ROZDZIAŁ 1
Fenomen chmury
Phenomenon of the cloud

Mirosław Kutyłowski

Technologie bezpieczeństwa dla przetwarzania w chmurze

1. Wstęp

Przetwarzanie w chmurze staje się obecnie atrakcyjną alternatywą wobec wdrażania dedykowanych systemów informatycznych. Pozwala to znacząco zredukować koszty zarówno w kategoriach hardware'u i software'u, jak i kosztów pośrednich związanych z nakładem pracy niezbędnym do uruchomienia i administracji systemem. Technologie chmurowe, mimo że znaczącą rolę na rynku rozwiązań informatycznych zdobyły stosunkowo niedawno, są w sensie technicznym rozwiązaniami dojrzałymi. Ich szerokie zastosowanie jest jednak w dużym stopniu warunkowane rozwojem sieci teleinformatycznych zapewniających niezawodną łączność o wysokich parametrach użytkowych. Obecnie nie stanowi to już problemu.

Migracja systemów informatycznych w nową rzeczywistość technologiczną nie jest jednak bezproblemowa. Jednym z kluczowych problemów jest zapewnienie odpowiedniego poziomu bezpieczeństwa. Kwestie bezpieczeństwa, tak trudne do rozwiązania w przypadku systemów konwencjonalnych, nie zawsze stają się łatwiejsze przy przejściu do systemów opartych na chmurze obliczeniowej. Rozwiązując jedne problemy, stajemy wobec nowych wyzwań – niekiedy jeszcze trudniejszych.

2. Prawny system ochrony danych w systemach teleinformatycznych

Ochrona systemów informatycznych musi być oparta nie tylko na rozwiązaniach technicznych, lecz także na ochronie organizacyjnej i odpowiednich zasadach prawa. Podczas gdy rozwiązania techniczne, a także – w pewnym stopniu – rozwiązania organizacyjne ewoluują dosyć szybko, zmiany w obszarze regulacji prawnej i norm technicznych postępują wolno. Z tego względu obowiązujące normy prawne odpowiadają często realiom technicznym z minionych dekad, nierzadko powodując zagrożenia bezpieczeństwa.

2.1. Odseparowanie fizyczne

Jedną z podstawowych zasad zapewniających bezpieczeństwo systemów przetwarzania danych w przypadkach, gdy konieczna jest ich ścisła kontrola, jest odseparowanie fizyczne nośników i urządzeń składających się na wspomniany system. Jest to dobra praktyka wywodząca się z przetwarzania danych metodami tradycyjnymi – tj. na papierze. Podejście to znajduje swe odzwierciedlenie w przepisach dotyczących choćby ochrony danych osobowych.

W sytuacji chmury obliczeniowej separacja fizyczna jest warunkiem, który z definicji nie jest spełniony. Źródłem efektywności ekonomicznej chmury jest współdzielenie zasobów oraz migracja danych i procesów przetwarzania danych do chmury, zazwyczaj nieznajdującej się pod kontrolą właściciela danych.

2.2. Odseparowanie logiczne

W sytuacji gdy pełna separacja fizyczna nie jest możliwa – choćby ze względu na konieczność zapewnienia interakcji z użytkownikami zewnętrznymi, proponuje się zabezpieczenia na poziomie logicznym mające zastąpić separację fizyczną. Rozwiązania takie jak *firewall* mają wprowadzić separację między procesami zachodzącymi wewnątrz chronionego systemu a światem zewnętrznym – tak jak w przypadku procedur dostępu fizycznego definiowane są procedury komunikacji z chronionym systemem i wzajemnego przepływu danych.

Metody separacji logicznej są wymieniane przez wiele przepisów dotyczących ochrony danych. Przepisy te mówią prawie wyłącznie o obowiązku instalacji odpowiednich systemów ochronnych, nie określając bliżej, jaki mają mieć stopień rzeczywistej efektywności. Brak szczegółowych regulacji wynika z dosyć skomplikowanej sytuacji pod względem technicznym (właściwie jedynym rozwiązaniem typu *firewall*, który zapewnia pełne bezpieczeństwo jest *firewall*, który w ogóle nie przepuszcza ruchu). W ostatnich latach pojawiły się systemy realizujące rozdzielenie logiczne wspomagane mechanizmami hardware'owymi[1], jednak jak dotąd nie są zbyt rozpowszechnione.

W przypadku przetwarzania w chmurze dochodzi do separacji nie na poziomie rozdzielenia przepływu danych między urządzeniami fizycznymi, ale między urządzeniami o charakterze wirtualnym. Jest to technika dużo bardziej zaawansowana, jednak przez posadowienie jej na niższym poziomie stosu protokołów może być co najmniej tak samo skuteczna. Wirtualizacja okazuje się nie tylko efektywnym rozwiązaniem dla zapewnienia łatwości korzystania z usług – w równym stopniu ułatwia ona administrowanie systemem, w tym faktyczne zapewnienie wysokiego poziomu bezpieczeństwa. Technologie chmurowe mają również wbudowane mechanizmy obserwacji urządzeń wirtualnych i nie pozwalają przekraczać im posiadanych uprawnień.

[1] Zob. http://www.lock-keeper.org (dostęp: 5.4.2013 r.).

2.3. Wyłączność kontroli

Bardzo istotnym zagadnieniem w obszarze bezpieczeństwa jest zapewnienie odpowiedniej kontroli nad czynnościami dokonywanymi przez użytkownika systemu. Stworzenie odpowiedniego systemu administrowania uprawnieniami jest jednym z trudniejszych i dotąd nierozwiązanych satysfakcjonująco problemów bezpieczeństwa komputerowego.

Podstawowym zagrożeniem są tu ataki polegające na zdobywaniu faktycznych możliwości wykonania określonych operacji przez obchodzenie mechanizmów kontroli zdefiniowanych w systemie. Metody ataku mogą bazować na wykorzystywaniu zarówno luk w interpretacji danych (takich jak technika *SQL injection*), jak i nieszczelnego systemu definiującego uprawnienia (co jest trudne do uniknięcia w dużych systemach).

W przypadku rozwiązań chmurowych problemy te nabierają olbrzymiego znaczenia ze względu na współdzielenie zasobów i zdalny dostęp do zasobów przez klientów.

3. Zagadnienia bezpieczeństwa rozwiązywane przez technologie chmurowe

Jakkolwiek przeniesienie systemów komputerowych do chmury obliczeniowej stwarza wiele problemów bezpieczeństwa, należy zauważyć również, że realizacja usług w ten sposób rozwiązuje pewne szeroko spotykane problemy w sposób bardzo efektywny.

3.1. Efektywność zarządzania

Implementacja chmury wiąże się w pewien sposób z uporządkowaniem zarządzania uprawnieniami. Ze względu na skalę przedsięwzięcia czynności te w chmurze obliczeniowej muszą być zorganizowane w dobrze udokumentowany i weryfikowalny sposób. Wiele czynności zostało zautomatyzowanych, dzięki czemu zredukowaniu ulega obszar, na jakim luki mogą powstać dzięki błędom lub w wyniku braku wystarczającej wiedzy administratora systemu.

3.2. Czas reakcji na zagrożenia bezpieczeństwa

Jednym z podstawowych zagrożeń w przypadku systemów tradycyjnych jest zbyt długi czas reakcji na odkryte luki bezpieczeństwa. Czas dokonywania niezbędnych poprawek w zakresie konfiguracji systemu, wymiany oprogramowania, instalowania dodatkowych zabezpieczeń itp. jest w wielu przypadkach zdeterminowany przez możliwości kadrowe posiadacza systemu – a tu wręcz regułą jest niewystarczająca obsada stanowisk administratorów systemu. Problemem może być również brak dostępu do specjalistów o wąskich specjalnościach, odpowiadających określonemu zagrożeniu.

Co prawda w przypadku technologii chmurowych mogą wystąpić dokładnie te same problemy z lukami bezpieczeństwa, jednak zarządzanie chmurą jest o tyle łatwiejsze, że następuje koncentracja obowiązków i uprawnień administracyjnych. Liczba koniecznych ręcznych interwencji w systemie zostaje znacząco zredukowana i może być dokonywana w skali globalnej przez wyspecjalizowane zespoły.

3.3. Chmura prywatna, publiczna czy hybrydowa

Technologia chmurowa nie narzuca współdzielenia zasobów przez różne systemy, a jedynie to umożliwia. Tym samym mamy do czynienia z zagadnieniem wyboru jednego z trzech następujących rozwiązań:

1) chmura prywatna: cała instalacja jest w wyłącznym użytkowaniu jednego podmiotu i znajduje się pod jego bezpośrednią kontrolą;
2) chmura publiczna: system znajduje się w przestrzeni publicznej, często poza obszarem jurysdykcji kraju klienta; kontrola nad taką chmurą ze strony pojedynczego klienta jest znikoma;
3) chmura hybrydowa: jakkolwiek chmura obliczeniowa jest współdzielona między wiele systemów, zaimplementowane są mechanizmy umożliwiające separację i rozliczalność czynności.

Pierwsza ze wspomnianych kategorii jest bezpieczniejsza, ale może okazać się mało atrakcyjna ekonomicznie. Druga może być stosowana jedynie w przypadkach niewymagających poważniejszej ochrony danych. Najbardziej atrakcyjną architekturą dla budowy systemów na potrzeby podmiotów gospodarczych i publicznych wydaje się architektura hybrydowa – łącząc efektywność ekonomiczną z względnie wysokim poziomem bezpieczeństwa.

4. Nowe zagrożenia bezpieczeństwa wprowadzane przez technologie chmurowe

4.1. Niebezpieczeństwa kontraktowe

Technologie chmurowe są rozwijane przez stosunkowo niewielką liczbę dużych producentów. Oparcie się na jakimkolwiek rozwiązaniu stwarza niebezpieczeństwo uzależnienia się od konkretnego globalnego koncernu. Zagrożenie ma charakter zarówno polityczny (w przypadku oparcia administracji publicznej na rozwiązaniach chmurowych), jak i ekonomiczny (wywiad gospodarczy prowadzony przez dostawcę rozwiązań chmurowych na rzecz macierzystego kraju). Na koniec, powierzając system chmurze, narażamy się na niebezpieczeństwa związane z kondycją ekonomiczną właściciela chmury. W przypadku bankructwa lub zaprzestania działalności właściciel danych może być postawiony w bardzo trudnej sytuacji.

4.2. Istnienie danych

Jedną z podstawowych usług przetwarzania w chmurze jest utrzymywanie zasobów informacyjnych nie u klienta chmury, lecz wyłącznie przez chmurę obliczeniową. Są to usługi nazywane StaaS (*Storage as a Service*). Są one szczególnie atrakcyjne, gdy po stronie klienta dane wprowadzane są w sposób rozproszony, przez wielu użytkowników. Zaletami StaaS są m.in. zaawansowana technicznie ochrona przed fizycznymi awariami nośników informacji, zmniejszenie kosztów sprzętu przez ich współdzielenie z innymi użytkownikami oraz krótki czas uruchomienia usługi w porównaniu do budowy własnych centrów magazynowania danych.

Stosowanie rozwiązań StaaS prowadzi jednak do sytuacji, gdy po stronie chmury następuje gromadzenie dużego wolumenu danych wprowadzanych stopniowo przez dłuższy okres, przy wykorzystaniu łączy komunikacyjnych o stosunkowo niskiej pojemności. Transfer tych danych w całości z powrotem do klienta może być niezwykle trudny ze względu na ograniczenia pojemności kanału komunikacyjnego z chmury do klienta i jest możliwy jedynie w sytuacjach wyjątkowych i stosunkowo wysokim kosztem. W normalnych sytuacjach wystarcza dostęp do danych za pomocą typowych zapytań bazodanowych. Ponieważ klient nie posiada kopii zbioru wprowadzonych danych, sprawdzenie prawidłowości odpowiedzi może być niewykonalne. W szczególności sprawdzenie przez klienta, czy zbiór danych znajdujący się w chmurze odpowiada dokładnie temu, który został wprowadzony przez właściciela danych, jest niewykonalne w bezpośredni sposób.

Rozwiązaniem przedstawionych problemów mogą stać się mechanizmy kryptograficzne zwane *Proof of Possesion* oraz *Provable Data Possesion*[2]. Idea polega na obliczeniu przez klienta dla każdego wprowadzanego do chmury rekordu dwóch krótkich kodów kryptograficznych. Jeden z nich dołączany jest do oryginalnego rekordu umieszczanego w chmurze, drugi zachowywany jest przez klienta. W dowolnym momencie klient może zadać zapytanie, na które chmura jest w stanie odpowiedzieć jedynie w przypadku, gdy ma dane wprowadzone przez klienta w niezmienionej postaci wraz z kodami kryptograficznymi. Z kolei klient może zweryfikować odpowiedź na podstawie lokalnie przechowywanych kodów kryptograficznych.

Wspomniane rozwiązania mają jednak tę wadę, że pojedynczym zapytaniem nie można zweryfikować całości danych, a jedynie wybrany, stosunkowo niewielki fragment. Zarazem może to być dowolny fragment – co powinno zniechęcać operatora chmury do niewłaściwej realizacji usług. Kolejną wadą tych rozwiązań jest to, że znajdują się obecnie raczej w sferze eksperymentalnej.

[2] *G. Ateniese*, *R. C. Burns*, *R. Curtmola*, *J. Herring*, *L. Kissner*, *Z. N. J. Peterson*, *D. Xiaodong Song*, „Provable data possession at untrusted stores" – ACM Conference on Computer and Communications Security 2007, s. 598–609.

4.3. Zarządzanie uprawnieniami

Tradycyjne podejście do ochrony zasobów informacyjnych łączy ochronę dostępu metodami logicznymi i fizycznymi. W przypadku operacji o krytycznym poziomie bezpieczeństwa (np. dokonywanych przez operatora systemu) zasadą sztuki jest rygorystyczne przestrzeganie zasad ochrony fizycznej. Znajduje to bezpośrednie odzwierciedlenie np. w przepisach dotyczących ochrony informacji niejawnych.

Podejście takie jest uzasadnione ograniczoną skutecznością środków zdalnego uwierzytelniania. Metody zdalne są oparte na dwóch mechanizmach: wiedzy osoby uwierzytelniającej się oraz środków technicznych będących w jej posiadaniu, takich jak tokeny kryptograficzne. Z konieczności wiedza musi być ograniczona do kilku stosunkowo prostych haseł. Z kolei osobiste urządzenia techniczne tak długo chronią, jak długo znajdują się pod wyłączną kontrolą właściciela.

W przypadku systemów opartych na paradygmacie chmury bezpośrednia fizyczna kontrola klienta nad przetwarzaniem danych jest w zasadzie niemożliwa. Wykorzystanie tej technologii w niektórych sytuacjach wymagających rygorystycznej kontroli nad niektórymi operacjami jest zatem wykluczone.

Z drugiej strony, w przypadku dużych systemów, ze skomplikowanym systemem praw dostępu przez jego użytkowników, chmura może oferować skuteczne rozwiązania zarządzania uprawnieniami. Koszt takich rozwiązań – zwykle trudny do sfinansowania – w przypadku chmury rozkłada się na wielu jej użytkowników. Dotyczy to w równym stopniu budowy i egzekwowania polityk dostępu. Jest to o tyle istotne, że błędy w tym obszarze dość często prowadzą do krytycznych zagrożeń bezpieczeństwa.

4.4. Nieuprawniony dostęp do danych i ich autentyczność

Jednym z podstawowych zagrożeń związanych ze stosowaniem technologii chmury jest niebezpieczeństwo nieuprawnionego dostępu do danych umieszczonych w chmurze. W przypadku rozwiązań klasycznych ochrona dostępu do danych leży bezpośrednio w gestii ich właściciela. W przypadku chmury następuje rozdzielenie ról. Jakkolwiek operator chmury może być związany obowiązkami kontraktowymi, udowodnienie udzielenia nieuprawnionego dostępu może być niezwykle trudne.

Rozwiązaniem szeroko stosowanym w takim przypadku jest umieszczanie w chmurze danych odpowiednio zaszyfrowanych. Stosowany tryb szyfrowania powinien uniemożliwiać np. fakt pojawienia się tych samych danych w różnych miejscach zaszyfrowanego zbioru. W przeciwnym przypadku, np. przy zastosowaniu trybu szyfrowania ECB, możliwe byłoby uzyskanie pewnych informacji na temat zbioru danych bez konieczności łamania algorytmu szyfrowania. Oczywiście, aby rozwiązanie to było efektywne, klucz do deszyfrowania nie może być dostępny dla operatora chmury.

Właściciel danych umieszczonych w chmurze powinien zabezpieczyć się przed jeszcze jedną możliwością – przed losową zmianą zawartości zaszyfrowanego zbioru danych. Istotnie, losowe zmiany nawet niewielkiej liczby bitów kryptogramu prowadzą do bardzo

głębokich zmian danych po ich zdeszyfrowaniu. Atakujący może w ten sposób zmodyfikować przechowywane dane mimo braku kluczy do szyfrowania. Aby temu zapobiec, stosuje się łącznie szyfrowanie wraz z technikami MAC (*message authentication code*).

Ze względu na siłę stosowanych technik kryptograficznych zdawać by się mogło, że zagrożenia zostały opanowane. Nie jest tak do końca. Problemem stają się już proste operacje przeszukiwania danych czy zapytania bazodanowe. Jakkolwiek istnieją pewne prace teoretyczne dotyczące możliwości szukania wzorca w zaszyfrowanych danych bez konieczności deszyfrowania, proponowane algorytmy są skomplikowane i mało efektywne obliczeniowo. Ich stosowanie prowadziłyby do rozwiązań ekonomicznie nieatrakcyjnych dla użytkownika chmury.

Warto zaznaczyć, że pewna ograniczona liczba zapytań bazodanowych może być realizowana bezpośrednio na kryptogramach. Dotyczy to głównie dodawania zaszyfrowanych liczb. Realizowane jest to przez techniki szyfrowania homomorficznego – są to jednak metody asymetryczne, o stosunkowo niskiej efektywności obliczeniowej.

4.5. Sekwencja dostępu

W przypadku stosowania odpowiedniego trybu szyfrowania danych przechowywanych w chmurze można by mieć nadzieję, że żadne informacje nie przepływają do operatora chmury. Niestety, wiele bardzo ważnych informacji może wyciekać w niekontrolowany sposób przez ujawnienie samej sekwencji dostępu do zaszyfrowanych danych. Problemem jest np. to, że rekordy danych często wykorzystywane przez użytkownika zbioru danych są również często pobierane z chmury. Częstotliwość użycia może być częściowo maskowana przez wykorzystanie mechanizmu *cache,* jednak i ta metoda niewiele daje w przypadku, gdy określony rekord może być modyfikowany i konieczne jest sprawdzenie jego bieżącego stanu.

Okazuje się, że wzmiankowana wyżej metoda *Traffic analysis* jest szeroko stosowana np. w działaniach śledczych. Zakres wyciekających informacji jest zaskakująco duży, jakkolwiek dane te dotyczą nie poszczególnych rekordów bazy danych, lecz jej ogólnego przeznaczenia oraz aktywności właściciela danych. Te ostatnie są niekiedy niezwykle cenne dla atakującego, cenniejsze nawet od statycznych danych przechowywanych w chmurze.

Problem ochrony informacji na temat sekwencji dostępu nie jest aż tak trudny w przypadku systemów zbudowanych w sposób konwencjonalny. Zupełnie inaczej jest w chmurze. Pewne możliwości techniczne ochrony w tym zakresie istnieją i są oparte na permutowaniu zawartości bazy danych i bezpiecznym hardware'owym *cache'u* u użytkownika[3]. Rozwiązania te wiążą się jednak z dużą złożonością komunikacyjną (w przypadku długotrwałego korzystania ze zbioru danych) i są trudne w implementacji[4].

[3] *S. Wang*, *X. Ding*, *R. H. Deng*, *F. Bao*, Private Information Retrieval Using Trusted Hardware, ESORICS 2006, s. 49–64, LNCS 4189.

[4] *M. Kutyłowski*, *Ł. Krzywiecki*, *P. Kubiak*, *M. Koza*, Restricted Identification Scheme and Diffie-Hellman Linking Problem, INTRUST 2011, s. 221–238, LNCS 7222.

4.6. Informatyka śledcza

W przypadku tradycyjnych systemów podstawowa metoda śledcza polega na przejęciu przez śledczych urządzeń, za pomocą których dochodzić mogło do przestępstw, i badanie ich zawartości – śladów pozostawionych w systemie przez działania prowadzone przez użytkownika. Dotyczy to nie tylko informacji bezpośrednio dostępnych, lecz również np. informacji fizycznie istniejących na nośnikach pamięci, a jedynie „zapomnianych" przez system operacyjny.

W przypadku systemów opartych na chmurze przejęcie urządzeń przez śledczych może być niezwykle kłopotliwe, gdy jest to chmura publiczna lub hybrydowa. Wyłączenie zasobów danych dla dużej grupy użytkowników narusza ich prawa i może mieć na tyle poważne konsekwencje ekonomiczne, polityczne, społeczne, że organy prowadzące dochodzenie mogą obawiać się podjęcia takich kroków. Innym krytycznym zagadnieniem w tym przypadku jest możliwość uzyskania dostępu do danych osób trzecich, co do których nie toczy się żadne postępowanie. Technologia chmury obliczeniowej może stać się w ten sposób efektywnym narzędziem sprawowania władzy dla reżimów o charakterze policyjnym.

5. Wnioski

Jak widać, realizacja systemów informatycznych w chmurze zmienia gruntownie sytuację pod względem kluczowych zagrożeń bezpieczeństwa. Z tego względu decyzja co do możliwości zastosowania technologii chmurowych musi być podjęta po analizie ryzyka przeprowadzonej odrębnie dla implementacji tradycyjnej i wykorzystania usług w chmurze.

Nie istnieje jednoznaczna odpowiedź, który tryb realizacji zadań jest bezpieczniejszy. W wielu obszarach (takich jak choćby przetwarzanie informacji niejawnych) brak jest dotąd technologii, które gwarantowałyby spełnienie fundamentalnych wymagań. Jednakże istnieje wiele obszarów, gdzie przeniesienie usług do chmury obliczeniowej przyniosłoby podniesienie poziomu bezpieczeństwa w sposób skokowy, przez wprowadzenie profesjonalnego i efektywnego ekonomicznie systemu zarządzania bezpieczeństwem.

Streszczenie

Technologia chmury obliczeniowej wskazywana jest przez wiele osób jako pragmatyczne rozwiązanie dla budowy dużych systemów informatycznych. Zalety ekonomiczne nie powinny jednak przesłaniać zagadnień bezpieczeństwa związanych z zastosowaniem chmury – mamy tu do czynienia zarówno ze znaczącym postępem na wielu obszarach w porównaniu do systemów konwencjonalnych, jak i nowymi problemami wynikającymi ze współdzielenia zasobów i przeniesienia danych w przestrzeń

wirtualną. Wiele tych problemów nie ma jeszcze dojrzałych rozwiązań technicznych. W niniejszym artykule zostały naszkicowane niektóre z nich.

Summary

Security technologies for cloud computing

Cloud computing technology is widely regarded as a pragmatic solution for building large ICT systems. Economic advantages, however, should not conceal security issues associated with the use of the cloud – we have to do both with a significant progress in many areas compared to conventional systems, as well as with new problems arising from sharing resources and transfering data to virtual space. A number of problems of this kind are still open and no mature technologies are available. This paper briefly presents some of them.