# Bezpieczeństwo w chmurach

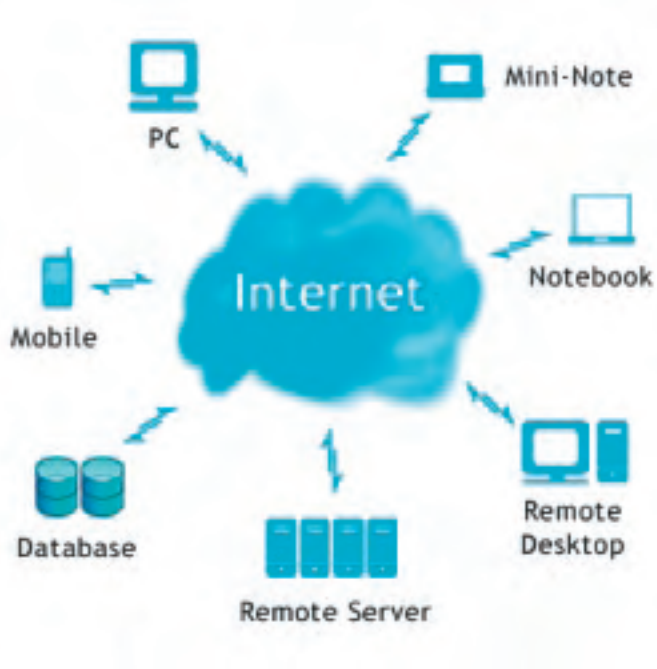
**dr inż. MAREK HOŁYŃSKI,** Instytut Maszyn Matematycznych, Warszawa

*Cloud computing* szybko awansowało do roli obowiązującego słowa magicznego. Jego orędownicy ogłaszają, iż jest to najbardziej obiecujący kierunek rozwojowy informatyki i robią to na tyle przekonywująco, że niemal co druga organizowana w ostatnim roku konferencja dotyczy jakiegoś aspektu przetwarzania w chmurze. Ale są też sceptycy utrzymujący, że z dużej chmury mały deszcz, a cały ten zgiełk to zręczny chwyt marketingowy, służący jedynie rozkręceniu popytu na sprzęt i usługi.

Obie strony mają trochę racji. Model przetwarzania oparty na zasobach zewnętrznych nie jest niczym nowym i w naturalny sposób stanowi rozwinięcie dotychczasowych koncepcji. Zamiast robić wszystko samemu na własnym komputerze, wyrzucamy co się da na zewnątrz, pozbywając się zawracania głowy i odciążając nasz system od zbędnych zadań.

## Nic nowego pod chmurami

Sam pomysł nie jest nowy, to raczej kolejna faza rysującej się już od dość dawna tendencji. Już w latach 70. pojawił się termin *distributed computing* na określenie systemów umożliwiających współdzielenie rozproszonych mocy obliczeniowych. Przebojem lat 80. był *outsourcing*, czyli jak sama nazwa wskazuje właśnie wykorzystywanie zasobów zewnętrznych. Potem modne stało się hasło *utility computing* oznaczający usługi komputerowe dostępne w domowym gniazdku podobnie jak prąd czy gaz. Po drodze była wirtualizacja – elastyczne dostosowanie sprzętu i oprogramowania zgodnie z wymaganiami odbiorców. Od jakiegoś czasu popularny jest skrót SaaS (*Software as a Service*), odnoszący się do udostępniania software'u użytkowego przez sieć.




**Rys. 1. Wizualizacja w postaci chmury pozwoliła w prosty sposób wytłumaczyć istotę cloud computing szerokiej publiczności**
**Fig. 1. Such visualizations allowed to explain the essence of cloud computing to the public**

*Cloud computing* nie jest zatem jakąś rewolucyjną ideą i istotnie do pewnego stopnia marketingową manipulacją. Sloganem jednak bardzo nośnym i pożytecznym – puchaty obłoczek i wychodzące z niego strzałki do różnych aplikacji i użytkowników działa na wyobraźnię. Pozwala w prosty wizualny sposób wytłumaczyć istotę i znaczenie tego trendu szerokiej publiczności.

Coraz rzadziej trafiają się znajomi pytający: „Co to jest ta chmura? Czy ja powinienem zacząć tego używać?" Już używasz, choć o tym nie wiedziałeś. Od paru lat masz konto gmaila i twoja skrzynka pocztowa wcale nie jest ulokowana w twoim laptopie, tylko na jakimś serwerze pocztowym gdzieś na świecie. To jest właśnie przetwarzanie w chmurze.

„Ojej, rzeczywiście nie pomyślałem o tym. Ale czy nie ma w tym jakichś zagrożeń? Nie chciałbym, żeby wszystko, co wysyłam i odbieram było powszechnie dostępne." Dobre pytanie. Wiele osób zastanawia się nad tym, czy chmura jest bezpieczna.

## Mały obłoczek?

Sprzedawcy informatycznej infrastruktury i serwisów sieciowych oczywiście utrzymują, że wszystko jest należycie zabezpieczone. Prawda, ale nie do końca. W Internecie przecież ciągle istnieją znane nam dobrze stare zagrożenia, a chmura dodatkowo stwarza nowe. Tu więcej danych narażonych jest na wyciek lub utratę, łatwiejsze staje się przejęcie konta albo aplikacji przez osoby nieuprawnione. Pojawiają się problemy z kompatybilnością wspólnie używanych narzędzi, brakuje standardów, serwery się przeciążają, zabezpieczenia interfejsów są niedostateczne. Nie przypadkiem w środowiskach chmury nastąpił znaczny wzrost liczby wykroczeń, zwłaszcza „oszustw 419" polegających na wyłudzaniu transferów pieniędzy (nazwa *419 scam* pochodzi od numeru artykułu w nigeryjskim kodeksie karnym).

Sceptycyzm ciągle dominuje w powszechnym odbiorze, podsycany częstymi doniesieniami o włamaniach, wirusach i utracie kluczowych danych. Czy w tej sytuacji powinniśmy mieć aż takie zaufanie do dostawcy usług, aby powierzać mu kontrolę nad firmowymi tajemnicami, dostępem do kont, maili, haseł i prywatnych archiwów? Trudno się zatem dziwić, że w ankiecie przeprowadzonej przez firmę Mimecast 62% przedsiębiorców uznało, że ich dane w chmurze nie są w pełni bezpieczne. Co więcej 54% z nich nie było pewnych, czy korzyści z *cloud computing* przewyższają potencjalne ryzyko ich stosowania.

Co gorsza przetwarzanie w chmurze nie zawsze spełnia wymagania obowiązujących przepisów prawnych. Niektóre z aplikacji nie mieszczą się w kryteriach narzucanych przez ustawę o ochronie danych osobowych. Ponadto część regulacji unijnych wiąże zgodę na usługi z miejscem ich świadczenia, co w przypadku chmury jest trudne do ustalenia. W wielu działach gospodarki, np. w bankowości, przepisy wewnętrzne są tak ostre, że o wprowadzeniu cloud computing nie może być mowy.

Znana jest też słabość metod silnego uwierzytelniania w chmurze. Zmniejszenie poziomu ryzyka okupuje się wtedy zredukowaniem funkcjonalności, albo ograniczeniem zakresu, do tzw. chmury prywatnej lub dedykowanej. Tak właśnie było podczas ostatniego Narodowego Testu Interoperacyjności Podpisu Elektronicznego, gdy jedna z uczestniczących firm zgłosiła podpis elektroniczny działający *in-the-cloud*. Szybko okazało się, że to tylko niewielki obłoczek o bardzo ograniczonym zasięgu.

## Chmury nie takie czarne

Żeby nie tworzyć obrazu zupełnie czarnej chmury, należy jednak wspomnieć o korzyściach dla bezpieczeństwa, wynikających z *cloud computing*. Należy do nich bez wątpienia uaktualnianie oprogramowania dokonywane automatyczne przez aplikacje. Nie zawsze bowiem mamy czas lub pamiętamy o *updatach* (a niektóre firmy dostarczają je już co godzinę), co szczególnie w narzędziach antywirusowych może mieć przykre konsekwencje. Ważna jest też naturalna redundancja chmury poprawiająca niezawodność sprzętu i oprogramowania, a rozproszone lokalizacje zmniejszają zależność od awarii sieci, nieprzewidzianych katastrof, czy kataklizmów pogodowych.

Docenia te zalety Unia Europejska inicjując opracowanie strategii rozwoju chmur obliczeniowych na naszym kontynencie. Komisarz Neelie Kroes chce nawet, żebyśmy na tym obszarze nie byli tylko *cloud-friendly*, ale *cloud- active*, inicjując zmiany. Przegląd sytuacji i praktyczne zalecenia w tej dziedzinie zawarte są w „Opinii w sprawie chmur obliczeniowych w Europie" przygotowanej przez Europejski Komitet Ekonomiczno-Społeczny, w której zagrożeniom poświęcono sporo miejsca.

Trzeba przyznać, że od czasu pojawienia się w końcu ostatniej dekady pierwszych specjalizowanych zabezpieczeń, ich skuteczność w chmurze stale rośnie. Dostępne są już rozwiązania w miarę sprawnie filtrujące przesyłane treści nie jak dotąd na komputerze odbiorcy, ale zanim one jeszcze do niego dotrą, określane jako *security in-the-cloud*. To przydaje się zwłaszcza w urządzeniach mobilnych o ograniczonej pojemności pamięci, bo tzw. rejestry sygnatur (spisy wirusów, trojanów, niebezpiecznych stron, etc.) osiągają już pokaźne rozmiary.

Pozytywnym zjawiskiem jest łączenie sił przez firmy zajmujące się tą dziedziną i tworzenie aliansów w rodzaju Trusted Cloud Initiative czy Cloud Security Alliance. To dobra wiadomość, bo wszystko wskazuje na to, iż przetwarzanie w chmurze, ze względu na swoją przydatność i wygodę, będzie się rozwijać. I rzecz jasna, pojawią się crackerzy wyćwiczeni w rozbijaniu chmur oraz podniebne wirusy i trojany.