Rzeczpospolita, 2015-02-17

Wojciech Cellary
Maciej Gawroński

Chmura z problemami

W artykule opublikowanym 13 stycznia przedstawiliśmy strategiczne znaczenie przetwarzania w chmurze dla sektora publicznego. Przypomnijmy, że przetwarzanie w chmurze (ang. *cloud computing*) jest modelem biznesowym oferowania sprzętu i oprogramowania na żądanie przez internet za opłatą proporcjonalną do użytkowania. Wykazaliśmy, że dzięki zastosowaniu przetwarzania w chmurze luka pomiędzy najbardziej i najmniej zaawansowanymi regionami w Polsce ulegnie zmniejszeniu, co uaktywni potencjał zamrożony w gorzej rozwiniętych regionach i przyspieszy rozpowszechnianie innowacji z korzyścią dla rozwoju kraju. Z tego względu, wdrożenie przetwarzania w chmurze w sektorze publicznym jest pożądane.

Jak każde rozwiązanie techniczno-organizacyjne, również chmura nie jest wolna od zagrożeń. Celem tego artykułu jest ich przedstawienie tak, aby wdrażając chmurę być świadomym jej uwarunkowań i móc ograniczyć związane z nimi ryzyko.

Poufność danych – ryzyko systemowe

Największym strategicznym wyzwaniem scentralizowanego przetwarzania danych, jakim obecnie jest przetwarzanie w chmurze, wydaje się zapewnienie poufności danych i e-prywatności obywateli.

Instytucje sektora publicznego przechowują ogromne ilości poufnych danych dotyczących zarówno obywateli, jak i przedsiębiorstw, które z mocy prawa są zobowiązane chronić. Odpowiednie dane są oczywiście objęte tajemnicą bankową, skarbową, handlową, medyczną, adwokacką, prokuratorską itd. Umieszczenie tych danych w chmurze nie znosi odpowiedzialności tych instytucji za zapewnienie ich poufności, ani odpowiedzialności osób, które mają dostęp do tych danych (w tym dostawcy chmury i jego personelu) za naruszenie ich poufności.

Niezależnie jednak od prawnych sankcji za naruszenie zasad dostępu do danych poufnych, centralizacja przechowywania i przetwarzania takich danych rodzi specyficzne ryzyko systemowe. Ryzyko, że ktoś mający możliwość naruszenia poufności i akceptując ewentualne konsekwencje w przypadku wykrycia, wyrządzi niepowetowane straty. Oczywiście, zawsze występuje ryzyko, że osoba mająca w systemie dostęp do konkretnych danych, z tych czy innych przyczyn (przekupstwo, szantaż, ideały, prywata) nadużyje swoich uprawnień. Ryzykiem specyficznym dla chmury może być jednak to, że firma obsługująca daną chmurę zdecyduje na poziomie własnej egzekutywy sprzeniewierzyć powierzone jej dane i wykorzystać je do własnych celów.

Odpowiedzią na ten problem może być wymóg "wbudowanej prywatności" (*privacy by design*), który zostanie wprowadzony tzw. Rozporządzeniem UE o ochronie danych osobowych (Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych), którego uchwalenie jest planowane na rok 2015/2016 a wejście w życie na 2017/2018. Jak wiadomo, wymóg ten może być spełniony przez odpowiednią architekturę chmury. Rozporządzenie UE o ochronie danych osobowych przewiduje nowe gwarancje ochrony danych osobowych, w tym ocenę skutków w zakresie ochrony prywatności danych (*'data protection impact assessment'*). Co to oznacza w praktyce? Instytucje przed rozpoczęciem operacji wykorzystania niektórych danych osobowych, w tym danych w środowisku internetowym, będą musiały dokonać analizy ryzyka związanego z potencjalnych wpływem takich operacji na prawa i wolności podmiotów danych. Dostawcy chmury będą musieli zmierzyć się z taką oceną. Oznacza to wprowadzenie prawnych gwarancji, dzięki którym zaufanie do rozwiązań chmurowych wzrośnie.

Z drugiej strony, patrząc z perspektywy bezpieczeństwa operacyjnego, warto zauważyć, że poprawnie zaprojektowane i wdrożone rozwiązania pracujące w chmurze mogą charakteryzować się wyższym poziomem bezpieczeństwa przy jednoczesnych niższych kosztach. W przypadku chmur publicznych działa tutaj między innym efekt skali. Wyższy poziom bezpieczeństwa przy niższych kosztach nawet biorąc pod uwagę tylko spełnienie wymogów prawnych w obszarze ochrony danych osobowych jest niezwykle atrakcyjnym rozwiązaniem dla administracji publicznej i samorządowej

Kontrola dostępu danych

Kolejny istotnym zagadnieniem, na które należy zwrócić uwagę w debacie nad bezpieczeństwem powierzenia przetwarzania danych do zewnętrznego dostawcy usługi w chmurze, jest aspekt kontroli dostępu do danych. W praktyce nie ma dzisiaj organizacji, która zapewnia, że dostęp do danych jest w 100% realizowany tylko przez jej pracowników. Przecież dostęp mają też serwisanci, wsparcie techniczne dla wybranych aplikacji i systemów, zewnętrzni administratorzy w ramach umów outsourcingowych, a dane często ze względu na koszty są przesyłane publicznymi łączami. Jeśli z tej perspektywy spojrzymy na problem kontroli dostępu, szybko okazuje się, że w przypadku dostawcy usługi w chmurze kontrola jego działań i poziomu bezpieczeństwa oferowanego przez niego jest niejednokrotnie łatwiejsza oraz efektywniejsza niż w przypadku bardziej tradycyjnych modeli informatycznych.

W każdym jednak przypadku państwo powinno ocenić i zdecydować, komu powierzy kontrolę nad konkretnymi kategoriami danych, które zamierza umieścić w chmurze. Jakie to będą instytucje lub firmy, gdzie będą położone ich serwery i centra przetwarzania danych, jaką można będzie sprawować kontrolę nad kierownictwem i personelem operatora konkretnej chmury. Państwo powinno też rozważyć, czy pewne kategorie danych nie powinny być przetwarzane wyłącznie pod pełną kontrolą służb państwowych – to jest bez udziału sektora prywatnego. Należy rozważyć utworzenie

Prywatnej Chmury Sektora Publicznego, w której będą przechowywane i przetwarzane poufne dane z sektora publicznego objęte różnymi tajemnicami.

Terytorialność

Z punktu widzenia bezpieczeństwa państwa, ryzykiem jest także ułatwienie fizycznego dostępu do danych "państwowo istotnych" obcym służbom i instytucjom. Za takie ułatwienie można uważać na przykład umieszczenie danych na serwerach za granicą. Stąd decyzja o przekazaniu do chmury międzynarodowej poszczególnych kategorii informacji powinna zostać podjęta z rozwagą.

Warto jednak spostrzec, że w dobie zdalnego dostępu do e-usług, w szczególności do e-usług administracji, atak może być dokonany z dowolnego miejsca na świecie – tak jak (domniemany) rosyjski atak hakerski na e-usługi państwa estońskiego. Stąd utrzymywanie danych na własnym terytorium może okazać się tylko pozornie bezpieczne.

Co więcej, utrzymywanie danych strategicznych na własnym terytorium również może rodzić ryzyka. Estonia podjęła decyzję o zabezpieczeniu danych poza swoimi granicami, z obawy przed rosyjską agresją terytorialną. Przekazanie danych za granicę może więc nie tylko generować ryzyko, ale je mitygować.

Certyfikacja

Największym problemem na przeszkodzie szerokiemu biznesowemu wykorzystaniu przetwarzania w chmurze jest brak zaufania. Chmura może oferować najwyższy poziom bezpieczeństwa, jednak gdy klient nie jest pewny tego bezpieczeństwa, samemu zwykle nie znając się na tym, niechętnie podejmie decyzję związaną z nieznanym mu poziomem ryzyka. Problemem jest więc zaufanie co do bezpieczeństwa. Rozwiązanie tego problemu jest znane od dziesięcioleci, jednak teraz dopiero zyskuje drastycznie na popularności. Jest nim korzystanie z brokerów zaufania, czyli z certyfikacji bezpieczeństwa.

Laicy nie wiedzą, co to znaczy "bezpiecznie". Bezpieczeństwo informacji jest jednak dziedziną zasadniczo opanowaną, w której obowiązują reguły znane specjalistom. Reguły te zostały ujęte między innymi w rodzinie norm ISO 27000. W tym w normie ISO/IEC 27001:2013 Technika informatyczna – Techniki bezpieczeństwa – System Zarządzania Bezpieczeństwem Informacji – Wymagania oraz ostatnio uzgodnionej normie ISO/IEC 27018:2014 *Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*[1], dotyczącej bezpieczeństwa danych osobowych w chmurze.

Stąd rozsądne jest promowanie i poleganie na standardach w dziedzinie bezpieczeństwa informacji. Standaryzacja i certyfikacja jako odpowiedź na problemy bezpieczeństwa informacji i zaufania do bezpieczeństwa jest już stosowana w

[1] Nie powstała jeszcze polska wersja tej normy. Tłumaczenie robocze: "Technika Informacyjna – Techniki bezpieczeństwa – Kodeks dobrych praktyk ochrony informacji identyfikującej osoby (IIO) w publicznych chmurach obliczeniowych działających jako przetwarzający IIO"

polskim[2] i unijnym[3] prawie. Projektowane przepisy wykonawcze do zmienionej ustawy o ochronie danych osobowych również odwołują się do norm ISO.

Cyfrowe ekspertyzy kryminalistyczne Z problemem monitorowania wiąże się również problem wspomagania cyfrowych ekspertyz kryminalistycznych (ang. *computer forensic*). Celem takiej ekspertyzy, jako części składowej reakcji na naruszenie bezpieczeństwa, jest:

- rozpoznanie, co się stało;
- zrozumienie, która część systemu uległa atakowi;
- opracowanie zabezpieczenia przed przeprowadzonym atakiem; oraz
- zebranie dowodów potrzebnych w postępowaniu sądowym.

Wszystkie te czynności są po stronie dostawcy chmury, pomimo, że poszkodowanymi są instytucje przechowujące dane w chmurze, a w konsekwencji ich interesariusze – obywatele i przedsiębiorstwa.

Zatem oczekiwać należałoby od dostawcy chmury, że zapewni spolegliwe i wiarygodne rozwiązanie systemowe zagadnienia zebrania, utrwalenia i analizy zdarzeń operacyjnych, które mogą wystąpić w oferowanym przez niego rozwiązaniu/produkcie.

Przepustowość sieci

Szerokie wdrożenie przetwarzania w chmurze wymaga pewnie działającego, niezawodnego i bezpiecznego internetu. Jeśli zawiedzie internet, to wszystkie instytucje przechowujące i przetwarzające dane w chmurze zostaną unieruchomione. W dostępie do internetu mamy na szczęście do czynienia z szybkim postępem. W „Agendzie cyfrowej dla Europy", która Polskę obowiązuje, znajduje się wymaganie zapewnienia do 2020 r. wszystkim obywatelom Unii Europejskiej dostępu do internetu o przepustowości przekraczającej 30 Mb/s, a przynajmniej połowie gospodarstw domowych – przekraczającej 100 Mb/s. Aktualnie w Polsce blisko 76% aktywnych łączy pozwala na transmisję do użytkownika z prędkością nie większą niż 10Mb/s, a tylko 4% umożliwia dostęp powyżej 30Mb/s W programie operacyjnym „Polska Cyfrowa" na lata 2014-2020, który jest już zatwierdzony przez Komisję Europejską, zakłada się dalszy rozwój szerokopasmowego internetu.

Uzależnienie od dostawcy i migracja

Jednym z dostrzeganych problemów wykorzystania chmury jest kłopot ze zmianą dostawcy. Eksport danych sam w sobie nie jest zagadnieniem trywialnym, może powstać problem zgodności formatów danych, problem z eksportem konfiguracji i ustawień, problem związany z wolumenem (wielkością danych do przeniesienia) –

[2] § 20 ust. 3 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

[3] Pkt 3.B Załącznika I do Rozporządzenia delegowanego Komisji (UE) NR 907/2014 z dnia 11 marca 2014 r. uzupełniającego rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1306/2013 w odniesieniu do agencji płatniczych i innych organów, zarządzania finansami, rozliczania rachunków, zabezpieczeń oraz stosowania euro

względem przepustowości interfejsów poszczególnych systemów oraz przepustowości samych łączy internetowych. Sytuacja komplikuje się dalej, jeśli przenoszone miałyby być wirtualne serwery. Instytucje publiczne winny zwrócić szczególną uwagę na kontraktowe i praktyczne zagadnienia uzależnienia od dostawcy i "wyjścia" z jego chmury / migracji do innego środowiska.

Problem przenoszalności danych dostrzegła Grupa Ekspercka Komisji Europejskiej ds. Kontraktów Przetwarzania w chmurze, gdzie współautor tego artykułu (MG) opracował raport i propozycje rozwiązań tego zagadnienia.

Podsumowanie

Jak wynika z tego krótkiego zestawienia, chmura obliczeniowa będąc potencjalnym rozwiązaniem wielu problemów informatyzacji państwa i udostępnienia e-usług administracji, posiada jednak specyficzne uwarunkowania strategiczne i operacyjne. Przejścia w chmurę obliczeniową należy więc dokonać twardo stąpając po ziemi.

prof. dr hab. inż. Wojciech Cellary, Uniwersytet Ekonomiczny w Poznaniu, Katedra Technologii Informacyjnych

radca prawny Maciej Gawroński, partner zarządzający w warszawskim biurze Bird & Bird, kieruje praktyką IT