.



ROZDZIAŁ 4

C E L
P R O J E K T U
T E Z E U S Z

W ramach działalności FTB został powołany projekt TEZEUSZ, który miał doprowadzić do odpowiedzi, czy projekt umieszczenia systemów archiwalnych banku w chmurze publicznej – w wariantcie najprostszym od strony prawnej/regulacyjnej i jednocześnie maksymalnie opłacalnym dla banku – może być skutecznie zrealizowany przez wybrany bank?

Celem projektu było:

1. Przygotowanie dokumentu ze wskazówkami najlepszych praktyk (best practices guidelines) dla scenariusza opisującego powyższy projekt. Model chmury publicznej został wybrany do celów projektowych intencjonalnie, gdyż generuje on najwięcej pytań odnośnie wykonalności takiego przedsięwzięcia, zarówno w aspekcie technicznym, jak i legislacyjnym. Cały projekt został oparty się o rzeczywiste dane banku Raiffeisen Polska (Bank), tak aby na tej podstawie mógł on przedstawić odpowiedni dokument do KNF.

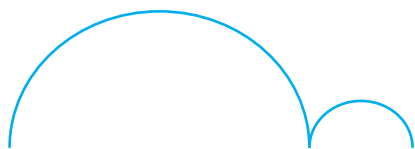
2. Analiza wykonalności technicznej projektu – na podstawie szczegółowych informacji technicznych o systemie archiwalnym, złożonym z kilkunastu maszyn (parametry serwerów, wymagania SLA, używane oprogramowanie itd.) zostały przedstawione bankowi dwie opcje rozwiązań chmurowych – Infrastructure-as-a-Service (IaaS) oraz Platform-as-a-Service (PaaS) w dwóch technologiach. Opis przeprowadzonej analizy został przedstawiony w rozdziale „Analiza dostępnych rozwiązań technicznych”. W wyniku analizy do kolejnego etapu prac wybrano rozwiązanie bazujące na modelu IaaS jako najprostszego w implementacji dla badanego przypadku użycia i wymagającego najmniejszej ilości zmian. Opis architektury został przedstawiony w rozdziale „Docelowa architektura rozwiązania”.

3. Analiza ryzyk projektowych (prawne, bezpieczeństwa danych, bezpieczeństwa połączeń, wyjście poza okres wsparcia, operacyjne: w trak-

cie migracji do chmury, na okres wykorzystywania zasobów udostępnianych wyłącznie w chmurze publicznej oraz w trakcie powrotu do rozwiązania lokalnego). Opis zidentyfikowanych ryzyk został przedstawiony w rozdziale „Ryzyka i wyzwania”.

4. Wycena kosztów – na podstawie omówionych z Bankiem wymagań odnośnie architektury IT, bezpieczeństwa oraz istotnych kryteriów wyboru, zostały przedstawione szacunkowe koszty przechowywania systemów archiwalnych w chmurze publicznej (tj. koszty mocy obliczeniowej, oprogramowania, wsparcia, wprowadzania zmian, warunków płatności itd.). Wycena bazowała na ogólnie dostępnych danych poszczególnych dostawców usług i została przekazana do Banku.

Dotychczas zebrane wnioski oraz żywe dyskusje, zarówno w ramach grupy projektu TEZEUSZ jak i poza nią, utwierdzają nas w przekonaniu, iż wykorzystanie chmury obliczeniowej może być atrakcyjną alternatywą dla systemów uruchamianych w ramach własnych Centrów Przetwarzania banków. Jaką formę przyjmie ostateczna architektura rozwiązania dla innych przypadków użycia, jest uzależniona zarówno od czynników legislacyjnych, jak i technicznych, co powinno być przeanalizowane dla każdego z nich z osobna. Mamy jednak nadzieję, że wspólnie z pomocą ZBP i FTB oraz we współpracy KNF z bankami – zostanie opracowane rozwiązanie wykorzystania chmury publicznej dla sektora finansowego, które będzie bardziej elastyczną alternatywą dla technologii aktualnie wykorzy-



ROZDZIAŁ 5

WYMAGANIA I ZAŁOŻENIA

W trakcie realizacji prac zostały zebrane wymagania, jakie powinny zostać spełnione przez docelową architekturę. Wymagania te zostały przedstawione przez przedstawicieli Banku. Zostały one opisane poniżej, gdyż w istotny sposób determinują kształt opracowywanego rozwiązania, a dodatkowo mogą być istotne dla analogicznych projektów związanych z wykorzystaniem chmury publicznej.

W1. Docelowe rozwiązanie powinno umożliwiać obsługę systemów i danych archiwalnych przez okres kilkunastu lat.

W2. Rozwiązanie powinno zapewniać trwałe usunięcie danych po wygaśnięciu danego archiwum.

W3. Docelowe rozwiązanie powinno zapewniać integralność danych.

W4. Rozwiązanie powinno zapewniać skalowalność (w górę i w dół) zarówno istniejących środowisk, jak i możliwość uruchamiania kolejnych systemów archiwalnych.

W5. Rozwiązanie powinno adresować wyzwania związane z zarządzaniem cyklem życia systemu w całym okresie świadczenia usługi, łącznie z rozwiązaniem problemu uaktualniania systemów operacyjnych i aplikacji.

W6. Zaproponowane rozwiązanie powinno umożliwiać przenoszenie systemów między różnymi usługodawcami w chmurze publicznej.

W7. Uruchomienie systemów archiwalnych powinno być możliwe w dwóch separowanych ośrodkach w ramach jednego dostawcy chmury publicznej.

W8. Dane powinny być przechowywane w Data Center położonych na terenie Unii Europejskiej, w ramach Europejskiego Obszaru Gospodarczego

W9. Rozwiązanie powinno być zgodne z zalecaniami KNF (w tym z zaleceniem dotyczącym outsourcingu oraz Rekomendacją D).

W10. Komunikacja sieciowa pomiędzy Bankiem, a infrastrukturą dostawcy powinna być zabezpieczona kryptograficznie.

W11. Dane przechowywane w systemach pamięci masowych dostawcy usługi muszą być zabezpieczone kryptograficznie i dodatkowo, w uzasadnionych przypadkach powinny zostać zastosowane mechanizmy zapewniające ich integralność.

W12. Powinien być zapewniony odpowiedni poziom separacji danych. Separacja fizyczna – tam gdzie jest to możliwe. Separacja logiczna – w przypadku, gdy dostawca usługi chmurowej nie jest w stanie zapewnić dedykowanej infrastruktury sprzętowej.

W13. Dostawca rozwiązania powinien być odpowiedzialny za proces zarządzania usługami

dostarczonymi Bankowi.

W14. Zasoby użytkowane przez Bank powinny być zabezpieczone poprzez odpowiednie mechanizmy bezpieczeństwa – kontrola i monitoring dostępu fizycznego osób do Data Center.

W15. Dostawca usługi jest zobowiązany do zapewnienia ciągłości działania usługi na poziomie określonym w stosownej umowie SLA.

W16. Dostawca usługi chmurowej jest zobowiązany aktywować usługi ochrony przed wszelkimi atakami oraz raportować do Banku wszystkie incydenty bezpieczeństwa.

W17. Aktualne metody uwierzytelniania powinny być przeniesione do rozwiązania proponowanego przez dostawcę rozwiązania o ile istnieje techniczna możliwość

W18. Dopuszczalna jest możliwość przeniesienia obecnie działających aplikacji na inne systemy operacyjne czy też serwery bazodanowe, o ile obniży to całkowity koszt utrzymania systemów i nie wpłynie na integralność danych.

Zespół projektowy przyjął poniższe założenia w czasie badania możliwości przeniesienia systemu do chmury oraz oszacowania kosztów utrzymania takiego systemu. Wszystkie poniższe założenia zostały przedstawione w ramach spotkań z innymi uczestnikami i zostały wypracowane na bazie informacji o systemie opisanym przez Bank.

Z1. Architektura rozwiązania w chmurze

Na początku projektu przyjęto założenie, że nowa architektura rozwiązania ma wykorzystywać rozwiązania wyłącznie chmury publicznej. Stąd też nie rozważano rozwiązań chmury prywatnej, hybrydowych, czy rozwiązania pomie-

dzy różnymi dostawcami chmury publicznej, uznając je za nazbyt skomplikowane.

Co więcej, przyjęto, że jeśli jakaś usługa (np. backup) jest oferowana w chmurze w modelu PaaS (Platform as a Service), to należy jej użyć przed rozwiązaniami opartymi o maszyny wirtualne IaaS (Infrastructure as a Service).

Z2. Na potrzeby projektu oraz w celu uproszczenia analizy przyjęto, że systemy Banku oparte o architekturę inną niż x86 i system operacyjny inny niż Linux zostaną zmigrowane i ujednolicone do wspólnej architektury x86/Linux.

Dodatkowo, nie analizowano migracji do chmury rozwiązań towarzyszących, które w chmurze nie są potrzebne, takich jak wirtualizator dla maszyn, system do zarządzania wirtualizacją. Funkcjonalność ta jest dostarczana w ramach usługi w chmurze publicznej.

Z3. Dostępność i wydajność systemu

Rozważany system jest systemem archiwalnym, który służy tylko do odczytu danych przez ściśle ograniczoną grupę osób w Banku (poniżej 15). W systemie tym nie są prowadzone już zmiany, a wykorzystywany jest tylko w trakcie pracy oddziałów Banku lub na prośbę audytorów lub kontrolerów. Założono więc, że system w chmurze będzie pracował 5 dni w tygodniu, w godzinach 8.00 – 18.00, ew. będzie włączany poza godzinami pracy, jeśli będzie taka konieczność. System naliczania opłat w chmurach ma minutową dokładność, a koszty są naliczane

tylko za ten czas, kiedy maszyna wirtualna jest uruchomiona. Stąd też zaplanowanie dostępności instancji w ramach rozwiązania ma bardzo istotne znaczenie dla TCO.

Z4. Licencje na oprogramowanie

Licencje na systemy operacyjne, systemy baz danych, aplikacje oraz narzędzia monitoringowe, zostaną zakupione w ramach usługi dostarczenia zasobów chmury publicznej. Licencje na aplikacje bankowe czy inne oprogramowanie, niezbędne do uruchomienia rozwiązań, zostaną dostarczone przez Bank.

Z5. Procedury utrzymaniowe docelowego rozwiązania po migracji rozwiązania do chmury Ustalono, że ze względu na zmianę architektury rozwiązania, po migracji do chmury procedury operacyjne zostaną zaktualizowane przez Bank oraz dostawcę, tak by uwzględniać inną specyfikę procesu wykonywania kopii zapasowej czy monitorowania systemu.

Z6. Lokalizacja i przyjęte ceny

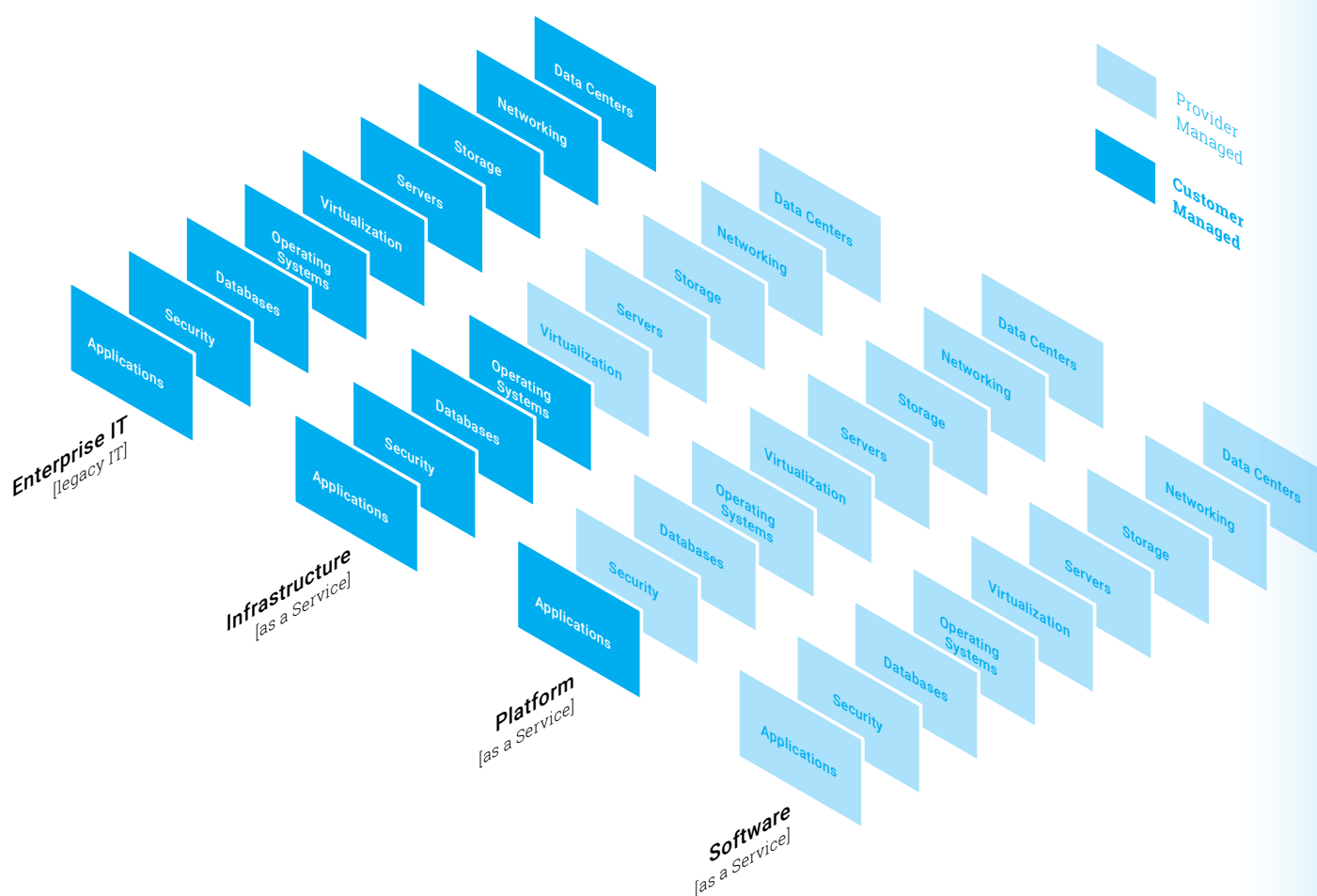
W trakcie prac projektowych uzgodniono, że dostarczanie usługi będzie odbywało się w Centrach Danych, zlokalizowanych w Europie a koszty będą policzone względem publicznie dostępnych cenników w EUR, bez uwzględniania jakichkolwiek zniżek, które mogą wynikać z ilości zaalokowanych zasobów, dodatkowych umów, itp. współpracy Banku oraz dostawców usług.

ROZDZIAŁ 6

ARCHITEK- TURA ROZWIĄ- ZANIA

W niniejszym rozdziale przedstawiono kroki, jakie podjęto w celu wyboru docelowego rozwiązania wyłącznie dla badanego przypadku użycia.

Analiza dotyczyła wyłącznie systemu o cechach opisanych wyżej. Oznacza to, że rozwiązanie opisane jako docelowe nie musi być rozwiązaniem optymalnym dla analogicznych środowisk w innych Bankach. Dlatego ważne jest, aby każdy inny przypadek użycia był przeanalizowany osobno i aby dla każdego z nich powstała dedykowana architektura rozwiązania w chmurze. Środowiska chmur publicznych rządzą się nieco innymi prawami i dostarczają wiele gotowych usług „z pudełka”.



Opis środowiska podlegającego migracji

W pierwszej kolejności zbadano cechy i opisano rodzaj środowiska, jakie wytypowano do przeniesienia do chmury publicznej. W projektach migracyjnych opis taki jest szczególnie istotny ze względu na fakt, iż aplikacje, dane oraz wykorzystywane procesy będą przystosowane lub zoptymalizowane do działania w ramach infrastruktury lokalnej. Skrócony opis został przedstawiony poniżej:

Rodzaj systemu podlegającego migracji.

Migracji podlega środowisko zbudowane z kilkunastu aplikacji działających pod kontrolą syste-

mu operacyjnego Windows/Linux. Dane przetwarzane przez aplikacje są przechowywane w bazach SQL oraz ORACLE. Dostęp do danych jest realizowany w trybie odczytu (generowanie raportów, wyszukiwanie danych, itp.) z wykorzystaniem modułów warstwy aplikacyjnej. Dane nie są modyfikowane lub uzupełniane. Środowisko jest traktowane jako archiwum i nie służy do realizacji głównych procesów biznesowych Banku. Dostęp do danych jest utrzymywany wyłącznie ze względu na wymagania legislacyjne. Ze względu na charakter danych (archiwum), środowisko musi być utrzymywane przez okres kilkunastu lat.

Cechy środowiska

- a) Typ aplikacji: są to własne aplikacje o charakterze monolitycznym, przystosowane do działania wyłącznie na wspieranym przez nie systemie operacyjnym. Nie posiadają one cech typowych aplikacji opartych np. o architekturę mikroserwisów, które w prosty sposób mogą być migrowane do chmury pracującej w modelu PaaS. Aplikacje wykorzystywane w migrowanym systemie działają w architekturze 3-warstwowej: DB + APP + Web/Desktop Access
- b) Rodzaj infrastruktury: środowisko jest w pełni zwirtualizowane. Jako hypervisor zastosowano rozwiązanie VMware dla serwerów x86-64 oraz PowerVM dla serwerów Power. W ramach środowiska uruchomiony jest podsystem kopii zapasowych, kontroli dostępu i bezpieczeństwa oraz monitoringu całego środowiska.
- c) Powiązania: opisywane systemy archiwalne są odseparowane od pozostałych systemów bankowych. Dostęp do aplikacji i danych systemu jest realizowany wyłącznie przez ściśle kontrolowaną grupę pracowników Banku.

Analiza dostępnych rozwiązań technicznych

W drugim etapie przeanalizowano modele uruchomienia usługi chmury publicznej dla środowiska opisanego w poprzednim punkcie.

Poniższy diagram pokazuje różne modele dostarczania usług chmurowych porównując jednocześnie zakres odpowiedzialności klienta końcowego jak i dostawcy chmurowego. Warto zauważyć, że modele bliższe lewej stronie dają największą możliwość dostosowania rozwiązania, ale wymagają największej inwestycji w zadania operacyjne. Im bardziej na prawo,

tym mniej mamy możliwości dostosowania rozwiązania do własnych potrzeb na warstwie infrastruktury aplikacji natomiast, zarządzanie rozwiązaniem jest w 100% w rękach operatora chmury. Ze względu na specyfikę aplikacji i danych podlegających migracji rozważano wyłącznie rozwiązania oparte na modelu Infrastructure as a Service (IaaS) oraz Platform as a Service (PaaS). Model Software as a Service (SaaS) został wyeliminowany ze względu na wysoce zindywidualizowany charakter aplikacji wykorzystywanych przez Bank.

Model IaaS

Model IaaS udostępniania zasobów chmury publicznej wydaje się najprostszym rozwiązaniem dla analizowanego systemu podlegającego migracji, ze względu na możliwość definicji własnych maszyn wirtualnych u dostawcy usługi i pełną kontrolę Banku nad środowiskiem pracy dla migrowanych aplikacji, począwszy od wersji zastosowanego systemu operacyjnego, przez jego konfigurację aż po proces instalacji aplikacji i ich konfiguracji. Dodatkowo, biorąc pod uwagę fakt, iż aktualnie wykorzystywane środowisko jest w pełni zwirtualizowane, istnieje małe ryzyko niepowodzenia podczas realizacji procesu migracji. Funkcjonalność infrastruktury dostarczanej w modelu IaaS (przydział zasobów CPU/RAM/Storage oraz mechanizmy kontroli dostępu, monitoringu, backupu oraz bezpieczeństwa połączeń w sieci VPN) pozwala w łatwy sposób odtworzyć funkcjonalności aktualnie wykorzystywanego środowiska.

Przy wykorzystaniu tego modelu usług w chmurze publicznej wyzwaniem jest zapewnienie

separacji środowiska wykorzystywanego przez Bank od środowisk innych użytkowników chmury publicznej na poziomie węzłów obliczeniowych (computing nodes) oraz wykorzystywanych zasobów dyskowych (storage resources). Jednym z rozwiązań tego problemu jest rozdzielenie zasobów obliczeniowych (węzłów, dysków) pomiędzy poszczególnymi środowiskami i/lub zabezpieczenie kryptograficzne danych, np. na poziomie systemów plików, ograniczenie dostępu poprzez modele uprawnień, ograniczenie ruchu sieciowego pomiędzy komponentami środowiska.

Model PaaS

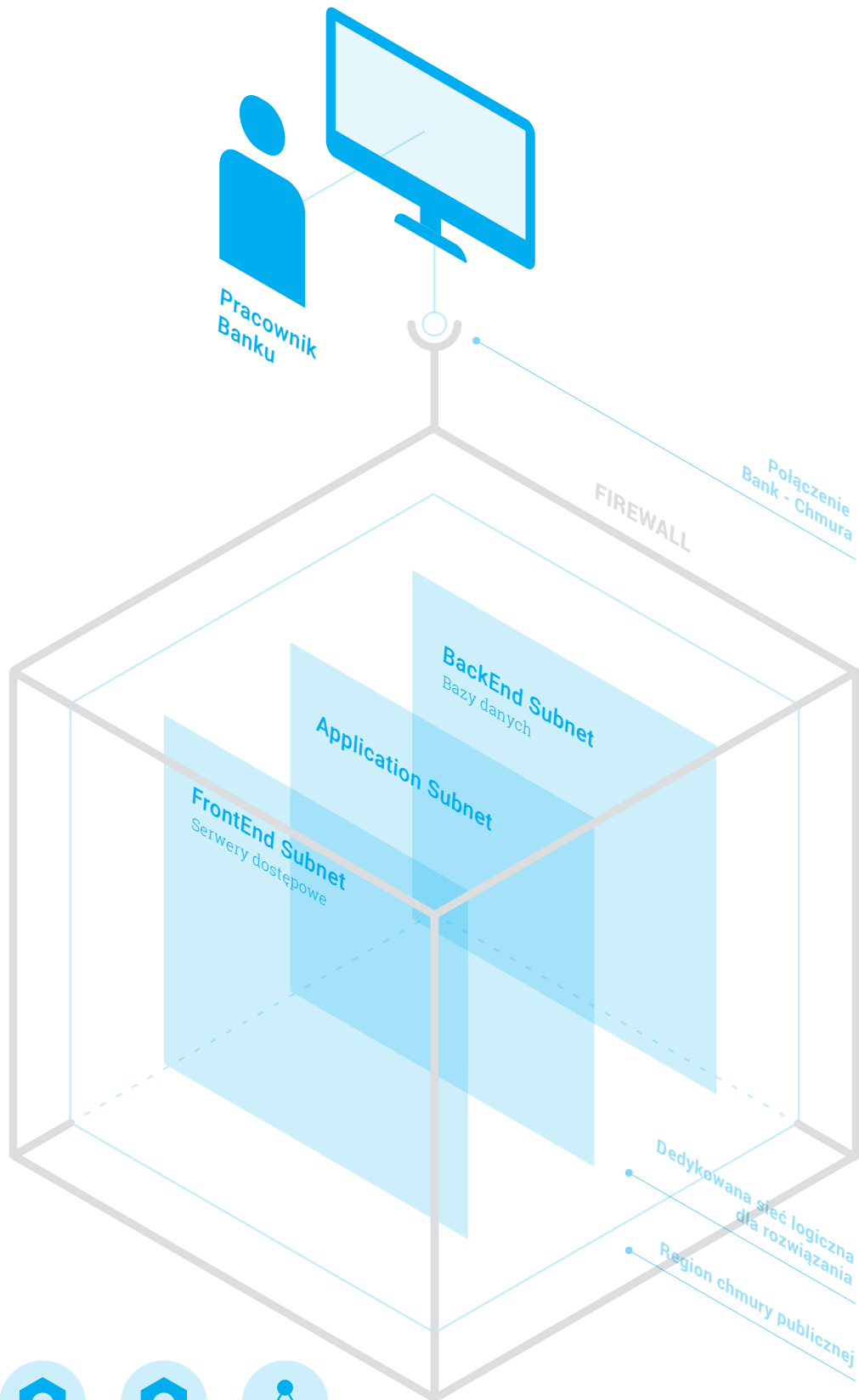
Jako alternatywę, podczas prac Zespołu projektowego, rozważano zastosowanie modelu Platform-as-a-Service (PaaS). W modelu tym migracji podlegałyby dane archiwalne do chmury publicznej, a na tej warstwie zostałyby zbudowane raporty, które prezentowałyby dane potrzebne zarówno pracownikom Banku do działalności bieżącej jak i ew. kontrolerom. W tym celu rozważano wykorzystanie zasobów składowania danych udostępnianych w modelu PaaS. Rozwiązanie to w przypadku analizowanych aplikacji wymagałoby znacznych nakładów pracy (np. przy konwersji danych z aktualnie wykorzystywanych baz) czy implementacji lub modyfikacji modułów wyszukiwania danych albo generowania wymaganych raportów, aby odwzorować pełną funkcjonalność obecnego systemu. Rozwiązanie to jest atrakcyjne dla systemów, jakie projektowane są z myślą o wykorzystaniu zasobów chmury publicznej lub tych, które wykorzystują zasoby w łatwy sposób

migrowalne do modelu PaaS, np. wykorzystując zasoby składowania danych typu object storage lub wykorzystując architekturę mikroserwisów. Co więcej, zastosowanie takiego rozwiązania jest możliwe, jeśli nadal w organizacji posiadamy zasoby głęboko znające architekturę aplikacji oraz strukturę danych. Niewątpliwą zaletą tego typu rozwiązań (PaaS) jest uniezależnienie się od wersji aktualnie zastosowanego oprogramowania w warstwie bazodanowej, aplikacyjnej, czy choćby wersji zastosowanego systemu operacyjnego, gdyż komponenty te nie muszą być zarządzane bezpośrednio przez Bank, ale są dostarczane przez dostawcę usługi chmury publicznej. Co więcej, model PaaS jest z reguły bardziej ekonomiczny, gdyż zmniejsza do minimum czynności operacyjne.

Docelowa architektura rozwiązania

Docelowe rozwiązanie zostało wybrane na podstawie charakterystyki migrowanego środowiska do chmury publicznej. Jest ono oparte na modelu IaaS, ale wyłącznie dla omawianego przypadku użycia. Dla innych systemów, jakie mogłyby być przeniesione do chmury publicznej, rozwiązanie oparte na modelu PaaS może okazać się bardziej atrakcyjne, zarówno pod względem łatwości implementacji i utrzymania systemu, jak i pod względem obniżenia kosztów.

W ramach przeprowadzonych prac udało się zaproponować potencjalną, techniczną architekturę rozwiązania w chmurze IaaS. Architektura ta skupia się na umieszczeniu aplikacji w ramach komponentów chmurowych, nie przedstawia precyzyjnie architektury samej aplikacji, która została w niej osadzona i może być trakto-



Monitoring rozwiązań



Backup rozwiązań



Modele uprawnień do zasobów chmury oraz rozwiązania oparte o usługę katalogową chmury

wana jako przykładowa, dla innych rozwiązań tego typu.

Architektura została zbudowana z wykorzystaniem komponentów wymienionych poniżej. Szczegóły implementacyjne (nazwy produktów, cechy rozwiązań), różnią się w zależności od dostawców usługi IaaS chmury publicznej. Opis tych cech w podziale na rozwiązania firm: Microsoft, IBM, Atende zostały opisane szczegółowo w załącznikach na końcu dokumentu.

Architektura ta zakładała m.in. takie elementy, jak zilustrowane na powyższym rysunku.

a) Komplet rozwiązań Firewall – jeden po stronie sieci Banku, drugi po stronie sieci rozwiązania, osadzonego w chmurze.

b) Połączenie typu Site2Site VPN, a więc tunel VPN zestawiany pomiędzy urządzeniami sieciowymi Banku a chmurą, w celu zabezpieczenia warstwy transportu dla komunikacji Bank – Chmura IaaS.

c) Dedykowaną sieć na poziomie logicznym (VLAN VNET), podzieloną na różne części (Subnet), w ramach których są umieszczone poszczególne warstwy rozwiązania. Podział taki umożliwia granularną kontrolę ruchu (ACL, Network Security Group) na poziomie portów, protokołów oraz kierunków ruchu pomiędzy warstwami aplikacji. Dedykowana sieć zapewnia również separację logiczną od rozwiązań innych użytkowników w ramach Centrum Danych oraz daje możliwość wpuszczenia ruchu tylko z wewnątrz przedsiębiorstwa.

d) Rozwiązania towarzyszące, takie jak:

- i. System zbierania, analizy logów i rekomendacji dla środowiska;
- ii. System archiwizacji i składowania kopii

bezpieczeństwa;

iii. Zarządzanie tożsamością i dostępem do obszarów rozwiązania wraz z raportami prezentującymi dostęp do zasobów.

Wszystkie te rozwiązania, wykorzystane razem podnoszą bezpieczeństwo i ograniczają obszar ataków na aplikację umieszczoną w chmurze, a wykorzystywaną tylko przez pracowników wewnątrz Banku.

Wykorzystane rozwiązania

Technologie wykorzystane w aplikacji nie są już rozwijane czy też wspierane, a okres wsparcia dla wszystkich tych technologii dobiegł końca. W rozwiązaniu wykorzystywane są m.in. takie technologie jak:

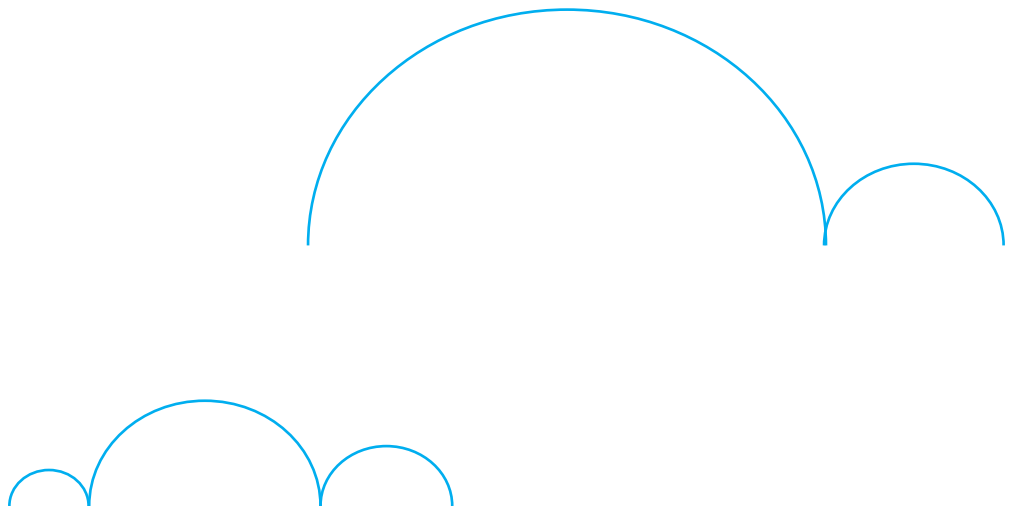
1. System operacyjny: Windows Server 2003 Standard Edition, Windows Server 2008 R2 Standard Edition
2. Serwer aplikacyjny: Oracle Application Server v10.1 oraz 9i ze środowiskiem Java 1.4
3. Serwer baz danych: Oracle 10.2 Standard Edition, Microsoft SQL Server 2005 Enterprise Edition

Wykorzystywanie technologii, które osiągnęły etap END OF LIFE w każdej chmurze obłożone jest nieco innymi restrykcjami i obwarowaniami.

Na ten moment każdy duży dostawca chmury publicznej zezwala na uruchamianie Windows Server 2003 pomimo braku wsparcia dla tej technologii od samego producenta. Pozostałe technologie, wymienione na liście, nie były przygotowywane z myślą o uruchamianiu ich w chmurze, natomiast w ich opisie nie ma

wymienionych specyficznych elementów, które nie pozwalałyby na wykorzystanie ich w chmurze (np. wykorzystanie wspólnego dysku dla dwóch maszyn wirtualnych jak w przypadku niektórych technologii klastrowych). W ramach prowadzonych prac, nie przeprowadzono prac typu „Proof Of Concept” by zweryfikować techniczną możliwość uruchomienia środowiska, gdyż wiązałoby się to z wykonaniem faktycznej

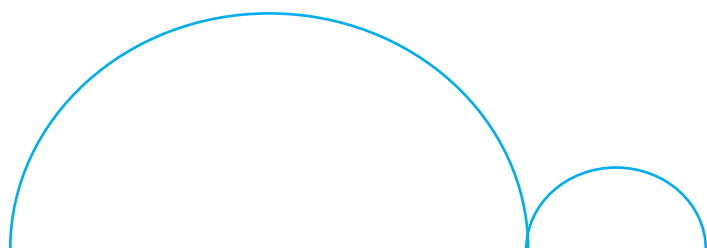
migracji do chmury. Po analizie aktualnego obciążenia systemu okazało się, że system jest w bardzo niewielkim stopniu wykorzystywany i jego parametry techniczne (takie jak ilość wirtualnych rdzeni procesora, pamięć czy wydajność podsystemu dyskowego) mogą być znacznie zmniejszone w celu optymalizacji kosztów rozwiązania po przeniesieniu do środowiska chmury publicznej.



ROZDZIAŁ 7

R Y Z Y K A
I W Y Z W A N I A

Każda migracja rozwiązania z aktualnego środowiska obarczona jest ryzykiem i wyzwaniami, które mogą się objawić dopiero na etapie migracji i implementacji. W przypadku jednak rozwiązania chmury publicznej dla rozwiązania Bankowego, zawierającego dane klientów, ważniejsze wydają się być ryzyka związane z aspektami prawnymi niż aspektami technicznymi.



Poniższa tabela wymienia najważniejsze grupy ryzyk, które można zmitygować jeszcze przed rozpoczęciem całego projektu.

Grupa ryzyka	Ryzyko w obecnym środowisku	Ryzyko w chmurze publicznej
Bezpieczeństwo połączeń i danych	W obecnym środowisku wszystkie jego komponenty znajdują się w Centrum Danych klienta. W trakcie projektu nie dyskutowano o poziomie zabezpieczeń tego środowiska ani w warstwie oprogramowania, ani sprzętu.	Połączenia do środowiska, dostępnego w ramach chmury, realizowane jest przez Internet z sieci Bankowej w ramach tunelu typu VPN: Site 2 Site VPN, zabezpieczonego rozwiązaniem IP SEC.
Wyjście poza okres wsparcia wykorzystywanego oprogramowania (OS, Baza danych, Serwer, Aplikacja)	Aktualnie używane oprogramowanie nie jest już wspierane przez producenta. Ze względu na fakt, że systemy są archiwalne, nie są aktualizowane ani migrowane do wyższych wersji produktów. Fizyczne urządzenia, które są używane również mogą wyjść poza fazę wsparcia / lub już wyszły. W przypadku urządzeń fizycznych istnieje ryzyko, że sprzęt, niezbędny do utrzymania środowiska, nie będzie już dostępny.	Aktualnie używane oprogramowanie nie jest już wspierane. Ze względu na fakt, że systemy są archiwalne, nie są aktualizowane ani migrowane do wyższych wersji produktów i nie planuje się takich operacji w przyszłości. Istnieje ryzyko, że tak stare wersje systemów nie będą w przyszłości wspierane na warstwie wirtualizacji w chmurze publicznej.

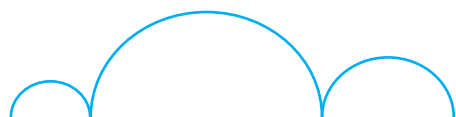
Mitygacja ryzyk

Dostępny jest cały szereg zabezpieczeń w zakresie zestawianych połączeń do środowiska w chmurze. Zakładamy, że połączenia nie są dostępne cały czas. Maszyny wirtualne nie mają publicznych adresów IP, nie mają dostępu do sieci Internet, do samych maszyn nie można dostać się z sieci Internet. Maszyny mają ściśle określony zestaw adresów do połączeń. Użytkownicy łączą się poprzez publiczne adresy bramek oraz rozwiązania równoważenia ruchu.

Połączenia są zabezpieczone poprzez wybrane rozwiązania typu firewall. Dostępne sieci są sieciami prywatnymi, niedostępnymi z zewnątrz. Alternatywnym rozwiązaniem może być połączenie fizyczne, dedykowane, prywatne dla Państwa, o gwarantowanej przepustowości i gwarantowanym opóźnieniu. Dyski maszyn wirtualnych w chmurze są szyfrowane rozwiązaniem BitLocker dla Windows lub DM-Crypt dla systemu Linux.

Ryzyko niedostępności występuje w obu wariantach – zarówno w przypadku wersji aktualnie używanej, jak i w przypadku migracji do chmury. Jedną z metod radzenia sobie z takim problemem w przyszłości jest wykorzystanie mechanizmów podwójnej wirtualizacji, gdzie na

maszynach wirtualnych w chmurze instalowany jest najnowszy system operacyjny z możliwością dalszej wirtualizacji, a dopiero na takim środowisku uruchamiane są maszyny opisywanego środowiska.



Grupa ryzyka	Ryzyko w obecnym środowisku	Ryzyko w chmurze publicznej
Powrót z „chmury” do środowiska on-premise / wyjście z aktualnego rozwiązania	Aktualny dostawca może przestać świadczyć usługę lub usługa może nie być u niego dostępna. Środowiska fizyczne mogą nie być dostępne.	Dostawca chmury może przestać świadczyć usługę lub usługa może nie być już dostępna.
Ryzyka prawne wynikające z: <ul style="list-style-type: none"> • Ustawa Prawo bankowe – zapisy nt. outsourcingu bankowego. • Rekomendacja D – rekomendacje dot. usług chmurowych 	Dla usług realizowanych lokalnie (Polska) – wzajemne zobowiązania kontraktowe w ramach obowiązującego prawa.	Dostawca usług powinien przedstawić dokument opisujący szczegółowe warunki świadczenia usług chmury publicznej, ze szczególnym uwzględnieniem warunków świadczenia usług dla instytucji finansowych.
Ustawa o ochronie danych osobowych – rekomendacje dot. usług chmurowych	Dla usług realizowanych lokalnie (Polska) – wzajemne zobowiązania kontraktowe w ramach obowiązującego prawa.	Warunki ustawy spełnione przy zastosowaniu odpowiednich mechanizmów szyfrowania danych.
Ryzyko przestoju środowiska systemowego	Dla systemów archiwalnych, nie stanowiących istotnego elementu działalności operacyjnej banku – pomijalne	Dla systemów archiwalnych, nie stanowiących istotnego elementu działalności operacyjnej banku – pomijalne

Mitygacja ryzyk

Powrót z chmury do rozwiązania on-premise to scenariusz, który zawsze należy zakładać. Proces będzie polegał na przeniesieniu maszyn na środowiska wirtualne, ustaleniu adresacji,

przetestowaniu połączeń i działania aplikacji w nowym środowisku. Proces przeniesienia rozwiązania będzie wymagał zaplanowania niedostępności.

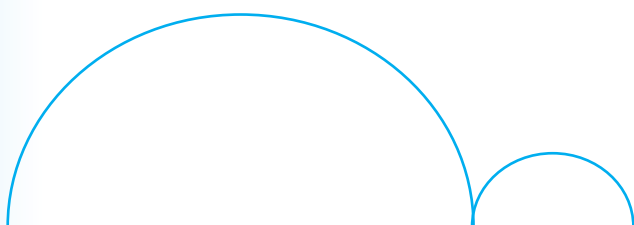
Ryzyka te mogą zostać zaadresowane w dokumencie do KNF, opisującym powyższe przedsięwzięcie. Wymagana opinia prawna od dostawcy usługi chmury publicznej opisująca warunki świadczenia usług, w szczególności odpowie-

dzialności wobec klientów banku, odniesienie do outsourcingu bankowego, podoutsourcingu, outsourcingu łańcuchowego, inspekcji w siedzibie podwykonawców itd.

Spełnienie wymagań opisanych w „Dekalogu chmuroluba”.

http://www.giodo.gov.pl/259/id_art/6271/j/pl

De facto zwiększenie dostępności systemów archiwalnych.



ROZDZIAŁ 8

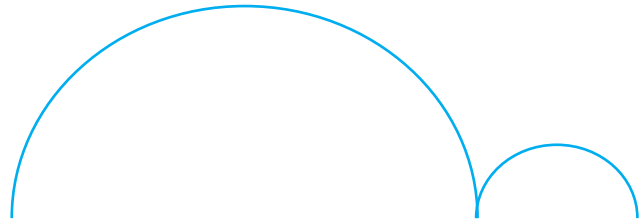
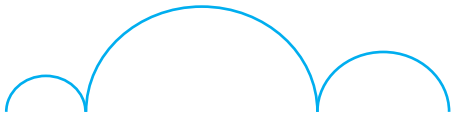
WNIOSKI

Chmura publiczna dla aplikacji monolitycznych – model IaaS

Dla aplikacji o charakterze monolitycznym, pierwotnie zaprojektowanych do pracy w tradycyjnej infrastrukturze IT w ramach DC banku, najprostszym sposobem przeniesienia ich do chmury publicznej jest wykorzystanie modelu IaaS, czyli modelu w którym wykorzystujemy maszyny wirtualne. Model ten umożliwia odwzorowanie pełnej funkcjonalności tradycyjnego środowiska pracy (szczególnie w przypadku, gdy środowisko IT wykorzystuje już mechanizmy wirtualizacyjne) bez – lub z minimalnymi zmianami związanymi z konfiguracją środowiska pracy aplikacji. Model ten pozwala na największą ingerencję w konfigurację środowiska aż do poziomu systemu operacyjnego, ale wymaga największego zaangażowania po stronie operacyjnej.

Chmura publiczna dla nowoczesnych aplikacji – model PaaS

Model PaaS jest alternatywą dla aplikacji projektowanych lub już uruchomionych z myślą o wykorzystaniu chmury obliczeniowej, niezależnie od tego, czy dotyczy to chmury prywatnej, czy chmury publicznej. Model PaaS jest najszybciej rozwijającym się obszarem chmury publicznej i pozwala osiągnąć najlepsze TCO oraz najkrótszy Time To Market. Przykładem takich aplikacji są te oparte na architekturze mikroserwisów, technologii kontenerów czy wreszcie serwery aplikacyjne, bazy danych i usługi dostępne w takim modelu. W takim przypadku, zarówno poszczególne komponenty aplikacji odpowiedzialne za obsługę konkretnych funkcji mogą być w łatwy sposób przenoszone do chmury publicznej uzniezależniając się od typu zastosowanego systemu operacyjnego. Rozwiązanie takie nie tylko umożliwia łatwą migrację aplikacji z DataCenter banku, ale umożliwia również prostą migrację aplikacji pomiędzy poszczególnymi dostawcami usług.



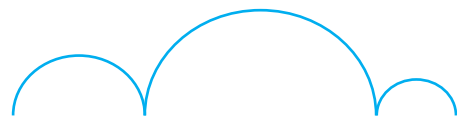
Przetwarzanie danych wrażliwych w chmurze publicznej

W dyskusjach głównym tematem w obszarze bezpieczeństwa przetwarzania danych wrażliwych były mechanizmy zabezpieczeń stosowanych przez usługodawcę chmury publicznej. We współdzielonych środowiskach IT (multi-tenancy) ma to szczególnie istotne znaczenie. Typowym rozwiązaniem tego problemu jest zastosowanie zaawansowanych mechanizmów kryptograficznych nie tylko do zabezpieczenia komunikacji z zasobami udostępnianymi w chmurze publicznej, ale również szyfrowania danych przetwarzanych na zasobach dyskowych udostępnianych przez usługodawcę. Mechanizmy kryptograficzne mogą być wdrażane zarówno na poziomie systemów operacyjnych (np. szyfrowane systemy plików), jak i na poziomie aplikacji (o ile mechanizmy takie są zaimplementowane). Alternatywą jest wykorzystanie dedykowanej infrastruktury w chmurze publicznej, która jest zaalokowana wyłącznie dla jednego usługobiorcy.

Dodatkowo ważne jest, aby upewnić się, czy dostawca usługi posiada certyfikaty lub wyniki audytów potwierdzające zgodność z wymogami bezpieczeństwa oferowanych usług, np.: SOC, ISO270001, ISO27018, czy PCI DSS.

Aspekt finansowy

Projekt ten jest interesujący finansowo dla Banku, jednak ze względu na charakter publikacji szczegółowe informacje finansowe (w szczególności obecne koszty utrzymania systemów archiwalnych w Banku) nie są publikowane.



ROZDZIAŁ 9

Z A Ł Ą C Z N I K I

ZAŁĄCZNIK 1

Atende: technologie wykorzystane w Architekturze docelowej.

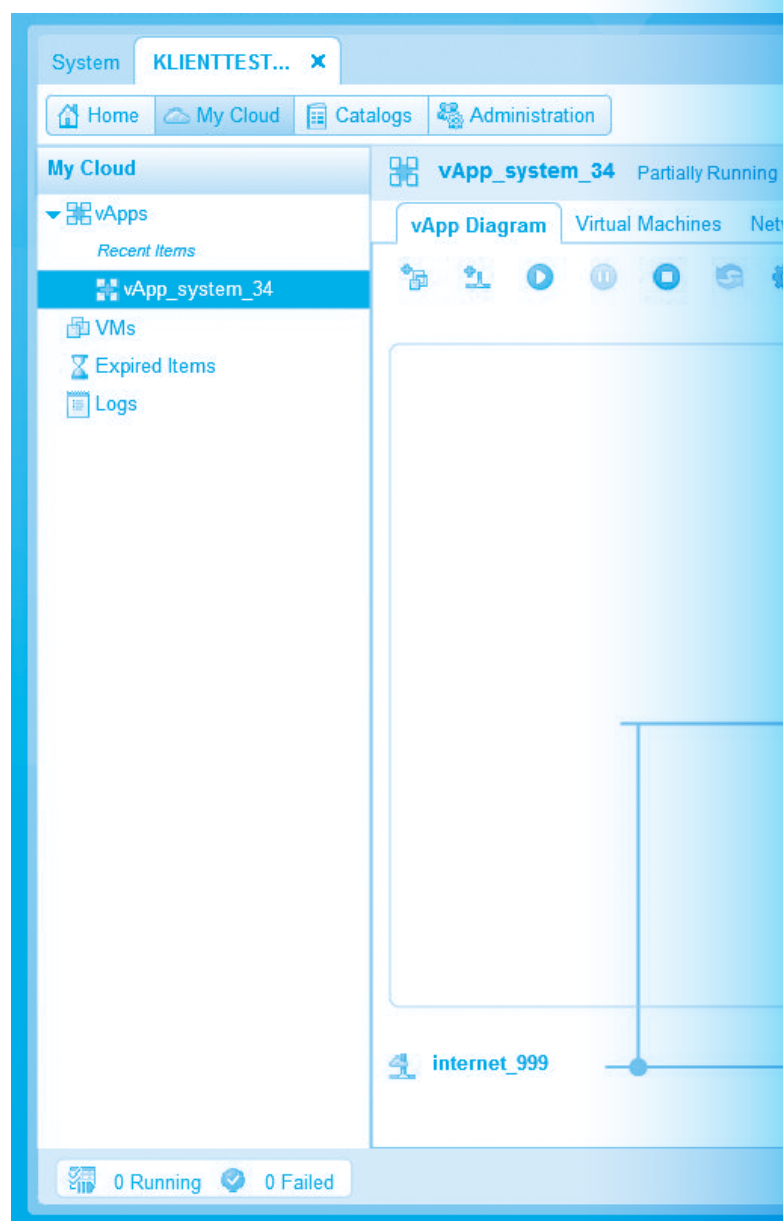
Atende S.A. oferuje usługi IaaS pod marką Atende Business Cloud. Uzupełnieniem świadczonych usług jest pakiet usług profesjonalnych, począwszy od projektowania i planowania rozwiązania, poprzez migrację, aż po utrzymanie, bieżące zarządzanie usługami i wsparcie Klientów w trybie 24x7x365.

Platforma

Środowisko Atende Business Cloud zbudowane jest w oparciu o najwyższej jakości rozwiązania dostępne na rynku cloud computing. Rozwiązanie działa w nowoczesnej serwerowni ATMAN w Warszawie. Środowisko zbudowane jest na sprzęcie i oprogramowaniu liderów rynkowych: VMware, HPE, HDS, EMC, Cisco, Fortinet.

Wirtualne Centrum Danych

Rysunek 1 Wirtualne Centrum Danych
W ramach usług Atende business Cloud, budowane są wirtualne centra danych, dostarczające

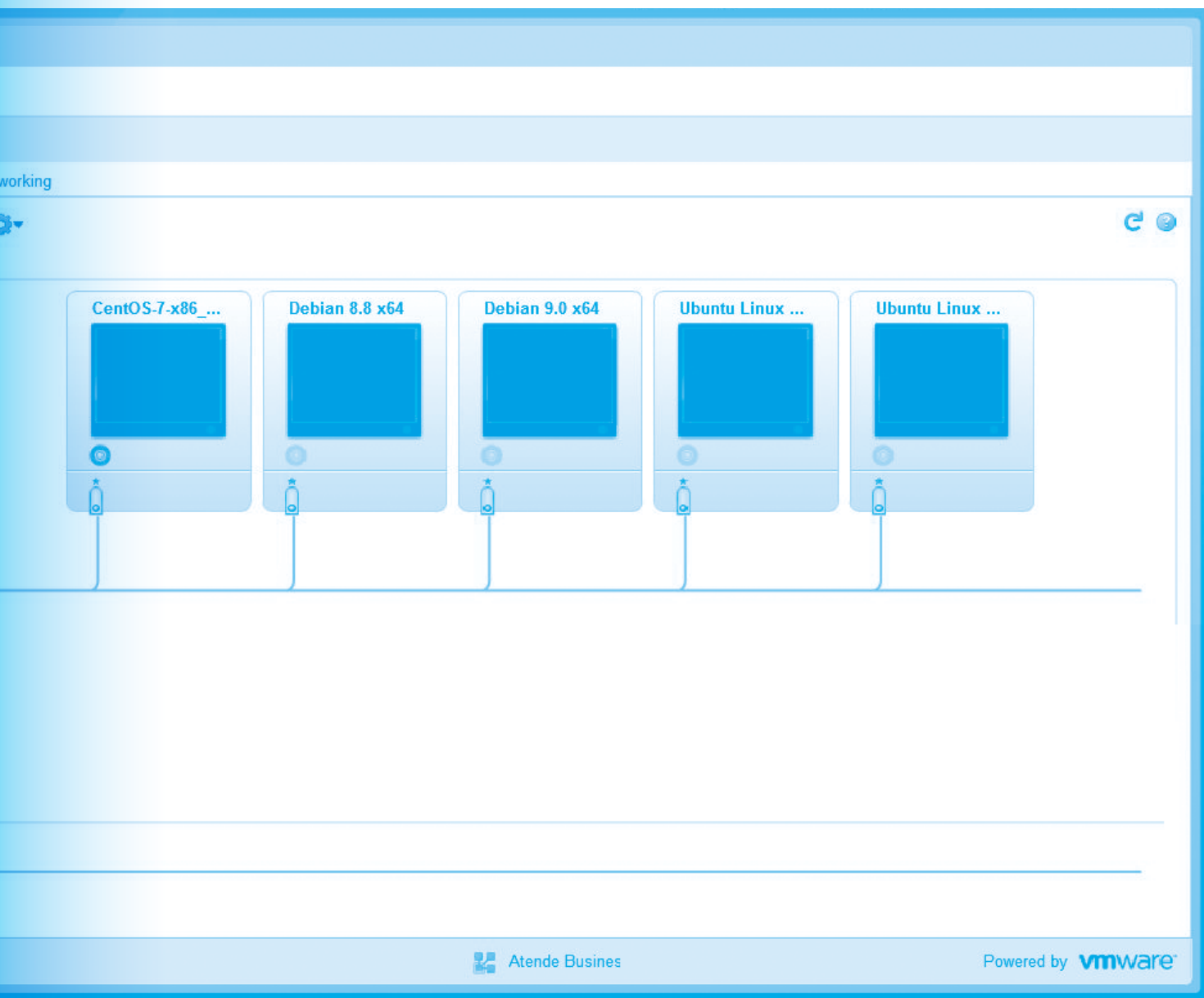


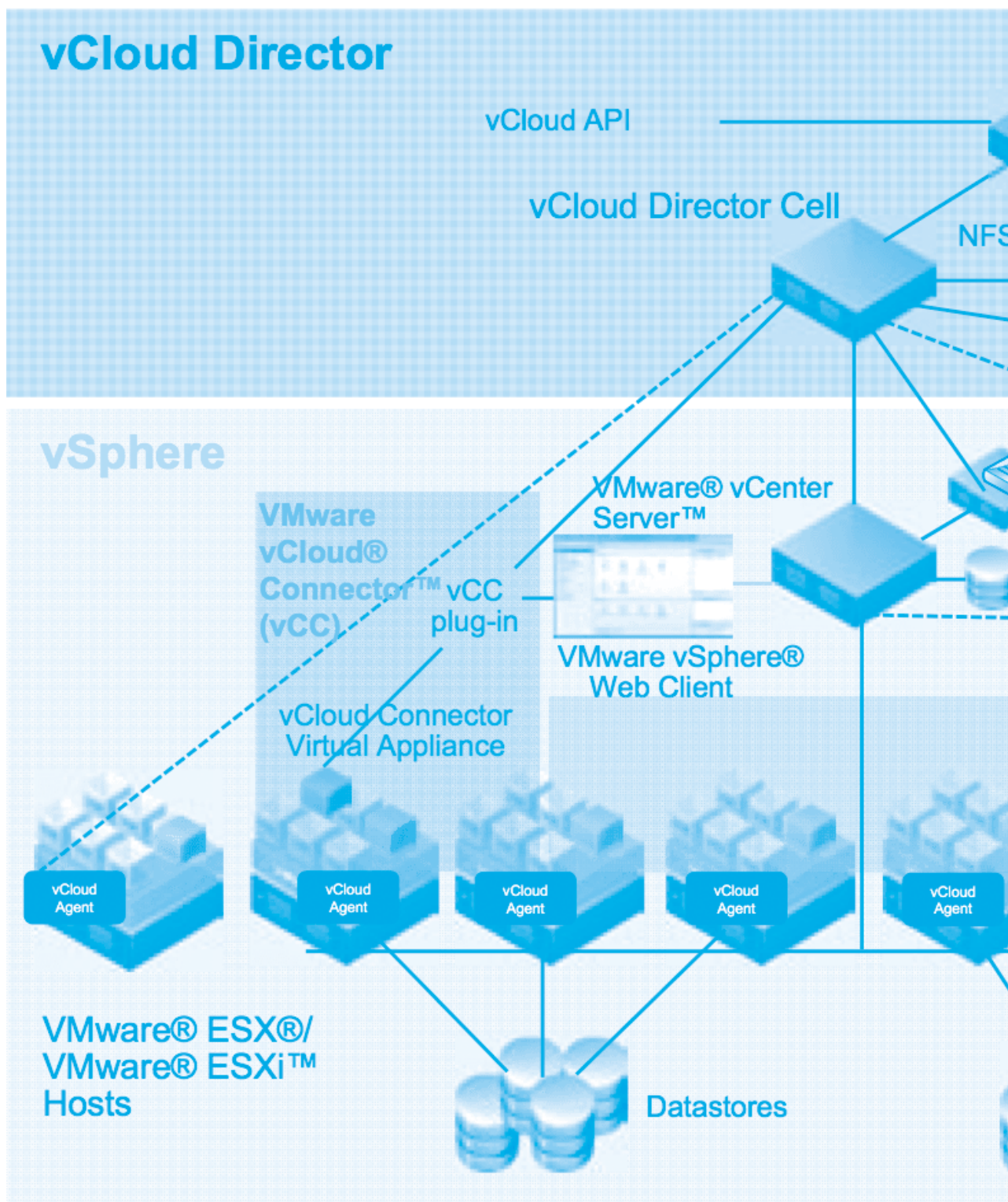
pulę zasobów i zapewniające odpowiedni poziom separacji poszczególnych klientów.

Centrum Danych

Rozwiązanie Atende Business Cloud zlokalizowane jest w Centrum Danych ATMAN o łącznej powierzchni 2500 m kw. Usługi świadczone w Centrum Danych ATMAN objęte są systemem zarządzania zgodnym z normą PN-EN

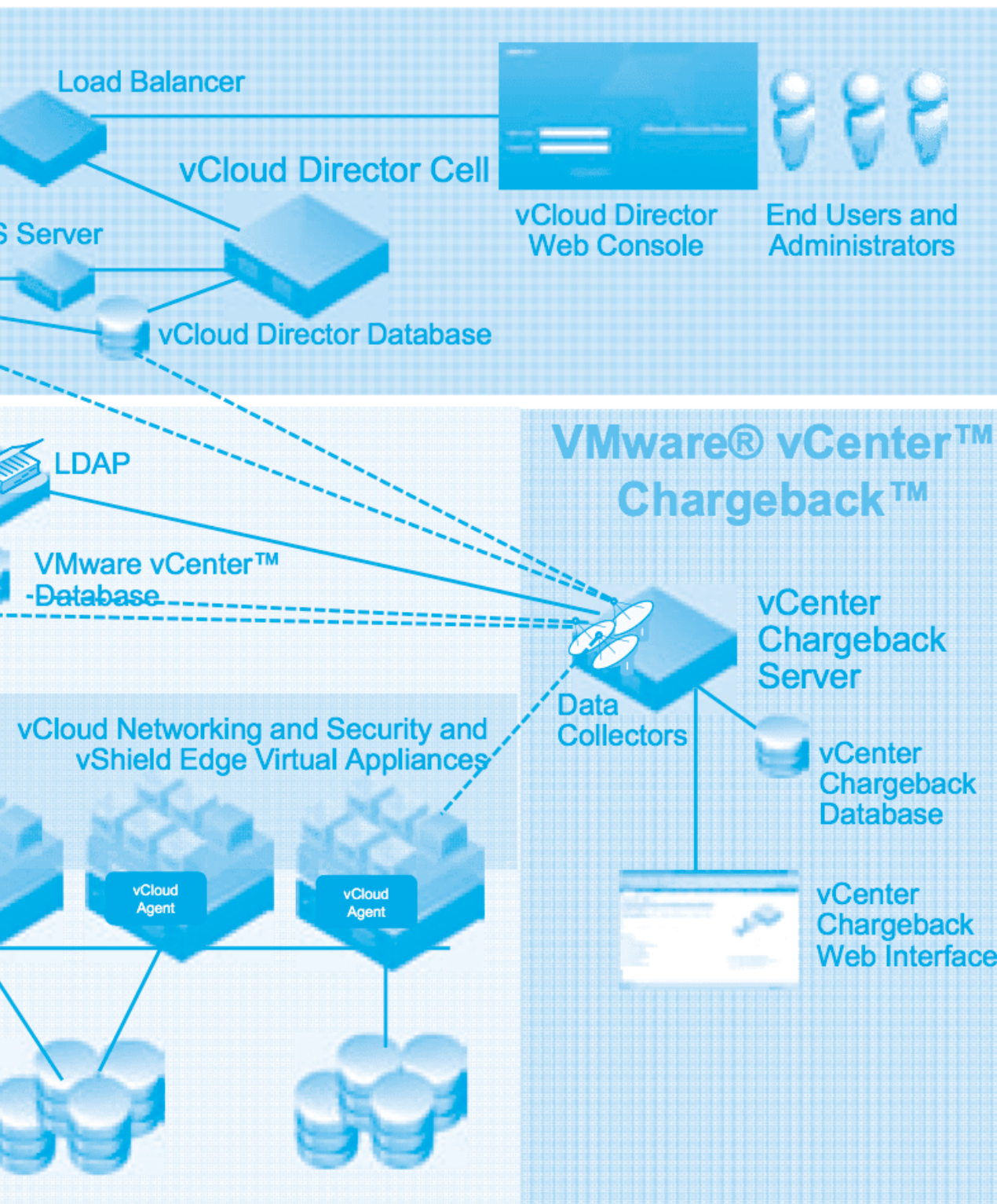
ISO 9001:2009 oraz systemem zarządzania bezpieczeństwem informacji zgodnym z normą ISO/IEC 27001:2005. Centrum Danych ATMAN posiada zdublowane niezależne podłączenia energetyczne średniego napięcia, zabezpieczone agregatami prądotwórczymi. System zasilania każdej szafy lub urządzenia zapewnia niezawodność na poziomie 2N. Cały system klimatyzacji pracuje w systemie redundancji





Rysunek 3

Architektura VMware vCloud Director



N+1 z N urządzeniami pracującymi i jednym gotowym do automatycznego startu w przypadku awarii któregośkolwiek z nich. Pomieszczenia serwerowni objęte są wielostrefowym, automatycznym systemem gaszenia, opartym o gaz obojętny. Data Center objęte jest monitoringiem w systemie 24x7x365 z wykorzystaniem telewizji przemysłowej. Całodobowa ochrona obiektu zapewniona jest przez umundurowanych strażników i system antywłamaniowy. Kluczowym aspektem współpracy z ATMAN jest dostęp do łącz transmisji danych z najmniejszymi opóźnieniami w Polsce. Dowolna awaria węzła sieci ATM nie wpływa na opóźnienia lub jakość przesyłu danych Klientów Atende Business Cloud. Dodatkowe >4500 km łączy międzymiastowych i >4400 km łączy międzynarodowych oraz styk z głównymi punktami (IX) wymiany ruchu w Polsce i na świecie zezwala na stworzenie dedykowanego połączenia z Atende Business Cloud. Elastyczność telekomunikacyjna po stronie Atende sprawia, że klienci Atende Business Cloud otrzymują możliwość dostępu do własnego Virtual Data Center poprzez dedykowane łącze lub Internet, w tym tunele VPN.

Architektura

Architektura rozwiązania (infrastruktura dzielona) bazuje na rozwiązaniach dedykowanych do budowy chmury publicznej. Unikalną cechą rozwiązań chmurowych Atende Business Cloud są fragmenty infrastruktury, które mogą mieć charakter infrastruktury dedykowanej z uwagi na uwarunkowania licencyjne. Architektura wykorzystuje komercyjne rozwiązania chmurowe oparte o oprogramowanie VMware w modelu operatorskim. Rozwiązanie jest proste i nieskomplikowane, nie korzysta z zasobów innych dostawców chmurowych. Dane są zlokalizowane w lokalizacji znanej i opisanej (Centrum Danych w lokalizacji Warszawa).

Serwery i Storage

Rozwiązanie sprzętowe w Atende Business Cloud opiera się na rozwiązaniach sprawdzonych na rynku. System serwerowy opiera się na serwerach HP Blade w obudowach HP C7000, na których uruchomione jest środowisko VMware. Przestrzeń dyskowa realizowana jest na wielu macierzach dyskowych dostępnych poprzez sieć Fiber Channel. Macierze takich firm jak HPE, HDS i EMC zapewniają najwyższy poziom wydajności i niezawodności. Połączone zasoby dysków SATA, SAS i SSD zapewniają odpowiedni poziom wydajności dyskowej dostosowanej do różnych zadań po stronie Klienta. Systemy uruchamiane w Atende Business Cloud mogą być replikowane na macierze zapasowe, które poza opcjami wysokiej dostępności z poziomu serwerów oraz systemu wirtualizacji, zapewniają bezpieczeństwo środowiska. Sprzęt jest połączony ze sobą za pomocą rozwiązań firm HP i Cisco (przełączniki LAN) oraz Brocade (przełączniki SAN) oraz Fortinet (wysoce wydajny firewall zewnętrzny). Backup środowiska zapewniony jest przez mechanizmy replikacji macierzy oraz dedykowane rozwiązania HP Data Protector. W zależności od poziomu ochrony wymaganej przez Klienta możliwe jest uruchomienie backupu całych systemów lub tylko części aplikacyjnej. Dane odkładane są na dedykowanych macierzach dyskowych lub na bibliotece taśmowej. Cała platforma obsługiwana jest przez dedykowany i doświadczony zespół inżynierów Atende, pracujących w trybie 24x7, którzy monitorują stan środowiska, zarządzają capacity i realizują zgłoszenia klientów.

Wirtualizacja

Środowisko Atende Business Cloud oparte jest na rozwiązaniu firmy VMware. Najważniejszą częścią usługi są hypervisorzy VMware ESXi uruchomione na wszystkich serwerach blade. Zapewniają one wysoki poziom stabilności i niezawodności rozwiązania.

System VMware vSphere zarządzany jest przez VMware vCenter. Na potrzeby wydzielenia dedykowanych i niezależnych od siebie środowisk oferujemy naszym klientom rozwiązanie VMware vCloud Director. vCloud Director w połączeniu z VMware vCloud Networking and Security zapewnia prosty interfejs użytkownika i separację na każdym możliwym poziomie (sieć, zasoby dyskowe, zasoby procesora, RAM, etc.)

Pozostały obszar oprogramowania

W Atende Business Cloud ma zastosowanie tylko technologia zgodna ze specyfikacją x86. W związku z powyższym rozwiązania bazodanowe ORACLE są migrowane do systemu opartego o x86. Rozwiązania bazodanowe typu Oracle DB po migrowaniu mogą być uruchamiane w środowisku wirtualizatora Oracle OVS (obniżenie kosztów licencyjnych). W rozwiązaniu chmurowym koszty oprogramowania wirtualizacyjnego i narzędzia tego oprogramowania są wliczone w koszty usługi utrzymaniowej. Zapewniamy również w modelu chmurowym licencje Microsoft na:

- systemy operacyjne
- bazy danych

Istnieje możliwość wykorzystania licencji będących własnością Klienta.

Zasoby wykorzystywane przez każdego z Klientów zliczane są w vCenter Chargeback zapewniając tym samym dokładne rozliczenie usług w trybie godzinowym.

Każde ze środowisk posiada dedykowany vShield Edge, który zapewnia zabezpieczenie firewall, router oraz urządzenie zapewniające funkcje NAT i load balancingu. Dzięki tym rozwiązaniom zapewniamy dodatkową warstwę ochrony środowiska klienta.

Procedury utrzymaniowe po migracji rozwiązania do chmury

Atende Business Cloud jest usługą świadczoną zgodnie z jakością (ISO 9001) i zasadami bezpieczeństwa (ISO 27001). Po migracji, proces wykonywania kopii zapasowej i/lub monitorowania systemu będzie dostosowany do nowej architektury systemu. Po migracji do chmury procedury operacyjne zostaną zaktualizowane do nowego modelu utrzymaniowego.

Zespół i certyfikaty

Zespół Atende i systemy spełniają szereg certyfikacji ISO 9001, AQAP 2110, ISO 27001. Systemy są wspierane przez inżynierów z certyfikatami wiodących producentów rozwiązań informatycznych. Atende kładzie duży nacisk na obsługę Klienta i zapewnienie odpowiednich warunków SLA. Atende oferuje wsparcie we wszystkich fazach projektu. Oferujemy możliwość wykorzystania katalogu usług zarządzanych w tym zarządzanie systemami Linux i Windows, dedykowany zespół wsparcia, Biuro Obsługi Klienta działające w trybie 24x7x365, gwarantowany czas reakcji i naprawy.

Atende jest uczestnikiem programu VMware vCloud Air Partner Program o statusie Enterprise. W umowie z Klientem określamy nie tylko parametry dostępności usług, ale także gwarantowane czasy reakcji i realizacji zgłoszenia oraz zabezpieczenie niedotrzymania SLA.

Wymaganie	Tak/Nie	Uwagi
<p>W1. Docelowe rozwiązanie powinno umożliwiać obsługę systemów i danych archiwalnych przez okres kilkunastu lat.</p>	Tak	Platforma Atende Business Cloud jest usługą rozwijaną i utrzymywaną od wielu lat. Produkt będzie rozwijany i będzie utrzymywany odpowiednio do nowych funkcjonalności środowiska chmurowego (kolejne wersje)
<p>W2. Rozwiązanie powinno zapewniać trwałe usunięcie danych po wygaśnięciu danego archiwum.</p>	Tak	Przy usunięciu usługi, dane mogą usuwane przy użyciu dostępnych mechanizmów i narzędzi
<p>W3. Docelowe rozwiązanie powinno zapewniać integralność danych.</p>	Tak	Integralność danych jest zapewniona na poziomie stosowanych rozwiązań i technologii chmurowych
<p>W4. Rozwiązanie powinno zapewniać skalowalność zarówno istniejących środowisk jak i możliwość uruchamiania kolejnych systemów archiwalnych.</p>	Tak	Naturalna cecha rozwiązania chmurowego, skalowalność pozioma.
<p>W5. Rozwiązanie powinno adresować wyzwania związane z zarządzaniem cyklem życia systemu w całym okresie świadczenia usługi łącznie z rozwiązaniem problemu uaktualniania systemów operacyjnych i aplikacji.</p>	Tak	W całym okresie świadczenia usługi pod warunkiem wspierania systemów operacyjnych oraz wybranych aplikacji dostępnymi aktualizacjami. Elementy EOS, mogą być objęte dodatkową, personalizowaną usługą.
<p>W6. Zaproponowane rozwiązanie powinno umożliwiać przenoszenie systemów między różnymi usługodawcami w chmurze publicznej</p>	Tak	Brak ograniczeń możliwości przeniesienia systemu do innego dostawcy chmurowego.

<p>W7. Uruchomienie systemów archiwalnych powinno być możliwe w dwóch separowanych ośrodkach.</p>	<p>Tak</p>	<p>Możliwość uruchomienia usługi w jednym z dwóch ośrodków na terenie Warszawy (usługa wykonywania dodatkowej kopii w drugim ośrodku)</p>
<p>W8. Dane powinny być przechowywane w DataCenter położonych na terenie Unii Europejskiej</p>	<p>Tak</p>	<p>Dane są przechowywane w jednym z dwóch ośrodków na terenie Warszawy (usługa wykonywania dodatkowej kopii w drugim ośrodku)</p>
<p>W9. Rozwiązanie powinno być zgodne z zaleceniami KNF (w tym z zaleceniem dotyczącym outsourcingu)</p>	<p>Wymaga uszczegółowienia zapisów prawnych</p>	<p>—</p>
<p>W10. Komunikacja sieciowa pomiędzy Bankiem, a infrastrukturą dostawcy powinien być zabezpieczony kryptograficznie</p>	<p>Tak</p>	<p>W zależności od dostępności warunków technicznych. Komunikacja może odbywać się poprzez połączenie typu Wirtualnej Sieci Prywatnej (VPN) lub za pośrednictwem połączeń dedykowanych z pominięciem styku z siecią Internet.</p>
<p>W11. Dane przechowywane w systemach pamięci masowych dostawcy usługi muszą być zabezpieczone kryptograficznie i dodatkowo w uzasadnionych przypadkach zastosowane powinny zostać mechanizmy zapewniające ich integralność</p>	<p>Tak</p>	<p>Dane przechowywane w systemach pamięci masowych nie są szyfrowane ale istnieje możliwość zastosowania szyfrowania na poziomie systemu operacyjnego za pomocą dodatkowych narzędzi. Integralność danych zapewniona jest tymi samymi mechanizmami co w środowiskach on-premise (np. RAID). Istnieje możliwość wykonywania dodatkowej kopii danych do drugiego ośrodka (replikacja)</p>
<p>W12. Powinien być zapewniony odpowiedni poziom separacji danych. Separacja fizyczna – tam gdzie jest to możliwe. Separacja logiczna – w przypadku, gdy dostawca usługi chmurowej nie jest w stanie zapewnić dedykowanej infrastruktury sprzętowej</p>	<p>Tak</p>	<p>Dostępna jest opcja separacji fizycznej w przypadku konieczności zapewnienia dedykowanej infrastruktury. Domyślnie ma zastosowanie separacja logiczna.</p>

<p>W13. Dostawca rozwiązania powinien być odpowiedzialny za utrzymywanie procesu zarządzania usługami dostarczany mi Bankowi.</p>	<p>Tak</p>	<p>Element standardowej usługi utrzymaniowej środowiska IaaS.</p>
<p>W14. Zasoby użytkowane przez Bank powinny być zabezpieczone poprzez odpowiednie mechanizmy bezpieczeństwa</p>	<p>Tak</p>	<p>Zasoby są zabezpieczone na wielu różnych poziomach: poprzez zgodność z wytycznymi (np. ISO, SOC2); poprzez bezpieczeństwo fizyczne (np. kontrola dostępu do pomieszczeń serwerowni); poprzez zabezpieczenia logiczne (wyposażenie infrastrukturalne typu FW, vLAN, VPN).</p>
<p>W15. Dostawca usługi jest zobowiązany do zapewnienia ciągłości działania usługi na poziomie określonym w stosownej umowie SLA</p>	<p>Tak</p>	<p>Poziom dostępności usługi jest opisany w umowie zawieranej pomiędzy Dostawcą i Klientem.</p>
<p>W16. dostawca usługi chmurowej jest zobowiązany aktywować usługi ochrony przed wszelkimi atakami oraz raportować do Banku wszystkie incydenty bezpieczeństwa</p>	<p>Tak</p>	<p>Środowisko chmurowe jest zaimplementowane u operatora (ATMAN), u którego działa Centrum Monitorowania Sieci (ang. Network Operations Center) w trybie 24/7 i monitoruje wydajność oraz bezpieczeństwo sieci I reaguje na wszelkie incydenty bezpieczeństwa. II linia monitorowania i reagowania jest uruchomiona w zespole NOC Atende Business Cloud</p>
<p>W17. Aktualna metoda uwierzytelniania powinna być przeniesiona do rozwiązania proponowanego przez dostawcę rozwiązania</p>	<p>Tak</p>	<p>W środowisku chmurowym IaaS, możliwe jest zastosowanie tych samych metod uwierzytelniania jak w obecnie wykorzystywanym systemie (np. uwierzytelnianie na poziomie aplikacji).</p>
<p>W18. Dopuszczalna jest możliwość przeniesienia obecnie działających aplikacji na inne systemy operacyjne czy też serwery bazodanowe o ile obniży to całkowity koszt utrzymania systemów</p>	<p>Tak</p>	<p>Rozwiązanie chmurowe Atende Business Cloud umożliwia migrację istniejących systemów i przeniesienie na systemy operacyjne zgodne ze standardem x86.</p>

ZAŁĄCZNIK 2

IBM: technologie wykorzystane w Architekturze docelowej.

Biorąc pod uwagę cel projektu oraz listę wymagań przekazanych przez Bank Raiffeisen, zespół IBM wziął pod uwagę dwa rozwiązania Chmurowe znajdujące się w portfolio IBM. Pierwszym jest IBM Bluemix Infrastructure (dawniej Softlayer), a drugim IBM Cloud Managed Services.

1. IBM Bluemix Infrastructure (dawniej Softlayer)

- a. infrastruktura dostępna w modelu usługowym (katalog usług, samoobsługa, opłata za faktyczne użycie, rozliczanie miesięczne, rozliczanie godzinowe, elastyczność);
- b. możliwość uruchamiania środowisk w architekturze x86 (Windows, Linux);
- c. maszyny wirtualne (kontrola do poziomu systemu operacyjnego);
- d. serwery fizyczne "Bare Metal" (kontrola do poziomu BIOS'u serwera);
- e. przestrzeń dyskowa (SSD, SAS, SAN);
- f. duża liczba usług dodatkowych (backup, monitoring, Disaster Recovery, etc.);
- g. możliwość zarządzania środowiskiem z poziomu interfejsu API;
- h. zgodność z normami i regulacjami (ISO 27001, ISO 27018, EU Model Clauses, Cloud Security Alliance, SOC1, SOC2, SOC3, PCI, HIPAA);
- i. łatwość przenoszenia środowisk zwirtualizowanych przy użyciu hypervisor'a VMware;
- j. różne możliwości połączenia z siecią Klienta (VPN, Direct Link).

Oba rozwiązania zapewniają usługi Chmurowe w modelu Infrastructure as a Service (IaaS), różnią się natomiast na poziomie funkcjonalnym. Poniżej zamieszczamy cechy charakterystyczne obu rozwiązań.

2. IBM Cloud Managed Services

- a. infrastruktura dostępna w modelu usługowym (katalog usług, samoobsługa, opłata za faktyczne użycie, rozliczanie miesięczne, elastyczność);
- b. możliwość uruchamiania środowisk w architekturze x86 (Windows, Linux) oraz Power (AIX);
- c. maszyny wirtualne (kontrola do poziomu systemu operacyjnego);
- d. przestrzeń dyskowa (SSD, SAS, SAN);
- e. usługi dodatkowe (backup, monitoring, patching, security, change management, configuration management, asset management) wliczone w cenę maszyny wirtualnej;
- f. gwarancja dostępności (SLA) na poziomie maszyny wirtualnej;

Decyzja co do wyboru konkretnego rozwiązania powinna być podjęta na podstawie szczegółowej analizy wymagań i zakresu projektu i w tym konkretnym przypadku wykracza poza zakres niniejszego opracowania.

Spełnienie wymagań Banku

– skrócony opis dla rozwiązania IaaS IBM Bluemix Infrastructure (dawniej Softlayer)



Wymaganie	Tak/Nie	Uwagi
W1. Docelowe rozwiązanie powinno umożliwić obsługę systemów i danych archiwalnych przez okres kilkunastu lat.	Tak	Polityka wsparcia konkretnych wersji systemów operacyjnych jest zgodna z polityką wsparcia każdego z producentów lub dostawców platform wirtualizacyjnych. Zakończenie okresu wsparcia może powodować konieczność działań adekwatnych do sytuacji (migracja wersji, eksport danych, przeniesienie do środowiska lokalnego).
W2. Rozwiązanie powinno zapewniać trwałe usunięcie danych po wygaśnięciu danego archiwum.	Tak	Po usunięciu przez Klienta maszyny wirtualnej bądź serwera fizycznego wszystkie przechowywane na nich dane są usuwane przy użyciu mechanizmu zgodnego ze standardem Ministerstwa Obrony Narodowej USA: DoD 5220.22-m.
W3. Docelowe rozwiązanie powinno zapewniać integralność danych.	Tak	Środowisko chmurowe działa w oparciu o te same mechanizmy zapewnienia integralności danych co środowiska lokalne.
W4. Rozwiązanie powinno zapewniać skalowalność zarówno istniejących środowisk jak i możliwość uruchamiania kolejnych systemów archiwalnych.	Tak	Standardowa funkcjonalność środowiska IaaS.
W5. Rozwiązanie powinno adresować wyzwania związane z zarządzaniem cyklem życia systemu w całym okresie świadczenia usługi łącznie z rozwiązaniem problemu uaktualniania systemów operacyjnych i aplikacji.	Tak	Dla wszystkich wspieranych systemów operacyjnych oraz niektórych standardowych aplikacji dostępne są wewnętrzne serwery aktualizacyjne. Pozostałe elementy mogą być objęte dodatkową, personalizowaną usługą.

<p>W6. Zaproponowane rozwiązanie powinno umożliwiać przenoszenie systemów między różnymi usługodawcami w chmurze publicznej</p>	<p>Tak</p>	<p>Umieszczenie systemu w środowisku chmurowym nie ogranicza możliwości przeniesienia tego systemu do innego dostawcy.</p>
<p>W7. Uruchomienie systemów archiwalnych powinno być możliwe w dwóch separowanych ośrodkach.</p>	<p>Tak</p>	<p>Usługi IaaS są dostępne w kilkudziesięciu centrach przetwarzania danych na całym świecie.</p>
<p>W8. Dane powinny być przechowywane w DataCenter położonych na terenie Unii Europejskiej</p>	<p>Tak</p>	<p>W Europie usługi IaaS są dostępne w następujących lokalizacjach: Holandia, Niemcy, Anglia, Włochy, Norwegia, Francja.</p>
<p>W9. Rozwiązanie powinno być zgodne z zalecaniami KNF (w tym z zaleceniem dotyczącym outsourcingu)</p>	<p>Wymaga uszczegółowienia zapisów prawnych</p>	
<p>W10. Komunikacja sieciowa pomiędzy Bankiem, a infrastrukturą dostawcy powinien być zabezpieczony kryptograficznie</p>	<p>Tak</p>	<p>Komunikacja może odbywać się poprzez połączenie Wirtualnej Sieci Prywatnej (ang. VPN) lub za pośrednictwem połączenia bezpośredniego (ang. Direct Link) z pominięciem sieci Internet.</p>
<p>W11. Dane przechowywane w systemach pamięci masowych dostawcy usługi muszą być zabezpieczone kryptograficznie i dodatkowo w uzasadnionych przypadkach zastosowane powinny zostać mechanizmy zapewniające ich integralność</p>	<p>Tak</p>	<p>Domyślnie dane przechowywane w systemach pamięci masowych nie są szyfrowane ale istnieje możliwość zastosowania szyfrowania na poziomie systemu operacyjnego za pomocą dodatkowych narzędzi. Integralność danych zapewniona jest tymi samymi mechanizmami co w środowiskach on-premise (np. RAID).</p>
<p>W12. Powinien być zapewniony odpowiedni poziom separacji danych. Separacja</p>	<p>Tak</p>	<p>Dostępna jest zarówno separacja fizyczna (tzw. Serwery Bare Metal) jak i separacja logiczna.</p>

fizyczna – tam gdzie jest to możliwe. Separacja logiczna – w przypadku, gdy dostawca usługi chmurowej nie jest w stanie zapewnić dedykowanej infrastruktury sprzętowej

W13. Dostawca rozwiązania powinien być odpowiedzialny za utrzymywanie procesu zarządzania usługami dostarczany mi Bankowi.

Tak

Standardowa funkcjonalność środowiska IaaS.

W14. Zasoby użytkowane przez Bank powinny być zabezpieczone poprzez odpowiednie mechanizmy bezpieczeństwa

Tak

Środowisko IaaS zabezpieczone jest na wielu różnych poziomach, od zgodności z oficjalnymi normami (np. ISO, SOC2), poprzez bezpieczeństwo fizyczne (np. Kontrola dostępu do pomieszczeń serwerowni) aż po zabezpieczenia logiczne (np. Firewall, vLAN).

W15. Dostawca usługi jest zobowiązany do zapewnienia ciągłości działania usługi na poziomie określonym w stosownej umowie SLA

Tak

Poziom dostępności usługi jest określany w stosownej umowie zawieranej pomiędzy Dostawcą i Klientem.

W16. Dostawca usługi chmurowej jest zobowiązany aktywować usługi ochrony przed wszelkimi atakami oraz raportować do Banku wszystkie incydenty bezpieczeństwa

Tak

W środowisku zaimplementowane jest Centrum Monitorowania Sieci (ang. Network Operations Center), które działa w trybie 24/7 i monitoruje wydajność oraz bezpieczeństwo sieci oraz reaguje na wszelkie incydenty bezpieczeństwa.

W17. Aktualna metoda uwierzytelniania powinna być przeniesiona do rozwiązania proponowanego przez dostawcę rozwiązania

Tak

Przeniesienie systemu do rozwiązania chmurowego nie wymusza konieczności zmiany metody uwierzytelniania. W środowisku IaaS, możliwe jest zastosowanie tych samych metod uwierzytelniania jak w obecnie wykorzystywanym systemie.

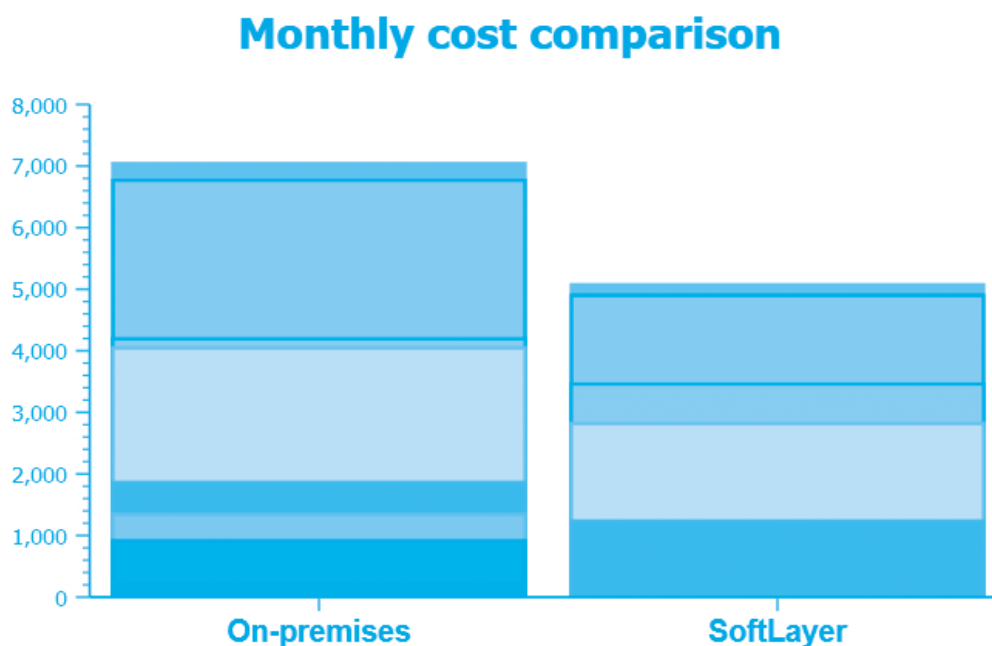
W18. Dopuszczalna jest możliwość przeniesienia obecnie działających aplikacji na inne systemy operacyjne czy też serwery bazodanowe o ile obniży to całkowity koszt utrzymania systemów

Tak

Rozwiązania Chmurowe firmy IBM umożliwiają zarówno migrację istniejących systemów (bez modyfikacji) jak i przeniesienie istniejących systemów na inne systemy operacyjne czy serwery bazodanowe. Obecnie wykorzystywane środowisko może zostać przemiegrwane do chmury IaaS bez zmiany np. typu systemu operacyjnego (dotyczy CMS)

Rysunek 1

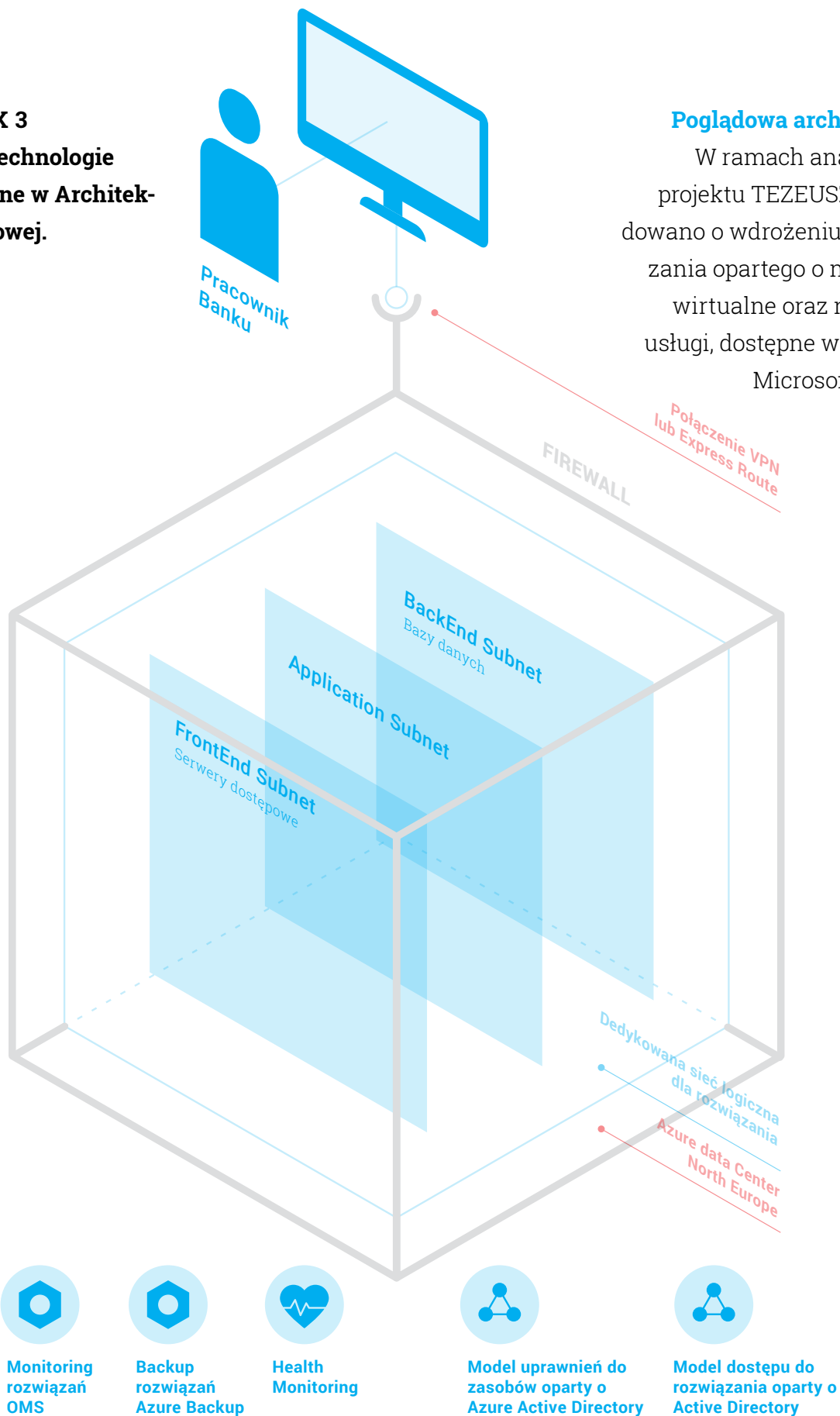
Przykładowy wynik działania kalkulatora TCO.



Aby ułatwić podjęcie decyzji o migracji lokalnej infrastruktury do rozwiązania Chmurowego firma IBM udostępnia kalkulator Całkowitych Kosztów Utrzymania (ang. TCO), który w sposób przejrzysty pokazuje obszary jakie należy wziąć

pod uwagę rozważając migrację do Chmury, oraz pozwala porównać najważniejsze elementy z punktu widzenia kosztów. Narzędzie dostępne jest pod adresem <http://www.softlayer.com/tco/> (uwaga: tylko w języku angielskim).

ZAŁĄCZNIK 3
Microsoft: technologie
wykorzystane w Architek-
turze docelowej.



Poniższa tabela prezentuje, mapowanie pomiędzy aktualnie wykorzystywanymi maszynami rozwiązań a maszynami wirtualnymi Microsoft Azure, które mogą zostać użyte w ramach chmury, do świadczenia usługi.

Więcej o maszynach wirtualnych Microsoft Azure oraz specyfikacji maszyn, zebranych w tabeli można przeczytać w ramach poniższej dokumentacji: <https://azure.microsoft.com/pl-pl/documentation/services/virtual-machines/>

Rola maszyny	Aplikacja główna	Wybór maszyny w chmurze Microsoft Azure
Active directory	Domain Controller	Seria A1
Aplikacja	AML	Seria A1
Aplikacja	XX Plus	Seria A2
Aplikacja	FC Host	Seria A2
Aplikacja	FC Host	Seria A2
Aplikacja	FC@	Seria A2
Aplikacja	FC@	Seria A2
Baza danych	AML	Seria A2
Baza danych	XX Plus	Seria A3
Baza danych	XX	Seria A3
Baza danych	XX (archive server)	Seria A2
Baza danych	iApply	Seria A7

Microsoft proponuje oprzeć budowę środowiska o maszyny wirtualne oraz usługi dodane występujące w chmurze Microsoft Azure.

Chmura ta charakteryzuje się m.in.:

- 1) Sześcioma operacyjnymi centrami danych na terenie Europejskiego Obszaru Gospodarczego, ponad 30 centrami na Świecie;
- 2) Usługami oferowanymi w modelu IaaS, PaaS jak i SaaS dostępnymi z jednego Panelu Zarządzania;
- 3) Minutowym rozliczaniem kosztów usług do-

stępnym z chmury w różnych modelach płatności;

- 4) Szeroką liczbą certyfikacji, przyznanych przez niezależne agencje rządowe jak i międzynarodowe instytucje audytowe, w tym takich jak SOC1, SOC2, SOC3, EU Model Clauses, EU-U.S. Privacy Shield, ISO/IEC 27001, 27017, 27018, 22301, HiPPA.

Pełna lista ponad 40 certyfikacji dostępna jest pod adresem <https://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx>.

Zgodność z wymogami Banku

Wymaganie	Tak/Nie	Uwagi
W1. Docelowe rozwiązanie powinno umożliwić obsługę systemów i danych archiwalnych przez okres kilkunastu lat.	Tak	Polityka wsparcia konkretnych wersji systemów operacyjnych jest zgodna z polityką wsparcia każdego z producentów. Zakończenie okresu wsparcia może powodować konieczność podjęcia działań. W przypadku chmury Microsoft nadal wspierane jest uruchomienie Windows 2003 mimo zakończenia wsparcia dla producenta tego oprogramowania. Co więcej, Microsoft przed wygaszeniem wsparcia dla konkretnej edycji systemu w chmurze informuje o tym z wyprzedzeniem i daje klientom czas na podjęcie działań, niezbędnych do migracji do wyższych wersji.
W2. Rozwiązanie powinno zapewniać trwałe usunięcie danych po wygaśnięciu danego archiwum.	Tak	Po usunięciu przez Klienta danych, dane te są usuwane w zadanym oknie czasowym w sposób nieodwracalny. Dodatkowo nośniki w centrach danych są usuwane zgodnie z procedurą NIST. https://www.microsoft.com/en-us/TrustCenter/Compliance/DISA#NISTRequirements

<p>W3. Docelowe rozwiązanie powinno zapewniać integralność danych.</p>	Tak	Środowisko chmurowe działa w oparciu o te same mechanizmy zapewnienia integralności danych co środowiska lokalne.
<p>W4. Rozwiązanie powinno zapewniać skalowalność zarówno istniejących środowisk jak i możliwość uruchamiania kolejnych systemów archiwalnych.</p>	Tak	Chmura obliczeniowa pozwala na skalowanie zarówno w szerz (Scale Out) jak i w górę / dół (Scale In). Skalowanie w szerz pozwala dodawać kolejne instancje maszyn wirtualnych czy usług, skalowanie w górę pozwala zwiększać parametry danej instancji.
<p>W5. Rozwiązanie powinno adresować wyzwania związane z zarządzaniem cyklem życia systemu w całym okresie świadczenia usługi łącznie z rozwiązaniem problemu uaktualniania systemów operacyjnych i aplikacji.</p>	Tak	Rozwiązania PaaS są aktualizowane automatycznie przez chmurę Microsoft. Rozwiązania IaaS mogą być aktualizowane przez usługę OMS, dostępną w chmurze. Systemy wirtualne są aktualizowane na bieżąco przez wewnętrzne mechanizmy Microsoft.
<p>W6. Zaproponowane rozwiązanie powinno umożliwiać przenoszenie systemów między różnymi usługodawcami w chmurze publicznej</p>	Tak	Umieszczenie systemu w środowisku chmurowym nie ogranicza możliwości przeniesienia tego systemu do innego dostawcy.
<p>W7. Uruchomienie systemów archiwalnych powinno być możliwe w dwóch separowanych ośrodkach.</p>	Tak	Usługi IaaS oraz PaaS są dostępne w ponad 30 centrach przetwarzania danych na całym świecie. W przypadku rejonu EOG dostępne jest 6 ośrodków
<p>W8. Dane powinny być przechowywane w DataCenter położonych na terenie Unii</p>	Tak	W Europie usługi chmury publicznej dostępne są w 6 ośrodkach w takich krajach jak Irlandia, Dania, Niemcy, Wielka Brytania. Od 2017 roku

Europejskiej

będą dostępne ośrodki w Francji.

W9. Rozwiązanie powinno być zgodne z zalecaniami KNF (w tym z zaleceniem dotyczącym outsourcingu)

Wymaga uszczegółowienia zapisów prawnych

W10. Komunikacja sieciowa pomiędzy Bankiem, a infrastrukturą dostawcy powinien być zabezpieczony kryptograficznie

Tak

Komunikacja może odbywać się poprzez połączenie Wirtualnej Sieci Prywatnej (Site2Site VPN) lub za pośrednictwem połączenia bezpośredniego (ang. Express Route) z pominięciem sieci Internet. Oba te modele dostępu mogą być mieszane, mogą działać równolegle.

W11. Dane przechowywane w systemach pamięci masowych dostawcy usługi muszą być zabezpieczone kryptograficznie i dodatkowo w uzasadnionych przypadkach zastosowane powinny zostać mechanizmy zapewniające ich integralność

Tak

Dane kont składowania danych, dyski maszyn wirtualnych mogą być szyfrowane za pomocą różnych mechanizmów w tym BitLocker, DM Crypt czy za pomocą algorytmów opartych o AES 256.

<https://docs.microsoft.com/en-us/azure/storage/storage-service-encryption>

W12. Powinien być zapewniony odpowiedni poziom separacji danych. Separacja fizyczna – tam gdzie jest to możliwe. Separacja logiczna – w przypadku, gdy dostawca usługi chmurowej nie jest w stanie zapewnić dedykowanej infrastruktury sprzętowej

Tak

Dostępna jest separacja logiczna dla usług i danych, możliwa jest separacja fizyczna dla wybranych rozwiązań.

W13. Dostawca rozwiązania powinien być odpowiedzialny za utrzymywanie procesu zarządzania usługami dostarczonymi Bankowi.

Tak

Usługa wbudowowana.

W14. Zasoby użytkowane przez Bank powinny być zabezpieczone poprzez odpowiednie mechanizmy bezpieczeństwa

Tak

Temat ten jest bardzo szeroki. Bezpieczeństwo usług gwarantowane jest na poziomie następujących warstw:

- bezpieczeństwo fizyczne dla budynków i infrastruktury
- bezpieczeństwo tożsamości i dostępu
- bezpieczeństwo procesów operacyjnych
- bezpieczeństwo sieci
- ochrona przed zagrożeniami i atakami
- audytowanie i logowanie zdarzeń
- szyfrowanie danych, kluczy

Szerzej ten temat jest omówiony w oficjalnym dokumencie Microsoft na temat bezpieczeństwa chmury publicznej.

<https://www.microsoft.com/en-us/trustcenter/Security/default.aspx>

W15. Dostawca usługi jest zobowiązany do zapewnienia ciągłości działania usługi na poziomie określonym w stosownej umowie SLA

Tak

Poziom dostępności usługi jest określany w stosownej umowie zawieranej pomiędzy Dostawcą i Klientem.

W16. dostawca usługi chmurowej jest zobowiązany aktywować usługi ochrony przed wszelkimi atakami oraz raportować do Banku wszystkie incydenty bezpieczeństwa

Tak

W środowisku zaimplementowane jest Centrum Monitorowania Sieci (ang. Network Operations Center), które działa w trybie 24/7 i monitoruje wydajność oraz bezpieczeństwo sieci i reaguje na wszelkie incydenty bezpieczeństwa.

W17. Aktualna metoda uwierzytelniania powinna być przeniesiona do rozwiązania proponowanego przez dostawcę rozwiązania

Tak

Przeniesienie systemu do rozwiązania chmurowego nie wymusza konieczności zmiany metody uwierzytelniania. W środowisku IaaS, możliwe jest zastosowanie tych samych metod uwierzytelniania jak w obecnie wykorzystywanym systemie.

W18. Dopuszczalna jest możliwość przeniesienia obecnie działających aplikacji na inne systemy operacyjne czy też serwery bazodanowe o ile obniży to całkowity koszt utrzymania systemów

Tak

Rozwiązania pozwala na migrację usług do usług PaaS, wymaga to jednak dostosowania rozwiązania i musimy być przeanalizowane przed rozpoczęciem procesu migracji.

ZAŁĄCZNIK 4

Skład zespołu projektowego „Tezeusz”

Autorzy raportu

(alfabetycznie):

Atende

Marcin Germel

Paweł Pętlicki

IBM

Robert Kleniewski

Karolina Marzantowicz

Andrzej Osmak

Microsoft

Michał Furmankiewicz

Raiffeisen Bank

Piotr Bubieńczyk

Michał Brandt

Piotr Kiersnowski

Przewodniczący projektu TEZEUSZ

Tomasz Pelczarski, Microsoft

Designed by:
Voilà! Information Design Studio
www.voila-infographics.com

