

Dane w chmurze, czyli gdzie?

27 października 2014

Coraz częściej zapisujemy różne informacje nie na dyskach swoich komputerów, ale na zewnętrznych serwerach – korzystamy z kalendarza oferowanego nam razem z pocztą elektroniczną, notatki robimy nie w notatniku, a na zewnętrznych dyskach, a zdjęcia zamiast drukować – wrzucamy do sieci. Gdzie tak naprawdę przechowywane są te informacje i co się z nimi dzieje? Przedstawiamy podstawowe problemy związane z tzw. chmurą.

CHMURA, CZYLI CO?

Najogólniej rzecz biorąc, chmura obliczeniowa (cloud computing) to usługa przechowywania i wykorzystywania danych, do których dostęp uzyskuje się przez Internet, na znajdujących się w innej lokalizacji komputerach. Oznacza to możliwość korzystania za pomocą sieci z dużych mocy obliczeniowych i dysków pamięci oraz ograniczenie wydatków na własny sprzęt (np. pamięć operacyjną), a przede wszystkim wygodę – do zapisanych w chmurze danych dostęp uzyskać można z każdego łączącego się z Internetem urządzenia – komputera, tabletu czy smartfona. Bo na tym polega zasadnicza różnica – w cloud computing dane „wiszą w chmurze”, a nie na dysku konkretnego komputera.

Rozróżnia się kilka rodzajów chmur, m.in. chmury prywatne i publiczne – te pierwsze przeznaczone są dla konkretnej organizacji, zlokalizowane są w jej siedzibie lub w siedzibie innej firmy związanej z nią umową. Natomiast chmury publiczne to infrastruktura, którą posiada wyspecjalizowana firma oferująca tę usługę wielu podmiotom jednocześnie. W tym modelu to dostawca często dyktuje warunki, a użytkownik przekazuje mu znaczną kontrolę nad swoimi danymi.

CHMURA – WYZWANIA

Gdzie zapisane są maile? Albo notatki umieszczone na Google Drive? Właśnie w chmurze. Jednak nazwa ta jest myląca – informacje te nie wiszą w powietrzu, lecz umieszczane są na jakimś serwerze zlokalizowanym w jakimś konkretnym miejscu. Choćby z tego powodu chmura to nie tylko komfortowe korzystanie on-line ze swoich plików, ale także wyzwania dotyczące ochrony danych osobowych.

Dane w chmurze nie są zapisywane na naszym komputerze, tylko innym, który może znajdować się na drugim końcu świata. Poza oczywistym brakiem możliwości fizycznego skontrolowania, w jaki sposób są one przetwarzane, oznacza to również obowiązywanie innych przepisów. Kluczowe znaczenie ma przy tym rozróżnienie między Unią Europejską i innymi państwami, które stosują europejskie standardy ochrony danych a resztą świata, w której nie obowiązują wystarczająco restrykcyjne przepisy chroniące dane osobowe. Przechowując zatem dane np. na serwerach amerykańskich firm, nie jesteśmy chronieni europejskim prawem. Przy czym, jak wskazała Grupa Robocza art. 29 (organ zrzeszający inspektorów ochrony danych UE), „usługa w chmurze oferowana przez jednego dostawcę może być realizowana poprzez połączenie usług szeregu innych dostawców, które mogą być dynamicznie dodawane lub usuwane w czasie trwania umowy z klientem”. Każdy taki dostawca może mieć siedzibę w innym państwie, w innym porządku prawnym, co tym dodatkowo komplikuje sytuację prawną użytkownika chmury.

Nie mamy też gwarancji dotyczących poufności danych. Skoro np. zdjęcia nie są przechowywane na naszym komputerze, tylko w chmurze, częściowo tracimy kontrolę nad tym, kto ma do nich dostęp. Jeśli dostęp do naszego albumu zdjęć ma każdy, kto otrzyma link – nie mamy realnej kontroli nad tym, kto go obejrzy. Zawsze istnieje też ryzyko wycieku lub nieautoryzowanego dostępu do danych przechowywanych w chmurze. Do tego dochodzi również działalność państwa, którego organy (np. policja, służby) mogą uzyskiwać informacje o zawartości „naszej” chmury bezpośrednio od jej dostawcy, bez naszej

wiedzy i możliwości reakcji. Wystarczy przypomnieć informacje ujawniane przez Edwarda Snowdena na temat programu PRISM, by stwierdzić, że amerykańskie służby zapewne z takiego dostępu korzystają.

ŚRODKI ZARADCZE?

Pomimo zasygnalizowanych wyżej problemów, przetwarzanie danych w chmurze ma bardzo duży potencjał, również w zakresie przetwarzania w ten sposób danych przez organy administracji publicznej. Z myślą o nich Generalny Inspektor Ochrony Danych Osobowych przygotował dokument o nazwie „Dekalog chmuroluba”. GIODO zaleca w nim, by podmiot publiczny, który decyduje się na przekazanie danych do chmury, uzyskał pełną informację o wszystkich lokalizacjach serwerów, na których będą przetwarzane dane. Jednocześnie dostawca usługi powinien zapewnić pełen dostęp do dokumentacji dotyczącej zasad bezpieczeństwa i środków technicznych przyjmowanych w poszczególnych centrach przetwarzania danych.

Jakkolwiek trudno sobie wyobrazić, by każdy z nas weryfikował zasady, na jakich dostawca, z którego usług chcemy skorzystać, będzie przetwarzać dane gromadzone w chmurze, warto chociaż przeczytać regulamin tej usługi. Ma to szczególne znaczenie w sytuacji, w której dane osobowe, które chcielibyśmy w chmurze przetwarzać, mają szczególną wartość lub powinny być w szczególny sposób chronione, np. tajemnicą adwokacką. Nie można też zapomnieć, że np. rezygnując z prowadzenia tradycyjnego kalendarza i przenosząc go do chmury, powierzamy komuś innemu ważne informacje o nas. A przecież nie wszystkimi informacjami chcemy się dzielić – część z nich powinna zostać na twardych dyskach, bądź wręcz w papierowych notatnikach.

Autorzy: Wojciech Klicki, Katarzyna Szymielewicz, Anna Wąlkowiak

Źródło: [Fundacja Panoptikon](#)