

Cloud computing

22 października 2012

Czy tajne służby wiedzą o nas coraz więcej dzięki usługom chmurowym? Okazuje się, że to tylko jeden z wielu problemów...

Z usług chmurowych korzystamy wszyscy, zwykle nie zdając sobie z tego sprawy. Uruchamiając wyszukiwarkę Google, logując się do Facebooka czy wreszcie pobierając pliki z Dropboksa, wpływamy na tryby wielkiej maszyny wykorzystującej tysiące serwerów w różnych częściach świata.

W sieci zostawiamy więc coraz więcej osobistych plików i nie ma żadnych wątpliwości co do tego, że w przyszłości trend taki będzie się utrzymywał. Automatyczne wysyłanie zdjęć do serwisów społecznościowych czy archiwizowanie plików z lokalnych komputerów w usługach chmurowych – to wszystko dzieje się na naszych oczach.

Przyjrzyjmy się poniżej, czym ryzykujemy, wykorzystując chmury, a także co możemy zrobić, by były one dla nas nieco bezpieczniejsze.

WYCIEK DANYCH

Zdecydowanie najwięcej obaw użytkowników rozwiązań chmurowych, dotyczy wycieku ich danych. Jak wspomniałem wcześniej, dla naszej wygody coraz więcej plików przesyła się do zdalnych serwerów automatycznie. W ten sposób, włączając komputer, możemy przeglądać zdjęcia zrobione smartfonem czy synchronizować swoje dokumenty na wszystkich urządzeniach w domu.

Głównym problemem tego typu technologii jest fakt, że interfejs umożliwiający podejrzenie naszych plików ma każdy internauta. Zwykle wystarczy więc wyłącznie znajomość hasła i loginu, by uzyskać dostęp do naszych osobistych danych, plików czy aktualnych e-maili.

Również w przypadku skali przemysłowej, gdzie technologie chmurowe dedykowane są całym przedsiębiorstwom, możliwy wyciek danych jest jednym z ważniejszych zagrożeń. Pod uwagę trzeba brać jednak nie tylko ataki z zewnątrz, ale również z wewnątrz firmy dostarczającej technologie typu cloud.

UTRUDNIONA MIGRACJA

Korzystając z narzędzi, które dostarczane są w modelu chmurowym, często w ręce zewnętrznych firm oddajemy również własne pliki. Jest to bardzo wygodne i oszczędza czas przynajmniej do momentu, gdy zechcemy przejść na rozwiązania konkurencji. W takim przypadku możemy liczyć na niemałe problemy.

Aby nie zagłębiać się w niezrozumiałe przykłady na polu rozwiązań korporacyjnych, warto przypomnieć chociażby przykład sieci społecznościowych Google+ i Facebook. Gdy wyszukiwarkowy gigant przygotował własną usługę tego typu, witryna Zuckerberga utrudniała eksport jakichkolwiek danych użytkowników, by utrudnić ewentualną migrację do nowego projektu.

Problem jest znacznie mniejszy, gdy mamy możliwość wygodnego pobrania swoich plików. W przypadku dysków sieciowych, takich jak Dropbox, bez problemu ściągniemy wszystkie swoje dane, które później łatwo wysłać np. do konkurencyjnego Dysku Google czy SkyDrive'a.

BRAK KONTROLI NAD URZĄDZENIAMI

Eksportowanie danych do chmury to jedno, jednak zarządzanie nimi to już zupełnie inny problem. O ile z zamieszczeniem pliku w sieci zwykle nie będziemy mieli większej trudności, tak już skasowanie zdjęcia czy dokumentu może okazać się niezwykle trudne bądź nawet niemożliwe.

O tym ostatnim przekonali się jakiś czas temu użytkownicy Facebooka. Witryna pozwalała na stworzenie bezpośredniego

linka do dowolnego zdjęcia w serwisie. Jeśli użytkownik decydował się na skasowanie grafiki, owszem znikająca ona z albumu, jednak wciąż dostępna była na serwerze i otworzyć mógł ją każdy, kto wcześniej zapisał sobie link.

Możliwość odczytu danych przez innych internautów, nawet po ich usunięciu, to jednak bardzo skrajny przykład. Zwykle należy liczyć się po prostu z faktem, że wszystko, co zamieścimy w usługach chmurowych, może tam pozostać na bardzo długo. Powracając do przykładu Facebooka, nawet jeśli skasujemy historię naszych rozmów z czatu, tak by nie były one dostępne dla innych użytkowników, wciąż znajdują się one w archiwach witryny (np. na wypadek gdyby potrzebowała ich policja lub sąd).

INWIGILACJA

W sieci nie brakuje osób, które donosiłyby o wszechobecnej inwigilacji. Trzeba uczciwie przyznać, że nowe technologie połączone np. z algorytmami rozpoznawania twarzy faktycznie mogą znacznie ułatwić różnego rodzaju służbom śledzenie ludzi.

Z drugiej strony należy zadać sobie proste pytanie: czy rzeczywiście kogoś poza naszymi znajomymi mogłyby interesować pliki, które przechowujemy w chmurze? Jeśli tak, warto dobrze przestudiować zasady korzystania z wybranych usług, jak również prześledzić historię współpracy ich dostawcy z organami ścigania. Niektóre duże firmy po prostu stają zwykle po stronie internautów, a inne wolą mieć lepsze stosunki z organami ścigania.

Autor: Adrian Nowak

Źródło: [Dziennik Internautów](#)