Wojciech Rafał Wiewiórowski: Danych osobowych nie przetwarzałbym w chmurze

30.11.2011

Generalny Inspektor Ochrony Danych Osobowych Wojciech Rafał Wiewiórowski uważa, że poziom bezpieczeństwa danych w chmurze jest niewystarczający, by przetwarzać w ten sposób informacje o charakterze danych osobowych. Zastrzegł przy tym, że tradycyjne rozwiązania też nie są całkowicie bezpieczne.

Jak Pan Minister ocenia poziom bezpieczeństwa danych osobistych w chmurze?

Trzeba odróżnić dwie kwestie, jeśli chodzi o dane przetwarzane w chmurze. Pierwsza to zasady bezpieczeństwa danych i ich zabezpieczenia przed „wyciekiem", czyli nieuprawnionym dostępem. Druga to kwestia zakresu dostępu do danych.

Jeśli chodzi o klasyczne bezpieczeństwo danych muszę przyznać, że wbrew pozorom rozwiązania cloudowe mogą być bezpieczniejsze niż tradycyjne. Większość centrów danych jest dobrze zabezpieczona przed atakami z zewnątrz. Poza tym scentralizowane centrum przechowywania danych, nawet jeśli tych centrów jest kilkadziesiąt – oznacza, że jest mniej obszarów, z których może nastąpić wyciek.

Jeśli chodzi o szerzej rozumiane bezpieczeństwo obejmujące również odpowiedź na pytanie, kto legalnie będzie miał dostęp do danych osobowych trzeba omóić znacznie więcej wątpliwości. Trudno jest dziś poprze umowę ograniczyć zakres podmiotów, które będą miały dostęp do danych w chmurze. Co prawda centra danych firmy, które są dostarczycielami usług chmurowych twierdzą, że dane pozostają tylko i wyłącznie pod naszą kontrolą, ale nie mamy możliwości stwierdzenia, czy dostarczyciel chmury nie ingeruje w te dane. W wielu przypadkach nie znamy też obowiązków, jakie ciążą na dostarczycielu chmury, jeśli chodzi o ujawnianie tych danych do organów publicznych (przede wszystkim policji i służbom specjalnym).

Jeśli chodzi o Stany Zjednoczone, skąd pochodzi większość dostarczycieli chmur, służby specjalne mają tam szeroki zakres niekontrolowanego dostępu do baz danych, które są składowane poza terytorium USA i nie zawierają danych obywateli USA. To oznacza, że np. instytucja polska, która przetwarza dane swoich klientów czy użytkowników w chmurze umieszczonej poza terytorium USA, musi zdawać sobie sprawę, że te dane w każdej chwili mogą być przekazane amerykańskim służbom.

Były przykłady takiego skandalu?

O tym, co uzyskały służby specjalne z reguły się nie dowiadujemy. Ale niektóre firmy potwierdzają, że w razie tego typu zgłoszenia służb specjalnych, musiały im przekazać dane. Przykładowo, ostatnio

przedstawiciele Microsoftu potwierdzili, że zapytani przez służby amerykańskie musieliby przekazać im dane klientów na podstawie Patriot Act.. Trzeba też pamiętać, że poza Patriot Act istnieje również Foreign Intelligence Security Act, który również umożliwia służbom wywiadowczym ingerencje w dane w chmurze.

Czy instytucja zamawiająca usługę w chmurze wie w jakim kraju będzie znajdować się chmura?

Generalnie podmiot zamawiający nie wie, gdzie dane będą przetwarzane. Oczywiście możemy to wpisać do umowy. Wówczas dane będą przetwarzane tylko w określonych centrach danych, na które się zgodziliśmy.. Musimy jednak pamiętać, że w większości przypadków chmurowych mamy do czynienia z tzw. „adhezyjną" czyli umową przez przystąpienie – nie negocjujemy niczego, tylko przekazujemy nasze dane na podstawie wzorca przedłożonego przez dostarczyciela chmury. Kiedy zaczynamy istotnie ingerować w umowę i dostosowywać ją do naszych potrzeb to – najprościej mówiąc – więcej za to płacimy.

Jak w prawie polskim i unijnym zabezpieczane są dane w chmurze?

Nie ma przepisów, które dotyczą konkretnie bezpieczeństwa chmury. Ale z drugiej strony przetwarzanie danych w chmurze jest tylko nowym modelem biznesowym. Z punktu widzenia technicznego nie są to rozwiązania nowe, technologie te istniały już wcześniej.

Czy zatem istniejące przepisy prawne przystają do tego, co dzieje się w chmurach?

Istniejące przepisy umożliwiają rozwiązanie wiekszości zagadnień związanych z prawną stroną cloud computingu. W niektórych kwestiach pozostają jednak nierozwiązywalne problemy. Np. w przypadku ochrony danych osobowych największym problemem nie jest wcale przekazywanie danych osobowych do kraju trzeciego. Nierozwiązalną przeszkodą jest to, że administrator danych osobowych powinien utrzymać możliwość kontrolowania i przeprowadzania inspekcji tego, kto jest przetwarzającym dane osobowe. Czyli jeżeli przyjmiemy – w uproszczonym modelu – że administratorem jest użytkownik chmury, a przetwarzającym jest ten, kto chmurę dostarcza, trzeba byłoby wówczas przyjąć, że administrator danych osobowych będzie sprawdzał i dokonywał inspekcji centra przetwarzania danych, które są własnością dostarczyciela chmury. To jednak jest niewykonalne. Nie ma możliwości, by jakikolwiek administrator danych osobowych dokonał inspekcji centrum przetwarzania danych dostarczyciela chmury.

Jeśli mówi Pan, że jest to problem nierozwiązywalny, rozumiem, ze jest on również nierozwiązywalny na gruncie prawa europejskiego?

Tak, z tego powodu, że tego typu norma wynika z dyrektywy (ws. ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych). Można rozwiązać ten problem w nowych ramach prawnych dla ochrony danych osobowych np poprzez przyjęcie tzw. wiążących reguł korporacyjnych (BCR / Binding Corporate Rules), czyli zespołu reguł, które obowiązują u danego przedsiębiorcy i są przez niego respektowane niezależnie od tego w którym kraju dane są przetwarzane. Wówczas można byłoby założyć, że z takiego obowiązku kontroli zwolniona jest osoba, która przekazuje dane do podmiotu, który posiada BCR. Jeśli zatem BCR przygotowałby dostarczyciel chmury, miałby możliwość wyłączenia się spod tego obowiązku.

A czy gdyby był pan małym polskim przedsiębiorcą – wybrałby pan tradycyjny serwer firmowy czy chmurę?

Jeśli przetwarzałbym dane nie mające charakteru danych osobowych, pewnie wybrałbym chmurę. W innym przypadku zdałbym się chyba na tradycyjne rozwiązania, pamiętając jednak, że nawet one nie są stuprocentowo bezpieczne.

Karolina Zbytniewska, EurActiv.pl