Uniwersytet Ekonomiczny w Katowicach

Studia Ekonomiczne. Zeszyty Naukowe
Uniwersytetu Ekonomicznego w Katowicach
ISSN 2083-8611 Nr 375 · 2018

Informatyka i Ekonometria 14

Piotr Czerwonka

Uniwersytet Łódzki
Wydział Zarządzania
Katedra Informatyki
pc@wzmail.uni.lodz.pl

Łukasz Zakonnik

Uniwersytet Łódzki
Wydział Ekonomiczno-Socjologiczny
Katedra Informatyki Ekonomicznej
lukasz.zakonnik@uni.lodz.pl

BEZPIECZEŃSTWO W CHMURZE VS BEZPIECZEŃSTWO TRADYCYJNE – STUDIA PRZYPADKÓW

Streszczenie: Chmura obliczeniowa od kilku lat staje się silną alternatywą dla rozwiązań w siedzibie organizacji pod względem zakresu funkcjonalności i rachunku kosztów. Jedną z głównych wątpliwości przy implementacji rozwiązań chmurowych jest jednak przestrzeń dotycząca zagadnień bezpieczeństwa informacji. Artykuł akcentuje wątpliwości dotyczące integracji usług uwierzytelniania w chmurze oraz poprawnej implementacji rozwiązań związanych z bezpieczeństwem informacji w wyniku projekcji standardowych rozwiązań na architekturę chmury obliczeniowej na podstawie studiów przypadków.

Słowa kluczowe: chmura obliczeniowa, bezpieczeństwo, uwierzytelnianie.

JEL Classification: M15, O33.

Wprowadzenie

Rozwój technologii związanych z chmurą obliczeniową przyczynił się w ostatnich latach do postępującego procesu reorientacji strategii IT zarówno małych, jak i dużych organizacji. Jest to spowodowane nie tylko potrzebą podążania za trendem wytworzonym przez międzynarodowe korporacje, ale również wykorzystaniem korzyści związanych z tą technologią i pogonią za poszukiwaniem przewagi konkurencyjnej. Rosnąca potrzeba elastyczności, innowacyjności i zysku sprawia, że coraz trudniej nie zauważać zalet, jakie niesie za sobą elastyczny i skalowalny model przetwarzania danych w chmurze.

Do zalet przetwarzania danych w chmurze można zaliczyć m.in.:

– redukcję kosztów początkowych dla mniejszych organizacji, które potrzebują usług IT,

- praktycznie natychmiastowy dostęp do zasobów obliczeniowych, bez wcześniejszych nakładów inwestycyjnych (redukcja kosztów IT),
- obniżenie barier IT dla innowacyjnych rozwiązań,
- łatwiejsze skalowanie usług np. w dużych korporacjach,
- dostęp do nowych grup aplikacji i usług, które nie mogły być dostępne bez rozmachu i możliwości przetwarzania danych drzemiących w chmurze [Avram, 2014, s. 531].

Potencjalne zalety chmury obliczeniowej są udokumentowane w licznych opracowaniach. Adaptacja usług w tym modelu przetwarzania danych w przeciągu ostatnich lat znacznie wzrosła w wielu obszarach (również w Polsce). Jest to spowodowane w dużej mierze tkwiącym w chmurze potencjałem: transformacji procesów biznesowych, obniżania wydatków związanych z IT i dostarczania aplikacji przetwarzających dane w czasie rzeczywistym, a także oferowaniem dostępu do wszechobecnej przestrzeni do przechowywania danych oraz nieograniczonej mocy obliczeniowej [Durao i in., 2014, s. 1321].

Rozwiązania chmurowe w przeważającej mierze są oferowane przed duże koncerny, które wypracowały nowe lub zmodyfikowały swoje modele biznesu i zaoferowały swoim klientom usługi obliczeniowe o bardzo szerokim zakresie. Dla przykładu, Microsoft – tworząc ofertę opartą na nowym modelu przetwarzania danych – kontynuował rozwój rozwiązań biurowych, korzystając z chmury obliczeniowej, oraz pracował nad migracją dobrze już znanych swoim klientom produktów do własnych centrów danych i poszerzał ofertę SaaS. Amazon zaoferował dostęp do „nieograniczonej" mocy obliczeniowej poprzez elastyczną gamę maszyn wirtualnych PaaS i możliwość przechowywania danych w warstwie IaaS. W przypadku najpopularniejszych usług chmurowych pojawiły się rozwiązania, których odpowiedniki były rozpowszechnione w tradycyjnym modelu przetwarzania danych, sam model ich implementacji w chmurze był mało skomplikowany, a ich znaczenie dla organizacji – dobrze zbadane i opisane [Cattaneo, 2014, s. 5].

Celem artykułu, oprócz rozważań teoretycznych, jest wskazanie, jakie zalety i bariery napotykają organizacje podczas wdrażania rozwiązań chmury obliczeniowej w swojej działalności – zwłaszcza w kontekście zagadnień dotyczących bezpieczeństwa. Zdefiniowanie wniosków umożliwiła analiza dwóch studiów przypadków.

Zastosowana w niniejszym opracowaniu metodologia badawcza obejmuje przegląd literaturowy publikacji na temat zalet i barier związanych z implementacją systemów informatycznych w chmurze obliczeniowej oraz zagadnień dotyczących tożsamości w chmurze obliczeniowej. W celu weryfikacji i odniesienia

się do problemów opisywanych w literaturze przedstawiono analizę przypadków przenoszenia systemów do modelu chmury obliczeniowej dla dwóch polskich przedsiębiorstw. Zdefiniowano następujące pytania badawcze:

1. Jakie korzyści i trudności wprowadzania rozwiązań chmurowych są omawiane w literaturze?
2. Czy korzyści i problemy napotykane w polskich przedsiębiorstwach – zwłaszcza dotyczące bezpieczeństwa – są podobne do tych raportowanych w literaturze?

1. Tożsamość tradycyjna vs tożsamość w chmurze (uwierzytelnienie i kontrola dostępu)

Pomimo niezaprzeczalnych zalet, nie wszystkie organizacje decydują się na wykorzystanie zasobów chmury obliczeniowej. Bariery związane z adaptacją chmury obliczeniowej są od lat niezmienne i należą do nich głównie:

- zagadnienia dotyczące obawy o bezpieczeństwo, prywatność danych i procesów związanych z ich przetwarzaniem w chmurze,
- dostępność i otwarty dostęp (sieciowy),
- niezawodność,
- interoperacyjność licznych rozwiązań chmurowych,
- wartość ekonomiczna (ukryte koszty),
- zmiany w organizacji IT,
- aspekty polityczne, regulacje prawne poprzez granice [Phaphoom i in., 2015, s. 167].

Prowadzone od lata badania pokazują [Oliveira, 2014, s. 497], że zagadnienia związane z prywatnością danych i bezpieczeństwem są czynnikiem, który budzi u potencjalnych użytkowników wiele obaw; mogą one wstrzymywać decyzje odnoszące się do wykorzystania zasobów chmurowych. Wynika to z przesłanek biznesowych, psychologicznych i technologicznych.

Środowisko chmury obliczeniowej, niezależnie od tego, czy chodzi o chmurę prywatną opartą na rozwiązaniach otwartych, czy chmurę publiczną dużego dostawcy, różni się sposobami implementacji komponentów gwarantujących szeroko rozumiane bezpieczeństwo od mechanizmów wykorzystywanych w tradycyjnych środowiskach on-premise. Wynika to zarówno z większej złożoności architektury chmury, jak i przede wszystkim z potrzeby udostępnienia dużo większego stopnia elastyczności oraz automatyzacji przy implementacji nowych aplikacji i usług w chmurze dla nowych narzędzi klienckich. Pomimo wykorzystywania tych samych języków programowania czy pracy w tych samych śro-

dowiskach uruchomieniowych zagwarantowanie podobnego zestawu funkcjonalności w chmurze czy środowisku tradycyjnym może wymagać innych umiejętności i odpowiedniego doświadczenia [Andriole, 2018, s. 80].

Sposób pracy użytkowników, wdrożone procedury administracyjne, przyzwyczajenia oraz zakres możliwości dotyczący zabezpieczenia danych jest uzależniony od środowiska informatycznego dostępnego w organizacji. Duża część istniejących korporacyjnych infrastruktur IT i mniejszych sieci komputerowych jest oparta na systemach Microsoft Windows (ponad 80% udziału na świecie i ponad 90% w Polsce) [www 2]. W przypadku środowisk zarządzalnych od wielu lat monopolistą w zakresie dostarczania usług zarządzających tożsamością i stanowiących rdzeń bezpieczeństwa infrastruktury również pozostaje Microsoft ze swoją usługą Active Directory. Prawie 95% organizacji z listy Fortune 1000 korzysta właśnie z tego rozwiązania do wsparcia procesów zarządzania IT.

W tradycyjnych środowiskach on-premise zazwyczaj występuje centralne repozytorium tożsamości i usługi, które pozwalają korzystać z tego repozytorium w procesie uwierzytelniania oraz autoryzacji. Znaczny wysiłek administracyjny jest skupiony na konfiguracji środowiska pracy użytkownika – zabezpieczenia stacji roboczych, zagwarantowania dostępu do zasobów oraz monitorowania parametrów jego pracy. Praca w środowisku on-premise jest oparta na kontroli dostępu do wewnętrznej sieci komputerowej, w której znajdują się zasoby organizacji. Nawet w przypadku rozległej sieci, składającej się z wielu lokalizacji, jednym z głównych zadań jest „zamknięcie" dostępu do własnej infrastruktury przed nieupoważnionymi podmiotami poprzez stosowanie np. wirtualnych sieci prywatnych, firewalli czy wyrafinowanych urządzeń dostępowych. Zagadnienia dotyczące bezpieczeństwa informacji i kontroli dostępu do danych organizacji ulegają zmianom i wymagają ciągłego rozwoju w pogoni za postępem technologii i wobec coraz bardziej wyrafinowanych e-zagrożeń. Administratorzy infrastruktur on-premise przez lata doskonalili swoje umiejętności i kontrolowali – z mniejszym lub większym powodzeniem – dostęp do informacji w korporacji. Jedną z większych zmian, a zarazem wyzwaniem stojącym przez organizacjami, był fenomen rozwoju popularności urządzeń mobilnych i wzrost ich znaczenia w pracy każdego przedsiębiorstwa. Tradycyjnie restrykcyjny model kontroli dostępu do zasobów spotkał się m.in. z trendem BYOD (Bring Your Own Device) i w wielu przypadkach wymuszał adaptację strategii mobilności w organizacji [Podgórski, 2016, s. 137].

Praca w chmurze obliczeniowej oznacza jeszcze więcej wyzwań i potencjalnie więcej obszarów, które należy ująć w polityce bezpieczeństwa [www 1]. Nowe sposoby dostępu klienckiego, nowe protokoły, chmurowe wersje znanych

usług to nie jedyne zadania, które stoją przed działami IT zmagającymi się z chmurą obliczeniową.

Chmura obliczeniowa w wieloraki sposób wpływa na zagadnienia dotyczące zarządzania tożsamością i dostępem (Identity and Access Management). Główną różnicą w stosunku do tradycyjnego modelu przetwarzania danych jest relacja pomiędzy usługodawcą chmury obliczeniowej a jej użytkownikiem. Zarządzanie tożsamością i dostępem musi być wykonywane we współpracy pomiędzy tymi bytami, a żeby było to możliwe, niezbędne staje się zaufanie pomiędzy klientem i usługodawcą, oddelegowanie odpowiedzialności administracyjnej oraz odpowiednie narzędzia umożliwiające wykonywanie niezbędnych operacji związanych z zarządzaniem tożsamością [Mogull i in., 2017, s. 129]. Zakładając, że organizacja może wykorzystywać usługi chmurowe udostępniane przez różnych usługodawców, zagadnienia związane z zarządzaniem tożsamością mogą charakteryzować się wysokim poziomem skomplikowania [Ghazizadeh i in., 2013, s. 3].

W przypadku chmury obliczeniowej informacja o tożsamości użytkowników jest zazwyczaj przechowywana w centralnym repozytorium tożsamości [Zwattendorfer i in., 2013, s. 12] – często nazywanego „tożsamość jako usługa" (Identity as a Service – IDaaS). Użytkownik chmury powinien mieć możliwość dostępu zarówno do panelu administracyjnego chmury, jak i do poszczególnych aplikacji w niej uruchomionych za pomocą tych samych poświadczeń. Do wsparcia takiej funkcjonalności w środowisku chmurowym wykorzystuje się mechanizmy uwierzytelniania i protokoły, które są charakterystyczne dla rozproszonych środowisk i aplikacji WWW. W przypadku zamkniętych środowisk tradycyjnych pod kontrolą systemów Windows do uwierzytelnienia stosuje się zazwyczaj protokoły Kerberos i NTLM, a w przypadku chmury obliczeniowej – OpenID. Znaczne różnice dotyczą też podejścia do procesu autoryzacji. W środowiskach tradycyjnych powszechnie używa się różnego rodzaju list kontroli dostępu do zasobów ACL (Access Control List). Chmura obliczeniowa jest oparta przeważnie na standardzie autoryzacyjnym OAuth.

Naturalnym następstwem transferu danych do chmury obliczeniowej jest integracja istniejących mechanizmów uwierzytelniania i autoryzacji z odpowiednikami z chmury. Użytkownicy Microsoft Azure otrzymują dostęp do usługi o takiej samej nazwie, jak w sytuacji wdrożeń on-premise, ale w przypadku chmury obliczeniowej usługa Active Directory występuje w wielu wersjach, co przekłada się na wiele dostępnych scenariuszy wdrożenia i integracji:

1. Azure Active Directory (AAD) – centralna usługa katalogowa do zarządzania kontami użytkowników i grup.

2. Rozwiązanie hybrydowe – integracja Azure AD i usług katalogowych on-premise. Organizacja posiada własną usługę katalogową i za pomocą odpowiedniego oprogramowania synchronizuje dane o użytkownikach z usługą katalogową w chmurze.
3. Azure AD Domain Services – chmurowy, zintegrowany z AAD, odpowiednik tradycyjnej usługi Active Directory, pozwalający na zarządzanie kontami komputerów i przeprowadzanie większości operacji charakterystycznych dla środowisk on-premise.
4. Do-it-yourself AD DS – niezintegrowana z AAD instalacja usługi Active Directory na maszynie wirtualnej w chmurze.

2. Studia przypadków

Z przeprowadzonych badań wyodrębniono dwie duże organizacje, które zrealizowały transfer części zasobów do chmury obliczeniowej Azure. Każda z nich stanęła wobec innych wyzwań i problemów związanych z transferem.

W obu przypadkach określono charakterystykę organizacji, wykorzystywane rozwiązanie ICT i główne przyczyny, dla których zdecydowano poszerzyć architekturę ICT o zasoby chmury obliczeniowej. Następnie przedstawiono główne etapy wdrażania rozwiązań chmurowych oraz wnioski z nich płynące.

2.1. Studium przypadku I

Pierwszą z analizowanych organizacji jest firma zajmująca się produkcją wyposażenia medycznego. Organizacja posiada pięć głównych lokalizacji, z których cztery znajdują się w Polsce, a jedna w USA. Z zasobów IT organizacji korzysta 251 pracowników, a nad sprawną pracą wszystkich komponentów związanych z bezpieczeństwem i elektronicznym przetwarzaniem danych w organizacji czuwa 8 pracowników działu IT. Badana organizacja dysponuje bogatym zapleczem serwerowym, ale już od min. pięciu lat szuka możliwości przeniesienia poza siedzibę swoich zasobów elektronicznych (w tym do chmury obliczeniowej) w celu redukcji kosztów oraz poszerzenia gamy usług elektronicznych zarówno dla intranetu, jak i dla zewnętrznych kontrahentów czy klientów.

Firma rozpoczęła transfer zasobów do chmury obliczeniowej od przeniesienia usług poczty elektronicznej. Usługi komunikacji elektronicznej były do tej pory utrzymywane w ramach zasobów własnych organizacji, ale ich zabezpie-

czenie i utrzymanie wymagało coraz większego wysiłku. Rozwiązaniem, które wybrano, był system pracy grupowej oparty na Microsoft Exchange.

Jednym z głównych czynników branych pod uwagę przy wyborze usługodawcy były względy bezpieczeństwa – rozwiązanie oferowane w modelu SaaS (Software as a Service) powinno umożliwić odpowiedni poziom szyfrowania transmisji danych, a także integrację mechanizmów zarządzania kontami i uwierzytelnianiem. Organizacja posiadała usługę Active Directory, której używała m.in. do wdrażania oraz utrzymywania polityk bezpieczeństwa na posiadanych stacjach roboczych i serwerach. Jednym z etapów migracji było wdrożenie dostarczonego przez usługodawcę oprogramowania pozwalającego na połączenie i synchronizację danych pomiędzy usługą katalogową klienta a bazą użytkowników usługodawcy. Wypracowane rozwiązanie umożliwiało utrzymywanie w firmie i u usługodawcy kopii kont użytkowników, które dzięki synchronizacji posiadały takie same atrybuty, hasła i politykę haseł. Wykorzystanie rozwiązania Microsoft Exchange w chmurze pozwoliło również na wdrożenie centralnie zarządzanych mechanizmów szyfrowania i podpisywania wiadomości pocztowych.

Organizacja po okresie stabilizacji nowych usług pocztowych zaczęła stosować umiejscowiony w chmurze obliczeniowej korporacyjny komunikator elektroniczny. Ze względu na posiadane już rozwiązania firmy Microsoft zdecydowano na wykorzystanie usługi Microsoft Skype. Komunikator miał być używany w celu zagwarantowania wsparcia komunikacji tekstowej, głosowej i wideo w ramach organizacji, ale również w komunikacji z partnerami handlowymi. Pomimo faktu, że usługa jest zaimplementowana w chmurze obliczeniowej, wymaga ona jeszcze poprawnej konfiguracji do funkcjonowania. W przypadku programu Skype do nawiązywania i utrzymywania konwersacji jest wykorzystywany protokół SIP (Session Initiation Protocol), a komunikacja z zewnętrznymi partnerami jest możliwa często dzięki dodatkowej konfiguracji po obu stronach (wymagana jest konfiguracja tzw. federacji). Konieczność wymiany konfiguracyjnych z partnerami i ustalenie wspólnych kroków, które powinny zostać podjęte, sprawiała najwięcej problemu w tej fazie wdrożenia usług chmurowych.

Firma dodatkowo przeniosła do chmury obliczeniowej mniejsze aplikacje nieposiadające kluczowego znaczenia dla organizacji – taka operacja była przeprowadzana najczęściej w trakcie porządkowania posiadanych zasobów IT. Ze względów bezpieczeństwa dostęp do aplikacji w chmurze był możliwy jedynie z lokalnych zasobów IR organizacji poprzez zbudowany tunel sieciowy VPN (Virtual Private Networking).

Ze względu na problemy komunikacyjne pomiędzy siedzibą główną a tą zlokalizowaną w USA, badana organizacja zaczęła analizować możliwość wykorzystania zasobów chmurowych umiejscowionych na kontynencie amerykańskim do innych usług IT, takich jak: zasoby plikowe, bazy danych czy usługi terminalowe. Ze względu na posiadaną infrastrukturę i doświadczenie z usługami Microsoft w chmurze obliczeniowej zdecydowano się na wykorzystanie platformy oferowanej przez Microsoft Azure. W ramach testów przeprowadzono konfigurację wszystkich pożądanych usług w chmurze, a także możliwość integracji mechanizmów zabezpieczeń z już wdrożonymi procedurami i usługami. W wyniku testów pojawiły się liczne bariery, przez które decyzja o migracji do Microsoft Azure została chwilowo wstrzymana; były to m.in.:

1. Mała różnorodność dostępnych w standardowych komponentach sieciowych możliwości implementacji tuneli. VPN oferowany przez Azure dawał jeden – najprostszy z możliwych – sposób uwierzytelniania tunelu.
2. Trudności z podjęciem decyzji co do modelu wdrożenia usług katalogowych w Microsoft Azure i potencjalnej synchronizacji lub całkowitej integracji usług odpowiedzialnych za uwierzytelnianie zlokalizowanych w siedzibie organizacji i w chmurze. Dodatkowym utrudnieniem była już istniejąca synchronizacja tożsamości z usługodawcą, oferująca rozwiązanie pocztowe. Brano pod uwagę rozwiązanie z wykorzystaniem DIY AD DS (Do-It-Yourself Active Directory Domain Services), która jest opcją najbardziej zbliżoną do dobrze poznanych, tradycyjnych rozwiązań, ale jest też rozwiązaniem oferującym na wejściu najmniejszą integrację z usługami chmurowymi.
3. Konieczność korzystania ze wsparcia zewnętrznych specjalistów IT przy wdrażaniu testowego rozwiązania. Dział IT organizacji nigdy nie pracował w chmurze Azure i posiadana wiedza nie wystarczała do przeprowadzenia często bardzo prostych operacji, a tym bardziej do dobrego zaprojektowania całej infrastruktury z wykorzystaniem zasobów Microsoft Azure.
4. Problem z podjęciem decyzji o sposobie udostępniania zasobów plikowych. Chmura Azure oferuje wiele usług magazynowania danych (np. plik, dysk, blob, kolejka, tabela, archiwum), a każdy z nich charakteryzuje się innymi cechami co do sposobu kontroli dostępu do danych, udostępnienia zasobu użytkownikowi, uwierzytelnienia, funkcjonalności. Część z nich jest też rzadko spotykana w tradycyjnych infrastrukturach IT on-premise.
5. Trudny do właściwego zaplanowania realny koszt usług w chmurze bez posiadania doświadczenia w tej dziedzinie.

6. Wiele z usług przeznaczonych do monitorowania i zapewniania poziomu bezpieczeństwa okazało się usługami płatnymi z osobnym sposobem naliczania należności za wykorzystanie usługi.

W trakcie testów udało się przeprowadzić wszystkie zaplanowane prace, ale wypracowane rozwiązania sprowadzały się właściwie do wykorzystania warstwy IaaS (Infrastructure as a Service) chmury i do uruchomienia oraz skonfigurowania maszyn wirtualnych w chmurze. Wybrano znane i sprawdzone rozwiązanie, które pozwala na wykorzystanie posiadanej już wiedzy i doświadczenia bez konieczności eksplorowania nowych zagadnień.

Pomimo wyboru usługodawcy, oferującego rozwiązania wywodzące się z rodziny produktów znanych w omawianej organizacji, szeroka gama usług sieciowych, tożsamości i monitorowania nie zostały wykorzystane na obecnym etapie. Organizacja była skłonna przenieść więcej funkcjonalności do chmury, co mogło spowodować zwiększenie funkcjonalności usług w chmurze i potencjalnie zmniejszenie kosztów ich wykorzystania poprzez przejście z poziomu IaaS na SaaS, ale uniemożliwił to brak odpowiednich kompetencji w organizacji.

2.2. Studium przypadku II

Drugą badaną organizacją była duża firma z branży finansowej, posiadająca dwie siedziby skupiające większość pracowników. Pozostała część zatrudnionych charakteryzuje się dużą mobilnością związaną z pracą w terenie.

Ze względu na potrzebę obsługi ponad 900 pracowników firma posiada dział IT zatrudniający 60 osób, którzy większość czasu poświęcają na bieżące rozwiązywanie problemów użytkowników (helpdesk) i utrzymanie funkcjonowania istniejących systemów informatycznych. Dodatkowo dział IT rozwija własne aplikacje, mające na celu m.in. analizę danych i raportowanie oraz udostępnianie poprzez web rozwiązań typu B2B i B2C. Organizacja posiada bogate zaplecze serwerowe, niezbędne do utrzymania serwerów zarządzania infrastrukturą (domena Active Directory), serwerów baz danych, WWW i serwerów pocztowych – jest jednak już przestarzała pod względem bazy sprzętowej oraz warstwy wirtualizacji i nie jest możliwa prosta relokacja zasobów pomiędzy usługami.

W 2015 r. organizacja pierwszy raz sięgnęła w stronę usług chmurowych w celu usprawnienia procesu komunikacyjnego w organizacji. Ze względu na dużą mobilność znacznej części pracowników i potrzebę obsługi dużej ilości urządzeń przenośnych zdecydowano się na obsługę komunikacji elektronicznej

przy pomocy ulokowanych w polskiej chmurze obliczeniowej usług Microsoft Exchange i Skype.

Jednym z priorytetów organizacji było nadzorowanie komunikacji wpływającej i wypływającej oraz kontrola nad poziomem zabezpieczeń każdego urządzenia, które wykorzystywało zasoby pocztowe. Wybór usługi Exchange pozwolił w pierwszym etapie na wymuszanie na urządzeniach mobilnych zasad bezpieczeństwa odnośnie do możliwości korzystania z funkcji telefonów (np. podłączania kart pamięci, ustawiania zasady haseł, wykorzystania aparatu fotograficznego, zasad wykorzystania wifi) oraz umożliwił zdalną kontrolę nad telefonem (np. wymuszenie powrotu do ustawień fabrycznych) w sytuacji np. kradzieży.

Potrzeba monitorowania przychodzących i wychodzących wiadomości pocztowych wraz z wykorzystaniem funkcjonalności poczty Exchange zaowocowała wdrożeniem dodatkowych mechanizmów zabezpieczenia poczty elektronicznej poprzez:

- tworzenie z poziomu serwera kopii każdej przychodzącej i wychodzącej wiadomości pocztowej,
- wymuszanie przekazywania do moderacji wychodzących wiadomości pocztowych zawierających pewne zadeklarowane wzorce znaków odpowiadających, np. numery kont bankowych lub dowodów osobistych,
- możliwość podpisywania i szyfrowania wiadomości poczty elektronicznej,
- uniemożliwienie trwałego usuwania poczty elektronicznej przez użytkowników,
- raportowanie wysyłanych i odbieranych wiadomości,
- ograniczenie dostępnych protokołów połączeniowych.

W trakcie pracy z zasobami w chmurze zmodyfikowano i uszczegółowiono obowiązujące polityki bezpieczeństwa, opierając się na literaturze i zebranych doświadczeniach, co pozwoliło na utrzymanie restrykcyjnych zasad dotyczących bezpieczeństwa (polityka haseł, kontrola dostępu do danych, monitorowanie aktywności użytkowników).

Zebrane przez dwa lata doświadczenia z wykorzystaniem chmury obliczeniowej uznano za satysfakcjonujące i postanowiono w większym stopniu oprzeć na niej własne systemy informatyczne.

Główne funkcjonalności, które miały być w drugim kroku przeniesione do chmury, to środowisko deweloperskie (serwery bazodanowe, usługi zarządzania projektami programistycznymi, serwery WWW), magazyny kopii zapasowych i archiwa danych, usługi analizy danych oraz produkcyjne platformy webowe B2B i B2C. Jako platformę docelową wytypowano środowisko Microsoft Azure. Dla ujednolicenia i uproszczenia mechanizmów autoryzacji zdecydowano się na

migrację wykorzystywanych rozwiązań komunikacyjnych (Exchange i Skype) również na platformę Microsoft Office 365.

W odróżnieniu od firmy opisywanej w pierwszym studium przypadku, organizacja mogła sobie pozwolić na wydelegowanie z działu IT zespołu osób odpowiedzialnych za proces projektowania i wdrożenia usług w Microsoft Azure. Grupa pięciu pracowników została również przeszkolona w certyfikowanym ośrodku szkoleniowym w zakresie zarządzania chmurą Azure. Ponadto Organizacja uzyskała silne wsparcie zewnętrzne w procesie projektowania infrastruktury zintegrowanej z Azure i planowania procesu transferu zasobów do chmury.

Lepsza znajomość środowiska chmurowego i chęć łatwiejszej integracji aplikacji ze środowiskiem chmurowym wpłynęły na wybór modelu usług katalogowych wykorzystanych w chmurze. Wybór rozwiązania hybrydowego pozwolił na łatwiejsze tworzenie aplikacji w chmurze z jednoczesnym pozostawieniem istniejących w organizacji rozwiązań odpowiedzialnych za uwierzytelnianie.

Do wyzwań, które stanęły przed organizacją, można zaliczyć m.in.:

- zweryfikowanie stanu prawnego dotyczącego możliwości składowania danych w chmurze i spełnienie wymagań odnoszących się do przetwarzania danych stawianych przez GIODO,
- integracja posiadanego systemu uwierzytelniania z systemem oferowanym przez usługodawcę dla zagwarantowania spójnego systemu logowania,
- zaprojektowanie procesu migracji danych użytkowników do chmury obliczeniowej i opracowanie harmonogramu migracji,
- konieczność adaptacji posiadanych aplikacji web do środowiska chmury obliczeniowej,
- przystosowanie do całkowicie nowego mechanizmu rozliczania licencji – w przypadku prostych usług Office 365 sytuacja jest bardzo klarowna; w przypadku infrastruktury serwerowej i własnych aplikacji web migracja aplikacji do chmury wymagała również opracowania i modyfikacji komponentów aplikacji pod względem sposobu rozliczania licencji.

Organizacja zaimplementowała oraz zintegrowała z posiadanymi zasobami ICT zaawansowane usługi chmurowe – również te związane z bezpieczeństwem. W znaczący sposób poszerzyło to możliwości monitorowania wszelkich procesów związanych z komunikacją elektroniczną w organizacji, a także pomogło spełnić wymagania odnośnie do konieczności ich archiwizacji i audytu. Wysokie kompetencje pozwoliły na szczegółowe zaplanowanie procesu migracji oraz dokładną analizę wątpliwości związanych z bezpieczeństwem przetwarzania danych w chmurze.

Podsumowanie

Chmura obliczeniowa jest często postrzegana jako ciekawa alternatywa dla tradycyjnego modelu przetwarzania danych, opartego na własnych zasobach. Potencjalne korzyści z jej wykorzystania przeciwstawia się wątpliwościom i obawom z nią związanym. Dostawcy chmury obliczeniowej poprzez odpowiednią konstrukcję paneli zarządzania starają się ją przedstawić jako środowisko maksymalnie przyjazne i proste, ale w rzeczywistości jest to bardzo skomplikowana konstrukcja, która w wielu aspektach znacząco różni się od dobrze poznanych tradycyjnych rozwiązań.

Przedstawione w artykule przykłady nie potwierdzają wszystkich obaw związanych z adaptacją chmury obliczeniowej w organizacji. Obawa przed powierzeniem swoich zasobów zewnętrznemu usługodawcy we współdzielonym środowisku nie jest już głównym elementem blokującym wdrożenia chmurowe (stanowi natomiast obiekt analizy, oszacowania ryzyka i dokładnego projektowania); również kwestie legislacyjne nie są tu dużą przeszkodą. Usługodawcy usług chmurowych dzięki posiadanym zasobom mogą łatwiej dostosować się do zmieniającego się prawa i adaptować swoje usługi do nowej rzeczywistości prawnej. Wdrożenia przeprowadzone w omawianych organizacjach pokazują również, że poprawne i bezpieczne wykorzystanie zasobów chmurowych wymaga zdobycia nowych umiejętności oraz znacznego poszerzenia horyzontów dotyczących rozwiązań IT. Wykorzystanie w chmurze nowych technologii, protokołów i architektur może stanowić znaczącą barierę przed prawidłowym zaprojektowaniem infrastruktury IT, ale oznacza też bardzo duże poszerzenie możliwości wykorzystania usług w organizacji.

Literatura

Andriole S. (2018), *Skills and Competencies for Digital Transformation*, "IT Professional", Vol. 20(6), s. 78-81.

Avram M. (2014), *Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective*, "Procedia Technology", Vol. 12, s. 529-534.

Cattaneo G. (2014), *The Demand of Cloud Computing in Europe: Drivers, Barriers, Market Estimates*, http://cordis.europa.eu/fp7/ict/ssai/docs/future-cc-2may-gcattaneo-presentation.pdf (dostęp: 10.10.2017).

Durao F., Carvalho J.F.S., Fonseka A., Garcia V.C. (2014), *A Systematic Review on Cloud Computing*, "The Journal of Supercomputing", Vol. 68(3), s. 1321-1346.

Ghazizadeh E., Zamani M., Ab Manan J., Pashang A. (2013), *A Survey on Security Issues of Federated Identity in the Cloud Computing*, 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings, 3-6 December.

Mogull R., Arlen J., Gilbert F., Lane A., Mortman D., Peterson G., Rothman M. (2017), *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*, Cloud Security Alliance, https://cloudsecurityalliance.org/download/security-guidance-v4/ (dostęp: 10.10.2017).

Phaphoom N., Wang X., Samuel S., Helmer S., Abrahamsson P. (2015), *A Survey Study on Major Technical Barriers Affecting the Decision to Adopt Cloud Services*, "The Journal of Systems and Software", Vol. 103, s. 167-181.

Podgórski G. (2016), *Strategie mobilności użytkowników w środowisku IT*, „Studia Ekonomiczne Regionu Łódzkiego", nr 23, s. 137-147.

Zwattendorfer B., Stranacher K., Tauber A. (2013), *Towards a Federated Identity as a Service Model* [w:] Kő A., Leitner C., Leitold H., Prosser A. (eds.), *Technology-Enabled Innovation for Democracy, Government and Governance*, Proceedings of Second Joint International Conference on Electronic Government and the Information Systems Perspective, and Electronic Democracy, EGOVIS/EDEM 2013, Prague, Czech Republic, August 26-28, s. 43-57.

[www 1] https://cloudsecurityalliance.org/group/cloud-controls-matrix/ (dostęp: 10.10.2017).

[www 2] https://www.netmarketshare.com/operating-system-market-share.aspx (dostęp: 1.10.2017).

SECURITY IN THE CLOUD VS TRADITIONAL SECURITY – CASE STUDIES

Summary: Cloud computing for several years has been building a strong alternative position for on-premise solutions in terms of the scope of functionality and cost accounting. One of the main doubts in the implementation of cloud solutions, however, remains the space regarding information security issues. The article emphasizes doubts regarding the integration of cloud authentication services, and the correct implementation of information security solutions as a result of the projection of standard solutions for cloud computing based on case studies.

Keywords: cloud computing, authentication, security.