

Bezpieczeństwo danych w chmurze: Dane przesyłane są do USA? Nie wiadomo

autor: **Tomasz Jurczak** 18.10.2015, 19:00



VMworld 2015 dobiegł końca. Zainteresowanie wykorzystanie cloud computingu rośnie. Pytanie pozostaje jednak aktualne – czy dane w chmurze obliczeniowej są bezpieczne? Zapytaliśmy ekspertów z zakresu danych osobowych jak i obszaru cyber security ile w tym zagrożeniu jest prawdy.

Chmura obliczeniowa – bezpieczna czy nie?

Podczas wydarzenia VMworld2015, organizator eventu, firma VMware Inc. zaprezentowała innowacje w obszarze jednolitej platformy chmury hybrydowej. Jak informuje firma, nowe usługi w chmurze publicznej VMware i umożliwią klientom szybsze tworzenie aplikacji, podniesienie poziomu bezpieczeństwa systemów IT, szybkie przywracanie usług po awariach oraz generowanie rzeczywistej wartości dodanej dla firmy.

Wiele osób zadaje sobie jednak pytanie czy korzystanie z rozwiązań w chmurze jest bezpieczne. W zasadzie odpowiedź zależy od tego, czy firma wybrała dla swoich potrzeb odpowiedni model chmury. Chmura prywatna pozwala mieć pełną kontrolę nad zasobami, publiczna (u poważnego providera) jest dostępna natychmiast, ułatwia rozliczanie kosztów i zapewnia wysokiej jakości backup i high availability, które wiąże się zazwyczaj z inwestycjami i czasem wymagany na wdrożenie w chmurze prywatnej. Ciekawy wydaje się zatem model chmury hybrydowej łączący zalety obu rozwiązań. Jednak jak twierdzą eksperci każde z tych rozwiązań na swój sposób jest bezpieczne. Przedstawiciele VMware zapewniają, że rozwiązania chmurowe są bezpieczne, choć zauważają, że wiele firm aby w pełni chronić

dane wrażliwe lub krytyczne dla biznesu, decyduje się na umieszczenie ich w chmurze prywatnej.

W przypadku publicznej chmury usługi i infrastruktura znajdują się poza firmą i to jest największym zarzutem wobec wykorzystania tego rozwiązania. Tymczasem dane w chmurze prywatnej chronione są za firewallem, a firma wykorzystuje własne zasoby IT do ich przechowywania. Zatem chmura hybrydowa łączy plusy obu rozwiązań, jednocześnie niwelując zagrożenie.

Temat jednak nie jest jednoznaczny, a cloud computingiem coraz częściej interesują się organy zajmujące się ochroną danych osobowych oraz regulatorzy, w przypadku np. banków, które korzystają z tych rozwiązań. W szczególności najważniejszym pytaniem pozostaje, czy nasze dane nie są przesyłane np. do USA.

Firmy muszą wykazać, co z tymi danymi się dzieje

Na początek warto zaznaczyć, że nie ma żadnego generalnego zakazu, który uniemożliwiałby przetwarzanie danych osobowych w chmurze. Istotne przy tym jest jednak to, jakie działania trzeba podjąć, żeby zachować wszystkie zasady ochrony danych osobowych, które wynikają z ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz z rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Poprosiliśmy Generalnego Inspektora Danych Osobowych o komentarz w tej sprawie:



dr Edyta Bielak-Jomaa, GODO

Można przetwarzać dane w chmurze, ale musimy wiedzieć gdzie ma to miejsce

Wskazać należy, że ustawa o ochronie danych osobowych zobowiązuje administratora danych do dbałości o bezpieczeństwo danych osobowych, a przepisy jej rozdziału 5 określają ogólne zasady ich zabezpieczania. Zgodnie z art. 36 ust. 1 tej ustawy, administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Wybór odpowiednich środków gwarantujących przetwarzanym danym optymalny stopień zabezpieczenia pozostawia jednak do uznania konkretnemu administratorowi danych osobowych. Obowiązki te nie ulegają w żadnym stopniu ograniczeniom w związku z wybranym modelem biznesowym, jakim jest cloud computing.

Z punktu widzenia obowiązujących przepisów, przetwarzanie danych, zwłaszcza danych osobowych w chmurze obliczeniowej, może nastąpić tylko wtedy, jeżeli ten, kto przekazuje dane (użytkownik chmury) będzie w stanie ustalić, w których centrach przetwarzania (tzn. gdzie umieszczonych) dane te będą przetwarzane.

Część dostawców chmur zapewnia użytkowników, że dane osobowe będą przetwarzane tylko w centrach znajdujących się na terenie Unii Europejskiej, co ma oznaczać, że dane osobowe nie będą przekazywane do tzw. krajów trzecich, o których mowa w ustawie o ochronie danych osobowych. Wydawać by się zatem mogło, że zapewniony będzie wystarczający poziom ochrony tych danych. Lecz niestety, tylko może się tak wydawać. Bowiem problemem, niezmiernie trudnym do rozwiązania, jest to, że umowa o przetwarzanie danych w chmurze, powinna być umową powierzenia przetwarzania danych w rozumieniu art. 31 ustawy o ochronie danych osobowych.

Zgodnie bowiem z tym przepisem, administrator danych może powierzyć innemu podmiotowi przetwarzanie danych, ale muszą być spełnione określone w ustawie warunki. Umowa musi być zawarta na piśmie, określać zakres powierzonych danych i cel ich przetwarzania. Podmiot, któremu administrator powierzył w ten sposób przetwarzanie danych osobowych, może je wykorzystywać wyłącznie w zakresie i celu wskazanym w tej umowie. Za prawidłowe przetwarzanie powierzonych danych osobowych, w tym ich właściwe zabezpieczenie, odpowiada administrator danych, co jednak nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.

Skonstruowanie takiej umowy z dostawcą chmury może być skomplikowane m.in. z tego powodu, że powinna ona przewidywać, przy użyciu jakich środków dane będą zabezpieczane. Musimy więc uzyskać bardzo dokładną informację na ten temat, a to w przypadku klasycznej chmury publicznej – niemającej ograniczeń co do terytorium ani co do podmiotu czy podmiotów, w których władaniu pozostają środki techniczne (serwery służące przetwarzaniu danych), może być bardzo trudne. Natomiast w przypadku chmur, w ten czy inny sposób dedykowanych danemu użytkownikowi – jak najbardziej możliwe, ale zapewne znacznie droższe.

Kolejna istotna trudność to zapewnienie administratorowi danych osobowych, czyli użytkownikowi chmury, uprawnień kontrolnych jej dostawcy (np. możliwości kontroli jego centrów przetwarzania danych). Zorganizowanie tego typu rozwiązania, zarówno od strony technicznej, jak i od strony czysto biznesowej, byłoby nie takie proste. Dodatkowym aspektem, który warto podnieść, jest przetwarzanie w chmurach informacji objętych tajemnicami prawnie chronionymi (np. informacji niejawnej), gdzie jej „eksport” do centrów obliczeniowych poza terenem Polski może być prawnie zabroniony.

Jednocześnie informuję, że kwestia przetwarzania danych w chmurze jest przedmiotem zainteresowania Generalnego Inspektora Ochrony Danych Osobowych, który z myślą o instytucjach publicznych przygotował „Dekalog chmuroluba” (dostępny pod linkiem http://www.giodo.gov.pl/259/id_art/6271/j/pl). Niemniej może być on również przydatny dla podmiotów spoza tej sfery.

UE nie ma złudzeń – zagrożenie dla konsumentów wzrasta

Kwestie cloud computingu analizuje też Komisja Europejska, która 4 listopada 2010 r. przyjęła kompleksową strategię dotyczącą ochrony danych osobowych w Unii Europejskiej

(komunikat KOM (2010) 609/3). Zakłada ona modernizację istniejących na poziomie Unii Europejskiej (UE) ram prawnych w zakresie ochrony danych osobowych i uwzględnienie w nich uregulowań prawnych związanych z rozwojem nowych technologii. Komisja stwierdza w nim, że „Cloud computing – tzn. przetwarzanie dokonywane w Internecie przy pomocy oprogramowania, dzielonych zasobów i informacji znajdujących się na zewnętrznych serwerach („w chmurze”) stanowi wyzwanie dla ochrony danych, ponieważ wiąże się z utratą przez jednostki kontroli nad ich potencjalnie poufnymi informacjami w sytuacji, w której przechowują one te dane korzystając z programów zainstalowanych na urządzeniach osób trzecich. Niedawno przeprowadzona analiza potwierdziła, że zarówno organy ochrony danych, zrzeszenia przedsiębiorców, jak i organizacje konsumentów są zgodne co do tego, że wzrasta zagrożenie dla prywatności i ochrony danych osobowych w związku z działalnością w Internecie”.

Jak Komisja Europejska postrzega bezpieczeństwo danych w chmurze. Udaliśmy się w tej sprawie do źródła.



Firmy zza oceanu zdobyły przewagę

dr Paweł Litwiński, członek grupy ekspertów Komisji Europejskiej ds. cloud computingu

Usługi świadczone w modelu cloud computingu mają dzisiaj ogromne znaczenie, szczególnie dla małych i średnich przedsiębiorstw oraz konsumentów, którzy masowo korzystają z tego rodzaju usług. Co ciekawe, ogromną przewagę rynkową w świadczeniu tych usług mają pozaeuropejscy dostawcy usług przetwarzania danych w chmurze – wynika ona w dużej mierze z innego podejścia podmiotów spoza Europy do kwestii ochrony danych osobowych. Same umowy o świadczenie tego rodzaju usług najczęściej nie podlegają przy tym negocjacji, zawierane są przez prostą akceptację regulaminu i często nie chronią należycie klienta (wystarczy prosty test: czy wiemy, co się stanie z naszymi danymi będącymi „w chmurze”, gdy dostawca usług zbankrutuje? a co będzie, gdy zapagniemy przenieść się do innego dostawcy – dostaniemy nasze dane z powrotem?).

Tą specyfikę dostrzegła Komisja Europejska, która podjęła inicjatywę opracowania wzorcowych postanowień do umów o świadczenie usług przetwarzania danych w chmurze, które miałyby z jednej strony zapewniać elementarną równowagę kontraktową, a z drugiej – respektować europejskie zasady ochrony danych osobowych. Niestety, prace nie wykazują ostatnio większej dynamiki, a szkoda, bo otoczenie prawne zmienia się bardzo szybko – wystarczy wspomnieć niedawny wyrok Trybunału Sprawiedliwości ze skargi Maxa Schremsa, który wyeliminował porozumienie Safe Harbor spośród instrumentów legalizujących przekazywanie danych osobowych do USA – a to porozumienie właśnie było często wykorzystywane przez dostawców usług cloud computing z USA jako podstawa prawna przekazywania danych do USA.

Trzeba też pamiętać, że poza zabezpieczenia wykorzystywanymi przez rozwiązania chmurowe, ważne jest wykorzystanie właściwych narzędzi bezpieczeństwa. Zapytaliśmy więc firmy zajmujące się obszarem cyber security co myślą o przechowywaniu danych w chmurze. Zdania są jednak podzielone.

Bezpieczeństwo danych w chmurze. Ewentualne ataki na tego typu rozwiązania są możliwe

Radosław Wesolowski z Grey Wizard

Bezpieczeństwo danych w chmurze zależy od wielu czynników, ale poprawnie skonfigurowana usługa z dobrze określoną polityką dostępu do danych i zasobów jest tak samo bezpieczna jak hosting dedykowany. Budując rozwiązania oparte na chmurze publicznej lub prywatnej przede wszystkim należy pamiętać o stosowaniu szyfrowania - zarówno połączeń wykorzystywanych do przesyłania informacji jak i samych danych, takie podejście bardzo ogranicza ryzyko wycieku danych wrażliwych w przypadku ewentualnego włamania. Kolejnym ważnym aspektem jest ustalenie polityki dostępu do danych i nadzór nad jej przestrzeganiem. Szczególnie istotne wydają się być dodatkowe zabezpieczenia takie jak dwu składnikowe uwierzytelnianie czy korzystanie z rozwiązań biometrycznych. Równie istotne są szkolenia pracowników na wypadek prób ataków typu „social engineering” czyli takich, których celem jest uzyskanie niejawnych informacji wykorzystując niewiedzę lub łatwowierność użytkownika, gdyż jak pokazują statystyki większość ataków pochodzi właśnie z wewnątrz firmy. Warto tutaj wspomnieć o konieczności wykonywania cyklicznych audytów bezpieczeństwa i odpowiednim zabezpieczeniu publicznych interfejsów programistycznych (API) w celu ochrony przed atakami typu „brute force”, których celem jest sprawdzenie wszystkich możliwych kombinacji nazwa użytkownika / hasło. Atak tego typu został skutecznie przeprowadzony na chmurę iCloud i spowodował wyciek zdjęć gwiazd. Na koniec należy pamiętać o wdrożeniu bezpiecznych procedur do przechowywania kopii zapasowych danych jak i ochronie przed atakami rozproszonymi typu DDoS.

Dane przechowywane w chmurze są narażone na ataki

Piotr Kupczyk, Kaspersky Lab Polska

Dane przechowywane w chmurze są narażone na ataki, o których nie myślimy zbyt wiele, gdy trzymamy nasze informacje na własnych dyskach wewnątrz firmy, czy w domu. Jednym z takich zagrożeń są ataki DDoS (ang. Distributed Denial of Service), których zadaniem jest zmniejszenie wydajności lub całkowite wstrzymanie usługi dostępnej online. Jeżeli atak taki zostanie wymierzony w infrastrukturę firmy zarządzającej chmurą, z której korzystamy, nasze dane mogą stać się niedostępne przez pewien – czasem nawet dość długi – czas. Co bardzo ważne – działania tego typu często stanowią swego rodzaju zasłonę dymną i towarzyszą im bardziej zaawansowane działania cyberprzestępcze, takie jak kradzież informacji przechowywanych w chmurze. Dlatego tak ważne jest to, by dane – przynajmniej te krytyczne dla funkcjonowania firmy – były przechowywane w chmurze w postaci zaszyfrowanej. Ceny ataków DDoS na czarnym rynku cyberprzestępczym są niebezpiecznie niskie – koszt jednodniowego ataku na infrastrukturę wskazanej firmy to zaledwie 200 dolarów. Istnieją nawet „sklepy”, w których można kupować i sprzedawać całe sieci zainfekowanych komputerów wykorzystywanych do zmasowanego atakowania określonych celów. Należy mieć to na względzie wybierając firmę świadczącą usługi przechowywania danych w chmurze. Warto zwrócić się w stronę organizacji oferujących skuteczną ochronę

przed atakami DDoS, najlepiej taką, która jest w stanie błyskawicznie dostosować się do ciągle ewoluujących technologii wykorzystywanych przez cyberprzestępców.

Michał Jarski, Regional Sales Director CEE, Trend Micro

Bezpieczeństwo chmury nie jest już blokadą

Bezpieczeństwo nie jest już blokadą, która definitywnie uniemożliwia korzystanie z modelu cloud computing. Chociaż dane wychodzą poza firmowe data center i może temu towarzyszyć poczucie, że traci się nad nimi kontrolę, to istnieje rozbudowana gałąź rynku rozwiązań, które potrafią ochronić firmowe zasoby w chmurze. Jeżeli chcemy otworzyć się na wszystkie możliwości i elastyczność, którą daje chmura, musimy zapomnieć jednak o tradycyjnym podejściu do bezpieczeństwa IT.

Chmura zapewnia bardzo dużą dynamikę i elastyczność, a to przekłada się m.in. na bardzo częste tworzenie i wyłączanie serwerów oraz usług. Przy tak zmiennym środowisku bardzo ważne jest to, żeby system bezpieczeństwa pozwalał na zautomatyzowanie jak największej liczby procesów. Możemy spodziewać się, że dostawca usług chmurowych zapewnia ochronę do pewnego poziomu, powinniśmy jednak zostawić część odpowiedzialności w rękach firmy. Warto założyć, że praktycznie każdy z serwerów znajdujących się w serwerowni albo w chmurze potencjalnie jest zainfekowany i może atakować inne maszyny. Dlatego istotne jest rozdzielenie serwerów i traktowanie każdego jako osobnej jednostki.

Źródło: gazetaprawna.pl

Artykuł z dnia: 2015-10-18

Autor: Tomasz Jurczak